# DEFENDING OUR DEMOCRACY: BUILDING PARTNERSHIPS TO PROTECT AMERICA'S ELECTIONS

## HEARING

BEFORE THE

## COMMITTEE ON HOMELAND SECURITY
## HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

FEBRUARY 13, 2019

**Serial No. 116–1**

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE
35–094 PDF WASHINGTON : 2019

## COMMITTEE ON HOMELAND SECURITY

Bennie G. Thompson, Mississippi, *Chairman*

Sheila Jackson Lee, Texas
James R. Langevin, Rhode Island
Cedric L. Richmond, Louisiana
Donald M. Payne, Jr., New Jersey
Kathleen M. Rice, New York
J. Luis Correa, California
Xochitl Torres Small, New Mexico
Max Rose, New York
Lauren Underwood, Illinois
Elissa Slotkin, Michigan
Emanuel Cleaver, Missouri
Al Green, Texas
Yvette D. Clarke, New York
Dina Titus, Nevada
Bonnie Watson Coleman, New Jersey
Nanette Diaz Barragán, California
Val Butler Demings, Florida

Mike Rogers, Alabama
Peter T. King, New York
Michael T. McCaul, Texas
John Katko, New York
John Ratcliffe, Texas
Mark Walker, North Carolina
Clay Higgins, Louisiana
Debbie Lesko, Arizona
Mark Green, Tennessee
Van Taylor, Texas
John Joyce, Pennsylvania
Dan Crenshaw, Texas
Michael Guest, Mississippi

Hope Goins, *Staff Director*
Chris Vieson, *Minority Staff Director*

# CONTENTS

Page

STATEMENTS

WITNESSES

PANEL I

PANEL II

FOR THE RECORD

APPENDIX

# DEFENDING OUR DEMOCRACY: BUILDING PARTNERSHIPS TO PROTECT AMERICA'S ELECTIONS

---

**Wednesday, February 13, 2019**

U.S. House of Representatives,
Committee on Homeland Security,
*Washington, DC.*

The committee met, pursuant to notice, at 10:03 a.m., in room 310, Cannon House Office Building, Hon. Bennie G. Thompson (Chairman of the committee) presiding.

Present: Representatives Thompson, Jackson Lee, Langevin, Payne, Rice, Correa, Torres Small, Rose, Underwood, Slotkin, Cleaver, Green of Texas, Clarke, Titus, Watson Coleman, Barragán, Demings, Rogers, King, Katko, Ratcliffe, Walker, Higgins, Lesko, Green of Tennessee, Taylor, Joyce, Crenshaw, and Guest.

Chairman Thompson. The Committee on Homeland Security will come to order. I welcome the Members to the first hearing of the Committee on Homeland Security of the 116th Congress. I appreciate your flexibility and that of our witnesses after we rescheduled the hearing due to the services of late Chairman John Dingell. Our thoughts and prayers are with his wife.

Today the committee will hold a hearing on defending our democracy, building partnerships to protect America's elections. Election security is a National security issue and it must transcend party politics because it requires a unified effort to protect America's elections. Unfortunately, this hearing is long overdue. During the 115th Congress, the Republican Majority spent much of its time ignoring the intelligence and refusing to acknowledge the threat to our democracy.

Frustrated by the lack of action on this critical issue, Democrats on this committee and the Committee on House Administration launched the Congressional Task Force on Election Security in July 2017. The task force met with dozens of elections experts, secretaries of State elections, and National security experts to assess vulnerabilities in election infrastructure and determine how to address them.

In February 2018, the task force produced a report that included 10 recommendations and introduced legislation to implement them. That legislation is now part of H.R. 1, the For the People Act, which the House is expected to consider in the coming weeks.

Fortunately, since 2016, progress has been made toward more secure elections. The Department of Homeland Security and Election

Assistance Commission have built stronger, more effective partnerships with State and local election officials. But it is unclear whether each agency has the resources necessary to meet the increasing demand for their resources.

Will EAC's $10 million budget provide sufficient resources for it to administer additional election security grants to States? Does DHS have the resources to provide its services to every State and county that requests them?

Congress needs to understand the existing capability of each agency. Now, existing capabilities can be leveraged, grown, and augmented. Local election officials are on the front lines of securing our elections, and their success depends on the support they receive from Federal and State governments.

Although some dispute that has—the election infrastructure local election officials oversee is vulnerable to hacking, cybersecurity experts have made a credible case. The Federal Government, especially Congress, must understand the resource constraints of local election officials and partner with them to address vulnerabilities to election infrastructure through grants and services.

The intelligence community has made clear the threats to our elections persist, so more work remains to be done. Just last month, Director of National Intelligence Dan Coats, warned, Russia in 2016 and unidentified actors as recently as 2018 have already conducted cyber activity that has targeted U.S. election infrastructure.

He went on to say, we should expect adversaries and strategic competitors to refine their capabilities and add new tactics as they learn from each other's experiences in advance of the 2020 elections.

I look forward to hearing from our panel of witnesses today about how Congress and Federal agencies can support efforts to further strengthen our elections and protect them from attack.

I welcome our Republican colleagues' support in these efforts and I look forward to working with all those whose goal is to protect America's elections and defend our democracy.

[The statement of Chairman Thompson follows:]

### Statement of Chairman Bennie G. Thompson

February 13, 2019

Election security is a National security issue that must transcend party politics, because it requires a unified effort to protect America's elections. Unfortunately, this hearing is long overdue. During the 115th Congress, the Republican Majority spent much of its time ignoring the intelligence and refusing to acknowledge the threat to our democracy.

Frustrated by the lack of action on this critical issue, Democrats on this committee and the Committee on House Administration launched the Congressional Task Force on Election Security in July 2017. The Task Force met with dozens of elections experts, State election officials, and National security experts to assess vulnerabilities in election infrastructure and determine how to address them. In February 2018, the Task Force produced a report that included 10 recommendations and introduced legislation to implement them.

That legislation is now part of H.R. 1, the For the People Act, which the House is expected to consider in the coming weeks. Fortunately, since 2016, progress has been made toward more secure elections.

The Department of Homeland Security and Election Assistance Commission (EAC) have built stronger, more effective partnerships with State and local election officials. But it is unclear whether either agency has the resources necessary to meet the increasing demand for their resources.

Will EAC's $10 million budget provide sufficient resources for it to administer additional election security grants to States? Does DHS have the resources to provide its services to every State and county that requests them?

Congress needs to understand the existing capability of each agency and how existing capabilities can be leveraged, grown, and augmented. Local election officials are on the front lines of securing our elections, and their success depends on the support they receive from Federal and State governments.

Although some dispute that the election infrastructure local election officials oversee is vulnerable to hacking, cybersecurity experts have made a credible case it is. The Federal Government—especially Congress—must understand the resource constraints of local election officials and partner with them to address vulnerabilities to election infrastructure though grants and services.

The intelligence community has made clear the threats to our elections persist, so more work remains to be done. Just last month, Director of National Intelligence Dan Coats warned, "Russia in 2016 and unidentified actors as recently as 2018 have already conducted cyber activity that has targeted U.S. election infrastructure." He went on to say we should expect "adversaries and strategic competitors to refine their capabilities and add new tactics as they learn from each other's experiences" in advance of the 2020 elections.

I look forward to hearing from our panel of witnesses today about how Congress and Federal agencies can support efforts to further strengthen our elections and protect them from attack. I welcome my Republican colleagues' support in these efforts, and I look forward to working with all those whose goal is to protect America's elections and defend our democracy.

Chairman THOMPSON. I now recognize the Ranking Member of the full committee, the gentleman from Alabama, Mr. Rogers, for an opening statement.

Mr. ROGERS. Thank you, Mr. Chairman.

I look forward to the opportunity to hear from our witnesses today regarding election security. The integrity of our elections is foundational to our democracy. All Americans should have confidence that voting equipment and systems are secure and your vote counts as they intended and that election results are accurately reported.

Last week DHS and DOJ released their findings that there was no evidence of any foreign interference in the 2018 election. I believe that the tremendous work done by DHS, our intelligence community and State and local leaders made that happen but there is certainly more work that can be done.

Much of our focus today will be on the work we still need to do to secure the technology and systems behind our elections but we can't lose sight of a simple lesson: Foreign intelligence services, domestic partisans, and on-line vandals do not care what our laws say. They are happy to use our public forums against us. My home State saw liberal activists deliberately mislead Alabamians regarding public endorsements and political issues in the 2017 U.S. Senate Special Election.

They bragged to liberal donors behind closed doors about their success in manipulating Alabama voters. H.R. 1 attempts to address these pressing issues but the bill's provisions are deeply naive. As it stands, H.R. 1 is an exercise in regulating everything that moves near a ballot box. The problems facing our election systems are more complex than that. Election security has long been a bipartisan priority for Members of this committee. It is my hope that this bipartisan tradition on this issue will continue in this Congress.

We need a deliberative, bipartisan process to solve these issues. Unfortunately it appears our committee will not have an opportunity to mark up the election security provisions in our jurisdiction. That is unfortunate because the election security provisions in this bill could be improved and I know Members on both sides of this committee have some good ideas on how to make those improvements. As it stands now, much of H.R. 1's 570 pages appear to be a political exercise.

That is why I am very disappointed that election security, an issue where we have an opportunity to work together to move bipartisan legislation has gotten caught up—getting caught up in a partisan political grab.

I hope that H.R. 1—when H.R. 1 stalls in the Senate, as it will, we will revisit the issue of election security in a bipartisan manner. I thank our witnesses for taking the time to speak to our committee about the work you are doing on the front lines of elections.

I yield back, Mr. Chairman.

[The statement of Ranking Member Rogers follows:]

STATEMENT OF RANKING MEMBER MIKE ROGERS

I look forward to the opportunity to hear from our witnesses today regarding election security. The integrity of our elections is foundational to our democracy.

All Americans should have confidence that voting equipment and systems are secure, their vote counts as they intended, and that election results are accurately reported.

Last week, DHS and DOJ released their findings that there was no evidence of any foreign interference in the 2018 election. I believe the tremendous work done by DHS, our intelligence community, and State and local leaders made that happen. But there is certainly more work to be done.

Much of our focus today will be on the work we still need to do to secure the technology and systems behind our elections. But we can't lose sight of a simple lesson: Foreign intelligence services, domestic partisans, and on-line vandals do not care what our laws say. They are happy to use our public forums against us.

My home State saw liberal activists deliberately mislead Alabamians regarding public endorsements and political issues in the 2017 U.S. Senate special election. They bragged to liberal donors behind closed doors about their success in manipulating Alabama voters.

H.R. 1 attempts to address these pressing issues, but the bill's provisions are deeply naive. As it stands, H.R. 1 is an exercise in regulating everything that moves near a ballot box.

The problems facing our election system are more complex than that. Election security has long been a bipartisan priority for Members of this committee.

It is my hope that this bipartisan tradition on this issue will continue in this Congress. We need a deliberative, bipartisan process to solve these issues.

Unfortunately, it appears our committee will not have an opportunity to mark up the election security provisions in our jurisdiction. That is unfortunate because the election security provisions of this bill could be improved.

And I know Members on both sides of this committee have some good ideas on how make improvements. As it stands, much of H.R. 1's 570 pages appear to be a political exercise.

That is why I am very disappointed that election security, an issue where we had an opportunity to work together to move bipartisan legislation, has gotten caught up in this partisan political power grab.

I hope when H.R. 1 does not advance in the Senate, we can revisit the issue of election security in a bipartisan manner.

I thank our witnesses for taking to the time to speak to our committee about the work you are doing on the front lines of elections.

Chairman THOMPSON. I thank the gentleman for his comments.

Other Members of the committee are reminded that under the committee rules opening statements may be submitted for the record.

[The statement of Hon. Jackson Lee follows:]

## Statement of Honorable Sheila Jackson Lee

Chairman Bennie G. Thompson thank you for holding today's hearing so that the committee may learn more about how the Department of Homeland Security is "Defending Our Democracy: Building Partnerships to Protect America's Elections."

At the outset, let me congratulate you Mr. Chairman on your election to lead this august committee, and Mr. Rogers on his election as Ranking Member.

Chairman Thompson, your participation in the House Administration Committee's Subcommittee on Elections Field Hearing held in Brownsville, Texas last week was substantive and impactful.

Also, your skillful leadership in co-chairing the 115th Congress' Task Force on Election Security, which resulted in a report last year which informs our hearing this morning.

I look forward to continuing working with the returning Members of the committee and welcome an outstanding cohort of new Members on both sides of the aisle, who I trust will find the important work advanced by this committee as fulfilling and rewarding as I have since joining its inception.

I thank today's witnesses:

*Panel 1*

- The Hon. Christopher C. Krebs, director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security; and
- The Hon. Thomas Hicks, chairman, Election Assistance Commission.

*Panel 2*

- The Hon. Alex Padilla, secretary of state, California;
- Mr. Noah Praetz, former director of elections, Cook County, Illinois;
- Mr. Jake Braun, executive director, Cyber Policy Initiative, University of Chicago; and
- The Hon. John Merrill, secretary of state, Alabama (Minority witness).

I thank each of today's witnesses for bringing their expert view on the partnerships among Federal, State, and local agencies responsible for ensuring the integrity of elections have matured since 2016 and about the resources and support necessary to prepare for the 2020 Presidential elections.

The efforts to ensure that every eligible person can register to vote, and cast a vote in a public election have spanned generations.

I have been persistent in my efforts to protect the rights of disenfranchised communities in my district of inner-city Houston and across the Nation.

Throughout my tenure in Congress, I have cosponsored dozens of bills, amendments, and resolutions seeking to improve voters' rights at all stages and levels of the election process.

This includes legislation aimed at:

1. Increasing voter outreach and turnout;
2. Ensuring both early and same-day registration;
3. Standardizing physical and language accessibility at polling places;
4. Expanding early voting periods;
5. Decreasing voter wait times;
6. Guaranteeing absentee ballots, especially for displaced citizens;
7. Modernizing voting technologies and strengthening our voter record systems;
8. Establishing the Federal Election Day as a National holiday; and
9. Condemning and criminalizing deceptive practices, voter intimidation, and other suppression tactics.

Along with many of my colleagues in the CBC, I was an original cosponsor of H.R. 9, the Fannie Lou Hamer, Rosa Parks, and Coretta Scott King Voting Rights Act Reauthorization and Amendments Act, which became public law on July 27, 2006.

I also authored H.R. 745 in the 110th Congress, which added the legendary Barbara Jordan to the list of civil rights trailblazers whose names honor the Voting Rights Act Reauthorization and Amendments Act.

This bill strengthened the original Voting Rights Act by replacing Federal voting examiners with Federal voting observers—a significant distinction that made it easier to safeguard against racially-biased voter suppression tactics.

In the 114th Congress, I introduced H.R. 75, the Coretta Scott King Mid-Decade Redistricting Prohibition Act of 2015, which would prohibit States whose Congressional districts have been redistricted after a decennial census from redrawing their district lines until the next census.

The voting rights struggles of the 20th Century are now joined by voting rights threats posed by the 21st Century.

Russia an adversary of the United States engaged in repeated attempts to interfere in the 2016 Presidential election, which prompted an unprecedented all-of-Government effort to alert local and State election administrators to be aware of the threat.

Russia targeted our Presidential election according to the report, "Background to Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution," provided by the Office of the Director of National Intelligence's National Intelligence Council.

Russia used every cyber espionage tool available to influence the outcome of the Presidential election by using a multifaceted campaign that included theft of data; strategically-timed release of stolen information; production of fake news; and manipulation of facts to avoid blame.

The Russian General Staff Main Intelligence Directorate (GRU) is suspected by our intelligence agencies of having begun cyber operations targeting the United States election as early as March 2016.

They took on the persona of "Guccifer 2.0," "DCLeaks.com," and Wikileaks as the identities that would be reported as having involvement in the work they had under taken to undermine our Nation's Presidential election.

Russia is blamed for breaching 21 local and State election systems, which they studied extensively.

In February 2018, special counsel Robert Mueller released indictments of 13 Russians, at least one of whom has direct ties to Russian President Vladimir Putin.

The 37-page indictment details the actions taken to interfere with the U.S. political system, including the 2016 U.S. Presidential election.

Among the charges, which include charges for obstruction of justice, are several especially notable details.

The indictment states that 13 defendants posed as U.S. persons and created false U.S. personas and operated social media pages and groups designed to attract U.S. audiences.

The social media profiles "addressed divisive U.S. political and social issues" and falsely claimed to be controlled by U.S. activists.

The defendants are also accused of using "the stolen identities of real U.S. persons to post on social media accounts" which, over time, became the chosen "means to reach significant numbers of Americans for purposes of interfering with the U.S. political system, including the Presidential election of 2016."

The goal of the effort was to sow discord in the U.S. political system, including the 2016 US. Presidential election.

The internet does not sleep—and nor do our Nation's on-line adversaries.

That Russia used cyber intrusions to attack United States political institutions to collect data to manipulate the media and the public with the purpose of influencing the outcome of the 2016 Presidential elections is now an undisputed fact.

The United States has enemies in other corners of the globe who would not hesitate to attack our election system if given the chance.

These foreign adversaries do not share our commitment to democracy, liberty, and human rights, or the precious freedoms we hold dear.

On January 6, 2017, Homeland Security Secretary Johnson, as one of his last official acts under the Obama administration, designated election systems as critical infrastructure, and created a new subsector under the existing Government Facilities Sector designation.

On that same day, President Elect-Trump was briefed by the intelligence community that Vladimir Putin had directed the cyber attack on the United States of America.

Since then, intelligence officials have continued to warn that foreign governments—including Russia, Iran, and China—could attempt to interfere in U.S. elections.

In March 2017, then-Federal Bureau of Investigation (FBI) Director James Comey testified before the House Permanent Select Committee on Intelligence that the Russians are not finished and that they will be back.

In February 2018, six intelligence agency chiefs issued a dire warning about the Kremlin's on-going efforts to influence the U.S. elections.

On January 29, 2019, the director of national intelligence testified before the Senate Select Committee on Intelligence that our adversaries "probably already are looking to the 2020 U.S. elections as an opportunity to advance their interests."

The House Committee on Homeland Security has the responsibility of providing for the cybersecurity of Federal civilian agencies as well as the security of the Nation's 16 critical infrastructure sectors from cyber and other threats.

The Election Infrastructure Subsector covers a wide range of physical and electronic assets such as storage facilities, polling places, and centralized vote tabulation locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of State and local governments.

The work to secure our Nation's election system from cyber threats is on-going, which is why this hearing is relevant.

I look forward to the committee's markup of H.R. 1, the "For The People Act," critical legislation to repair and strengthen our democracy.

While this bill's language brings much-needed improvements to election administration by providing a funding stream to support the replacement of outdated voting systems, and support for the administration of Federal elections there is still more that must be done.

Specifically, that we should be mindful of the provision of voting systems for in-person voting and allow for sufficient machines to serve the population that will cast ballots at each polling location during early voting and on election day.

The U.S. Department of Homeland Security's (DHS) mission in cybersecurity and infrastructure protection is focused on enhancing greater collaboration on cybersecurity across the 16 critical infrastructure sectors and the sharing of cyber threat information between the private sector and Federal, State, and local partners.

This committee will work hand-and-glove with the House Judiciary and House Administration Committees as well as the Senate Committees to ensure that the tools applied to the current threat to our elections is effectively and adequately addressed.

We know the threats that computing devices and systems face, which are almost too numerous to count:

- Bot-nets;
- Ransom-ware;
- Zero Day Events;
- Mal-ware;
- Denial-of-Service Attacks;
- Distributed Denial-of-Service Attacks;
- Pharming;
- Phishing;
- Data Theft;
- Data Breaches;
- SQL Injection;
- Man-in-the-middle attack.

The list goes on, but suffice it to say that as hard as one person in our Government is working to stop cyber attacks there are likely another thousand attempting to breach a system or device owned by a United States citizen.

During the 2016 election we learned of new threats from cyber space that go far beyond any that would have been considered in previous elections.

This Congress is poised to do the hard work of delving into the issue of Russian involvement in our national election and providing solutions.

The work today must focus on election recovery should a serious cyber incident occur during an election.

Vulnerabilities of computing systems are not limited to intentional attacks, but can include acts of nature, human error, or technology failing to perform as intended.

I am particularly concerned that so many jurisdictions rely on electronic poll books, to check-in voters before issuing them ballots, with no paper back-ups.

Finally, the use of untrustworthy paperless electronic voting machines without sufficient paper ballot options will come to an end when H.R. 1 becomes law.

The right and better approach to election cybersecurity is to be prepared and not need options for voters to cast ballots should voting systems fail, rather than being unprepared and needing options for voters to cast ballots during an election that are not available.

We must be steadfast in our resolve to have a strong shield to defend civilian and critical infrastructure networks for all threats foreign and domestic.

I look forward to the testimony of today's witnesses.

Thank you.

Chairman THOMPSON. I would like to extend a welcome to our first panel of witnesses. First I would like to welcome Chris Krebs, the director of DHS's Cybersecurity and Infrastructure Security

Agency back to testify before this panel. Director Krebs has been at the helm of DHS's cybersecurity activities since 2017 and he has been an integral player in shaping and developing the Department's election security capabilities.

Next I am pleased to welcome Mr. Tom Hicks, the current chairman of the U.S. Election Assistance Commission, and also congratulate him on swearing in a new batch of election assistance commissioners.

We had the opportunity to hear from the chairman in 2017, when he came to speak before the Congressional Task Force on Election Security. I look forward to hearing about his work since that time. Without objection, the witnesses' full statements will be inserted in the record. I now ask each witness to summarize his statement for 5 minutes, beginning with Mr. Krebs.

## STATEMENT OF CHRISTOPHER C. KREBS, DIRECTOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. KREBS. Thank you. Chairman Thompson, Ranking Member Rogers, and Members of the committee. Good morning and thank you for the opportunity to testify regarding the Department of Homeland Security's efforts to secure the vote. First, however, I would like to, once again, thank this committee for its leadership in establishing the Cybersecurity and Infrastructure Security Agency, or CISA.

By creating our new agency and law, Congress formally recognized DHS's role as the leader of the National effort to safeguard Federal networks and critical infrastructure from cyber and physical threats. On behalf of the agency, once again, thank you. This morning, I want to update this committee on the progress made over the last 2 years working with the election community.

CISA's election security mission is clear, to support the efforts of election officials and their private-sector partners consistent with the Constitution, existing law, and electoral tradition. Since 2016 we have learned quite a bit through partners like the Election Assistance Commission, and thousands of election officials across the country, like you will hear in the next panel, that know elections.

They know their systems. They know what they need to conduct a successful election. Over the last 2 years, in focused, oftentimes humbling engagements, we have become partners with the election community. For the 2018 election, we worked with all 50 States, over 1,400 local and territorial election offices, 6 election associations, and 12 election vendors.

Our approach is threefold: Making sure the community has—the election community has the information they need to defend their systems, making sure the election community has the technical support and tools they need to defend their systems, and building enduring partnering—partnerships to enhance resilience, and advance security efforts together.

In 2018 we focused on building scalable, repeatable mechanisms to dramatically grow our information-sharing capabilities. The Elections Infrastructure Information Sharing and Analysis Center, or EI–ISAC was established. By Election Day, EI–ISAC had over

1,400 members, the fastest-growing ISAC of any critical infrastructure sector.

We share contextualized threat information and actionable—threat intelligence and actionable information that was enriched through our close partnership with the intelligence community and law enforcement.

More importantly, State and local election officials were sharing what they were seeing on their own networks. We also deployed intrusion detection capabilities, or Albert Sensors, to provide real-time detection capabilities on election networks.

As of Election Day in 2018, these sensors offered protections to election infrastructure and voter registration databases for more than 90 percent of registered voters. For reference, during the 2000 election, we were below 30 percent of coverage.

Second, we provide technical support and services to election officials and vendors. Initially, we offered our standard services, including cyber hygiene, scans, and risk invulnerability assessments that we offer Federal agencies and other infrastructure sectors.

As we refined our understanding of election officials' requirements, we shifted to capabilities that are quicker, less intrusive, and can scale to more jurisdictions. This scalability is critical because while our initial efforts in 2016 were primarily targeted in State—State election officials, we recognize the need to increase our support to counties and municipalities who operate elections as well.

Our Last Mile Initiative sought to provide information customized to the local county level. This initiative provided no-cost tailored information on cyber safeguards, threats and risks, and a checklist of cybersecurity action items.

The final area of focus has been building enduring partnerships toward a collective defense. While it may seem mundane, governance, communications, coordination, training, and planning are the critical foundational elements of our Nation's efforts to secure our elections.

These efforts, and others, contributed to a secure 2018 election. The Department of Homeland Security and the Department of Justice recently concluded there is no evidence that any identified activities of a foreign government or a foreign agent had a material impact on the integrity or security of election infrastructure or political campaign infrastructure used in the 2018 midterm elections.

While 2018 is behind us, the 2020 election season is already under way. We are clear-eyed that the threat to our democratic institutions remain, and we must continue to press for increased security and resilience of our election systems. Over the next 2 years, CISA will focus on expanding engagement to the local level.

We will continue to work with election officials to improve both, there and our understanding of risk. With that better understanding of risk, we can support efforts by election officials and Congress to obtain the resources they need to secure their election systems. Once again, thank you for the opportunity to appear before the committee today. I look forward to your questions.

[The prepared statement of Mr. Krebs follows:]

## PREPARED STATEMENT OF CHRISTOPHER C. KREBS

FEBRUARY 13, 2019

Chairman Thompson, Ranking Member Rogers, and Members of the committee, thank you for the opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) progress in reducing and mitigating risks to our Nation's election infrastructure. DHS has worked to establish trust-based partnerships with State and local officials who administer our elections, and I look forward to sharing with you an update on our work during the 2018 midterm election cycle.

Leading up to the 2018 midterms, DHS worked hand-in-hand with Federal partners, State and local election officials, and private-sector vendors to provide them with information and capabilities to enable them to better defend their infrastructure. This partnership led to a successful model that we aim to continue and improve upon in the 2020 election cycle.

Since 2016, DHS's Cybersecurity and Infrastructure Security Agency (CISA) has led a voluntary partnership of Federal Government and election officials who regularly share cybersecurity risk information. CISA has engaged directly with election officials—coordinating requests for assistance, risk mitigation, information sharing, and incident response. To ensure a coordinated approach, CISA convened stakeholders from across the Federal Government through the Election Task Force.

The Department and the Election Assistance Commission (EAC) have convened Federal Government and election officials regularly to share cybersecurity risk information and to determine an effective means of assistance. Since 2016, the Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) has worked to establish goals and objectives, to develop plans for the EIS partnership, and to lay the groundwork for developing an EIS Sector-Specific Plan. Participation in the council is voluntary and does not change the fundamental role of State and local jurisdictions in overseeing elections.

DHS and the EAC have also worked with election vendors to launch an industry-led Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed council with leadership designated by sector membership. The SCC serves as the industry's principal entity for coordinating with the Federal Government on critical infrastructure security activities related to sector-specific strategies. This collaboration is conducted under DHS's authority to provide a forum in which Federal and private-sector entities can jointly engage in a broad spectrum of activities to coordinate critical infrastructure security and resilience efforts, which is used in each of the critical infrastructure sectors established under Presidential Policy Directive 21, Critical Infrastructure Security and Resilience. The SCC has helped DHS further its understanding of the systems, processes, and relationships particular to operation of the EIS.

Within the context of today's hearing, I will address our efforts in 2018 to help enhance the security of elections that are administered by jurisdictions around the country, along with our election-related priorities through 2020. While there was activity targeting our election infrastructure leading up to the midterms, this activity is similar to what we have seen previously and occurs on the internet every day. This activity has not been attributed to nation-state actors and along with the Department of Justice (DOJ), we concluded that there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political or campaign infrastructure used in the 2018 midterm elections.

### ASSESSING THE THREAT

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

In addition to working directly with State and local officials over the past 2 years, we have partnered with trusted third parties to analyze relevant cyber data, including the Elections Infrastructure Information Sharing and Analysis Center (EI–ISAC), the National Association of Secretaries of State, and the National Association of State Election Directors. DHS field personnel deployed around the country furthered information sharing and enhanced outreach.

## ENHANCING SECURITY

During the 2018 midterms, CISA provided a coordinated response from DHS and its Federal partners to plan for, prepare for, and mitigate risk to election infrastructure. Working with election infrastructure stakeholders was essential to ensuring a more secure election. CISA and our stakeholders increased awareness of potential vulnerabilities and provided capabilities to enhance the security of U.S. election infrastructure as well as that of our democratic allies.

Election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections. In partnering with these officials through both new and on-going engagements, CISA will continue to work to provide value-added—yet voluntary—services to support their efforts to secure elections in the 2020 election cycle.

## IMPROVING COORDINATION WITH STATE, LOCAL, TRIBAL, TERRITORIAL, AND PRIVATE-SECTOR PARTNERS

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

CISA works with the EI–ISAC to provide threat and vulnerability information to State and local officials. Through funding by CISA, the Center for Internet Security created and continues to operate the EI–ISAC. The EI–ISAC has representatives co-located with CISA's National Cybersecurity and Communications Integration Center (NCCIC) to enable regular collaboration and access to information and services for election officials.

## PROVIDING TECHNICAL ASSISTANCE AND SHARING INFORMATION

Knowing what to do when a security incident happens—whether physical or cyber—before it happens is critical. CISA supports election officials with incident response planning including participating in exercises and reviewing incident response playbooks. Crisis communications is a core component of these efforts, ensuring officials are able to communicate transparently and authoritatively when an incident unfolds. In some cases, we do this directly with State and local jurisdictions. In others, we partner with outside organizations. We recognize that securing our Nation's systems is a shared responsibility, and we are leveraging partnerships to advance that mission. CISA actively promotes a range of services including:

*Cyber hygiene service for internet-facing systems*.—Through this automated, remote scan, CISA provides a report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the internet, such as on-line voter registration systems, election night reporting systems, and other internet-connected election management systems.

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

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

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

*Classified information sharing.*—To most effectively share information with all of our partners—not just those with security clearances—DHS works with the intelligence community to rapidly declassify relevant intelligence or provide as much intelligence as possible at the lowest classification level possible. While DHS prioritizes declassifying information to the extent possible, DHS also provides Classified information to cleared stakeholders, as appropriate. DHS has been working with State chief election officials and additional election staff in each State to provide them with security clearances.

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

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

## ELECTION SECURITY EFFORTS LEADING UP TO THE 2018 MIDTERMS

In the weeks leading up to the 2018 midterm elections, DHS officials supported a high degree of preparedness Nation-wide. DHS provided free technical cybersecurity assistance, continuous information sharing, and expertise to election offices and campaigns. EI–ISAC threat alerts were shared with all 50 States, over 1,400 local and territorial election offices, 6 election associations, and 12 election vendors.

In August 2018, DHS hosted a “Tabletop the Vote” exercise, a 3-day, first-of-its-kind exercise to assist our Federal partners, State and local election officials, and private-sector vendors in identifying best practices and areas for improvement in cyber incident planning, preparedness, identification, response, and recovery. Through tabletop simulation of a realistic incident scenario, exercise participants discussed and explored potential impacts to voter confidence, voting operations, and the integrity of elections. Partners for this exercise included 44 States and the District of Columbia; EAC; Department of Defense, including the Office of the Secretary of Defense, U.S. Cyber Command, and the National Security Agency; DOJ; Federal Bureau of Investigation; Office of the Director of National Intelligence; and National Institute of Standards and Technology (NIST).

Through the “Last Mile Initiative,” DHS worked closely with State and local governments to outline critical cybersecurity actions that should be implemented at the county level. For political campaigns, DHS disseminated a cybersecurity best practices checklist to help candidates and their teams better secure their devices and systems.

On Election Day, DHS deployed field staff across the country to maintain situational awareness and connect election officials to appropriate incident response professionals, if needed. In many cases, these field staff were co-located with election officials in their own security operations centers. DHS also hosted the National Cybersecurity Situational Awareness Room, an on-line portal for State and local election officials and vendors that facilitates rapid sharing of information. It gives election officials virtual access to the 24/7 operational watch floor of the CISA NCCIC. This setup allowed DHS to monitor potential threats across multiple States at once and respond in a rapid fashion.

Our goal has been for the American people to enter the voting booth with the confidence that their vote counts and is counted correctly. I am proud to say that our efforts over the past 2 years have resulted in the most secure election in modern history.

## NO EVIDENCE OF ELECTION INTERFERENCE

The Secretary of Homeland Security and the Acting Attorney General have concluded that there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political or campaign infrastructure used in the 2018 midterm elections for the U.S. Congress. The activity we did see was consistent with what we shared in the weeks leading up to the election. Russia, and other foreign countries, including China and Iran, conducted influence activities and messaging campaigns targeted at the United States to promote their strategic interests.

ELECTION SECURITY EFFORTS MOVING FORWARD

Ensuring the security of our electoral process remains a vital National interest and one of our highest priorities at DHS. In the run-up to the 2020 election season, DHS will continue to prioritize elections by broadening the reach and depth of information sharing and assistance that we are providing to State and local election officials, and continuing to share information on threats and mitigation tactics.

DHS goals for the 2020 election cycle include improving the efficiency and effectiveness of election audits, continued incentivizing the patching of election systems, and working with the National Institute of Standards and Technology (NIST) and the States to develop cybersecurity profiles utilizing the NIST Cybersecurity Framework for Improving Critical Infrastructure. We will also continue to engage any political entity that wants our help. DHS offers these entities the same tools and resources that we offer to State and local election officials, including trainings, cyber hygiene support, information sharing, and other resources.

DHS has made tremendous strides and has been committed to working collaboratively with those on the front lines of administering our elections to secure election infrastructure from risks. Just last week, DHS officials provided updates to the secretaries of state, State election directors, and members of the GCC and SCC on the full package of election security resources that are available from the Federal Government, along with a roadmap on how to improve coordination across these entities. DHS also worked with our intelligence community partners to provide a Classified 1-day read-in for these individuals regarding the current threats facing our election infrastructure.

We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure. However, we recognize that there is a significant technology deficit across SLTT governments, and State and local election systems, in particular. It will take significant and continual investment to ensure that election systems across the Nation are upgraded and secure, with vulnerable systems retired. These efforts require a whole-of-Government approach. The President and this administration are committed to addressing these risks.

Our voting infrastructure is diverse, subject to local control, and has many checks and balances. As the threat environment evolves, DHS will continue to work with Federal agencies, State and local partners, and private-sector entities to enhance our understanding of the threat; and to make essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

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

Chairman THOMPSON. Thank you for your testimony. I now recognize Mr. Hicks to summarize his statement for 5 minutes.

## STATEMENT OF THOMAS HICKS, COMMISSIONER, U.S. ELECTION ASSISTANCE COMMISSION

Mr. HICKS. Good morning, Chairman Thompson and Ranking Member Rogers and Member of the committee. I am pleased to appear you today to offer testimony on the pressing issue of how to build partnerships to better protect American elections.

Today's hearing comes 3 months after the 2018 midterm elections. Early estimates indicate that a record number of eligible Americans cast their vote in November. I congratulate the Nation's election administrators and their teams for a job well done, inspiring work that the staff and I saw, first-hand, as we travel across the Nation in the weeks surrounding the election.

This work, coupled with improved lines of communications between Federal, State, and local officials and Federal agencies that serve them resulted in no indication of foreign attacks on our Nation's election infrastructure.

The EAC is the only Federal agency focused solely on elections. This focus is of great value to election administrators and the voters they serve. The commission's mission and other mandates established under the Help America Vote Act, HAVA, are as relevant today as at any time since the watershed bipartisan legislation was signed into law.

We commissioners and the EAC staff stand ready to roll up our sleeves to address the unique needs of those we serve. Just last week, two new commissioners, Benjamin Hovland and Ben Palmer—Donald Palmer were sworn in, joining Vice Chair McCormick and myself to make up a full slate of commissioners the agency has had in nearly a decade.

Today's hearing and many of the commission's own efforts focus on election security, which is only one key component of election administration. I have attached to my written statement, a diagram that demonstrates the many different competencies that require election administrator's awareness and attention, knowledge of election law and election technology, to vote tabulation and post-election audits.

Election officials must operate in each of these areas with no room for error. That is why the EAC works to provide its resources to each of our competencies. That is why we partner with other Federal agencies to leverage their subject-matter expertise.

Some of the EAC's Federal partners include DOD, DHS, Department of Justice, National Institute of Standards and Technology, and the United States Postal Service. This morning I will briefly address the EAC's work to help States secure their elections, including efforts to swiftly and responsibly distribute $380 million in newly appropriated HAVA to States and the on-going work to test and certify voting systems.

In the Consolidated Appropriations Act of 2018, Congress appropriated $380 million in HAVA to the States, in eligible territories for projects and programs to improve the administration of Federal elections. Within 3 months of the appropriation, the EAC received distributed requests for 100 percent of the funds from all 55 eligible jurisdictions and States.

One hundred percent of the funds were quickly distributed to eligible States and territories to draw down. The EAC staff is currently exam the—examining the Federal financial reports regarding how States spent funds last year, the recent Federal furlough has slightly delayed this process.

But from our early assessments, we believe that about 58 percent of the funds went toward shoring up election security and about 33 percent of the funds was used to purchase voting equipment.

After we complete our 2018 spending analysis, we will provide more specific details about the expenditures and the State's future plans for using HAVA funds. The distribution of HAVA funds is only one example of the EAC's work to strengthen election security. The EAC serves as a central partner with DHS in ensuring that—the success of our National security efforts.

DHS has stated that the election security for Government Coordinating Council, the GCC, was formed faster than any other similar critical infrastructure sector council today. The EAC took a needed early leadership role in working toward this accomplishment.

Building on that success, the EAC convened discussions between election system vendors and DHS for the formulation of the Sector Coordinating Council, the SCC. Both the SCC and the GCC were formulated before the 2018 election year, less than 1 year from the critical infrastructure designation by DHS.

In addition, ahead of the 2018 mid-term elections, the EAC focused on steps our commission could take to further serve election officials operating in a new threat environment.

On multiple occasions, the EAC brought together election officials, lawmakers, security experts, academics, and Government partners, for discussion and events to tackle this vital issue. While taking—talking about election security at forums is important, so is hands-on training.

The EAC staff was involved in the establishment of Harvard University's Belfer Center tabletop exercise, which have since been conducted across the country. In addition, since 2015, the EAC has presented its election official as I.T. manager, training to officials representing hundreds of elections jurisdictions across the country and we will increase our efforts following the 2016 election.

This training is available on-line through FVAP program, that many more election officials can easily access to complete these efforts. The EAC has also produced a video and supporting materials to help local election officials explain the many levels of election security for their jurisdictions.

The final area I will highlight today during my testimony is the EAC's testing and certification program. The EAC—the Help America Vote Act charges the EAC with administrating a Federal program for setting voluntary voting system guidelines and testing for vendors may choose to have EAC accredited and monitored labs test their voting systems against those guidelines for certification.

The guidelines contain requirements for security as well as other important components such as accessibility, usability, and interoperability. These components and functions of the same are deliberated and developed in public working groups under the direction of the EAC's Technical Guidelines Committee, which is chaired by the director and under secretary of commerce for standard and technology.

After development and approval by the TGDC, the voluntary guidelines are submitted to the EAC's executive director, provided for the EAC's Standards Board and Board of Advisors, published for public comment and presented to the EAC's commissioners for consideration and approval.

Last spring, the EAC conveyed its advisory boards to review and comment on the adoptions of the newest versions of the guidelines VVSG 2.0. Both boards recommended that the EAC adopt VVSG 2.0. Now that a quorum—I ask for 1 additional minute or 30 seconds.

[Laughter.]

Chairman THOMPSON. Granted.

Mr. HICKS. Thank you, sir.

Quorum has restored to the EAC. We anticipate that the VVSG 2.0 will soon be posted for public comment and we will hold public hearings on the proposed guidelines.

Members of the committee, the EAC's mission includes supporting election officials across the country as they administer Federal elections and the EAC is committed to that work, to always seeking better ways to do it. I welcome your feedback and I look forward to answering questions you may have.

[The prepared statement of Mr. Hicks follows:]

PREPARED STATEMENT OF THOMAS HICKS

FEBRUARY 12, 2019

Good morning Chairman Thompson, Ranking Member Rogers, and Members of the committee. I am pleased to appear before you today to offer testimony on the pressing issue of how to build partnerships to better protect American elections. As the 2020 Presidential Election approaches and jurisdictions across the Nation prepare to host a number of State and local elections in the months ahead, I assure you that supporting election officials in their work—including providing election security tools and resources—is one of the most important responsibilities of the U.S. Election Assistance Commission, better known as the EAC.

Today's hearing comes 3 months after the 2018 midterm election. Voter confidence in our election system is an issue the EAC often publicly addressed ahead of last year's election and it is intrinsically tied to the topics I will discuss today. With early estimates indicating that a record number of all eligible Americans participated in the 2018 midterms, it is important to recognize the incredible ingenuity and care that election officials and those with whom they work demonstrated ahead of the midterms and continue to exhibit today. It is this work that shores up the very foundation of our democracy and instills voter confidence. EAC Commissioners and the Commission's staff saw this first-hand in the weeks surrounding the midterm election as we traveled the Nation to observe everything from pre-election preparations to post-election audits. In 2018, the work of our Nation's election administrators and their teams, coupled with a dramatically improved line of communication between Federal, State, and local election officials and the Federal agencies that serve them, resulted in no indication of foreign attacks on our Nation's election infrastructure. I am proud of the role the EAC played in that coordinated effort.

The EAC is the only Federal agency that focuses solely on elections, and this focus is of great value to election administrators and the voters they serve. The EAC's mission and other mandates established under the Help America Vote Act (HAVA) are as relevant today as at any other time since that watershed, bipartisan legislation was signed into law. When HAVA passed HAVA in 2002, Congress set out to make sweeping and much-needed reforms to the Nation's voting process. Congress established the EAC to serve as the Federal leader in helping States carry out that vision, and the Commission has done so successfully. The EAC has helped election officials in each State and U.S. territory identify and implement legally-required changes to the way America votes. The Commission has a strong relationship with State and local election leaders and the voters they serve, which makes progress possible and remains of great value as lawmakers consider additional ways to support the administration of Federal elections.

We Commissioners and the exemplary EAC staff stand ready to roll up our sleeves to address the unique needs of those we serve. Just this week, two new EAC commissioners, Benjamin Hovland and Donald Palmer, were sworn in, joining Vice Chair Christy McCormick and me to make up the first full quorum of Commissioners the agency has had in nearly a decade. While the EAC has made great strides over the years, we always seek to do better and to do more.

Certainly one of the primary focuses of our efforts, election security is only one component of election administration. I have attached a diagram to this testimony that demonstrates the many different competencies that require election administrator awareness and attention. Election officials must operate in each of these areas, so the EAC works on each of them. Knowledge of election law, finance, accessibility standards, security considerations, election technology, public relations and human resources are all core on-going election official responsibilities. As officials prepare to administer an election, they must be experts on mail, street file maintenance, voter registration, military and overseas voting, local candidates and campaign finance laws, project management, polling places and real estate, advance voting, and logistics. On Election Day and beyond, election officials must also direct activities such as voting and tabulation, canvassing, auditing, administering recounts, and carrying out list maintenance. Many of these topics are covered in the

EAC's Election Administration and Voting Survey report to Congress, including the 2018 report that is under way now and will be delivered to you this summer.

It is worth noting that in addition to this work, the EAC provides voters with vital resources and assistance needed to register to vote and to cast ballots, and it includes administering the National clearinghouse of election administration information to continually equip our partners in Congress, State and local government, private industry, advocacy organizations, other Federal agencies, academia, and others in the elections industry with the information they require and rely on.

The EAC also works alongside Federal partners to leverage their subject-matter expertise to augment the EAC's whole-of-elections perspective with specialized products. The EAC works with these partners to produce EAC products, help other agencies better develop products for election stakeholders, and help our stakeholders understand and integrate these products into the context of their array of responsibilities. These partners include the Department of Defense, the Department of Justice, the Department of Homeland Security, the National Institute of Standards and Technology (NIST), and the United States Postal Service.

Today I will focus my remarks on election security, one of the most integral components of the EAC's work. The EAC has worked diligently to help States secure their elections, especially in months leading up to last year's election. The EAC expeditiously distributed newly-appropriated HAVA funds to the States, assisted our Federal partners in establishing and managing the critical infrastructure operational framework, continued to test and certify voting systems, and highlighted and distributed important best practices in election administration. This work yielded substantial benefits in 2018 and continues as we look ahead to 2020.

## DISTRIBUTING NEWLY-APPROPRIATED HAVA FUNDS

In the Consolidated Appropriations Act of 2018, Congress appropriated $380 million in HAVA funds to the States and eligible territories for projects and programs to improve the administration of Federal elections. Within 3 months of the appropriation, the EAC received disbursement requests for 100 percent of the funds from all 55 eligible States and territories, a remarkable percentage, and 100 percent of the funds were quickly made available for the eligible States and territories to draw down.

Less than 2 weeks after these new funds were signed into law by President Trump, the EAC issued Notice of Grant Award letters to each State. Within 3 weeks of the signing, Missouri became the first State to request its funds. In the subsequent 10 weeks, the EAC conducted a webcast public forum to explain how the funding would proceed, worked directly with the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED) to share information, conducted multiple webinars to further discuss how the funds may be used, consulted with members of the disability community to hear their views on use of the funds, and had frequent contact with each State in an effort to move the funds quickly.

The EAC website also provides access to a set of Frequently Asked Questions regarding the funds. The attached map, also on the EAC website *(www.eac.gov),* shows the amount of funds appropriated to each State. The EAC fulfilled its promise to get the funds to the States as quickly as possible, and the Commission continues to consult with States and territories regarding the proper use of the funds, which were disbursed after the States provided a short narrative describing plans for how the funds will be used.

The EAC has used the new HAVA funds not just as an opportunity to provide much-needed financial support to the States, but also as a mechanism to promote best-practice information sharing among election administrators. Details from the State plan documents have been shared with the entire election community and on the EAC website. It is essential that the States and territories have access to the wealth of ideas and innovative approaches contained in other States' individualized planned activities as they plan their own use of the funds. As we continue to work closely with the State and local leaders charged with spending these funds, the EAC's staff will continue to compile the information we receive so that the election community and others will have access to particulars of how the States and territories are expending their funds to further update and secure their election systems.

The EAC's staff is currently examining Federal Financial Reports regarding how States spent funds last year. The recent Federal furlough has slightly delayed this process, but from our early assessment, we believe that about 58 percent of funds spent went toward shoring up election security and about 33 percent were used to purchase voting equipment. After we complete our 2018 spending analysis, we will provide more specific details about those expenditures and about States' future plans for using new HAVA funds. I've attached to this testimony two charts detailing how States initially indicated they planned to spend funds and the percentage of total funds allotted for activities such as election security and updating election equipment.

## CRITICAL INFRASTRUCTURE ACTIVITIES

The distribution of HAVA funds is only one example of the EAC's work related to election security. The EAC has been serving as a central partner with the Department of Homeland Security (DHS) in ensuring the success of this National security effort well before the 2017 Critical Infrastructure designation by former Secretary Jeh Johnson. The DHS has stated that the election sector's Government Coordinating Council (GCC) was formed faster than any other similar critical infrastructure sector council to date. The EAC took an early leadership role in working toward this accomplishment, and we recognize it as an exemplary proof-point of how local, State, and Federal Governments can effectively work together toward the shared goal of protecting our Nation's election infrastructure.

Building on that success, the EAC also convened discussions between election system vendors and the DHS for the formation of the Sector Coordinating Council (SCC). Thanks to the swift establishment of the GCC and the well-established relationships between the EAC and election equipment vendors, work on the SCC began in the summer of 2017, and its official formation meeting took place before the end of last year. Both councils were functioning before the 2018 election year, less than 1 year from the Critical Infrastructure designation by the DHS.

The EAC Chair serves on the GCC Executive Committee, and all EAC Commissioners are chartered members of the GCC. Like many members of the GCC, the EAC is seeking security clearances through the DHS and has been assured that the Department will be addressing those security requests soon.

During the last Presidential Election cycle, the EAC was a key player in Federal efforts to share vital security information with the States and educate our Federal partners about ways to best serve the needs of election administrators. For example, the EAC:

- Distributed urgent security alerts and threat indicators from the DHS and the Federal Bureau of Investigation (FBI) to States and territories to help protect election systems from specific cybersecurity threats.
- Met on multiple occasions with staff from the DHS, the FBI, and the White House to discuss specific and nonspecific threats, State and local election system security and protocols, and the dynamics of the election system and its 8,000-plus jurisdictions Nation-wide.
- Served as the Federal Government's primary communication channel to provide real-time cybersecurity information to election officials around the country. This information included current data on cyber threats, tactics for protecting election systems against these threats, and the availability and value of DHS resources for protecting cyber assets.
- Participated in and convened conference calls with Federal officials, secretaries of state, and other State chief election officials, local election administration officials, Federal law enforcement, and Federal agency personnel to discuss the prospect of designating elections as part of the Nation's critical infrastructure. These discussions focused on topics such as coordinating security flashes from the FBI, the implications of a critical infrastructure designation, education on the Nation's election system, and the dynamics of successfully communicating information to every level of election officials responsible for running the Nation's election system.
- Provided DHS with perspective, information, and data related to the election system, introductions to officials in the election community, and information that assisted the agency with shaping communications in a manner that would be useful to the States and local election officials.
- Published a white paper entitled "U.S. Election Systems as Critical Infrastructure" that provided a basic understanding of critical infrastructure for election officials.
- Contributed to multiple foundational DHS documents used to structure the Elections Systems Critical Infrastructure designation and sector.

Ahead of the 2018 Midterm Election, the EAC focused on steps our commission could take to further serve election officials operating in the new threat environment. The EAC brought together election officials, security officials, academics, and Federal Government partners for an Election 2018 kick-off summit at the National Press Club in January 2018. Just 1 month ahead of the mid-term election in October 2018, we gathered a similar audience here in the Capitol Visitors Center for an election readiness summit that featured, among others, Senators Blunt and Klobuchar, as well as high-level officials from DHS and the National Counterintelligence and Security Center. These events and others like them throughout 2018 raised awareness of the security preparations election officials had under way and the resources available to the States and localities to help with this critical work.

While talking about election security at forums is important, the EAC also knows the importance of training. EAC staff was intricately involved in the establishment of Harvard University's Belfer Center Table-Top Exercises, which have since been conducted across the country. During the past year, the EAC has also developed and presented its "Election Official as IT Manager" training to officials representing hundreds of election jurisdictions across the country, and we are working with the DHS to put this training on-line through the FedVTE platform so that many more election officials can easily access it.

The EAC also produced a video and supporting meeting materials to help local election officials explain the many levels of election security at their jurisdiction. The video was designed to be viewed at civic group meetings and election worker trainings. It can also be customized by jurisdictions, and some States are tailoring the video to their voters and processes. We plan further work in this regard. In addition, the EAC Commissioners continuously meet with State and local election officials at regional conferences across the country. These visits allow the Commissioners to apprise officials of best practices, promote resources available from the EAC and our Federal partners in agencies such as the United States Postal Service, the Federal Voting Assistance Program (FVAP) within the Department of Defense, the Department of Justice, and the DHS, and discuss current concerns and topics in election administration, such as contingency planning, accessibility, voter registration, and technology management.

On Election Day 2018, we were pleased to have our newly-hired chief information officer and the head of our Testing and Certification Program on-site with other Federal agencies and key election stakeholders who gathered at the National Cybersecurity & Communications Integration Center (NCCIC). We are proud of the role we played last year, and we continue to seek new ways to provide election security support to State and local election leaders.

## TESTING AND CERTIFICATION/VOLUNTARY VOTING SYSTEM GUIDELINES

The Help America Vote Act charges the EAC with administering a Federal program for setting a voluntary National standard for testing and certificating voting systems. This testing standard is the EAC's Voluntary Voting System Guidelines (VVSG), and vendors may choose to have EAC-accredited and monitored labs test their voting systems against these guidelines for certification. The guidelines contain requirements for security, as well as other important components—such as accessibility, usability, and interoperability. In fact, while security is a guiding consideration of certification, so is accessibility for voters with disabilities and voters with limited English proficiency.

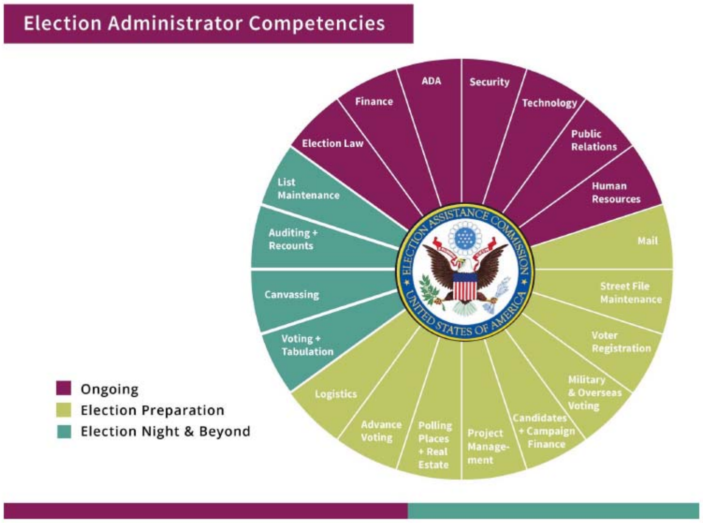
These considerations are deliberated and developed in public working groups under the direction of the EAC's Technical Guidelines Development Committee (TGDC), which is chaired by the director and under secretary of commerce for standards and technology. This TGDC's membership is made up of technical and scientific experts from fields such as security, accessibility, voting machine production, and voting machine use. After development and approval by the TGDC, the voluntary guidelines are submitted to the EAC's executive director, provided to the EAC's Standards Board and the Board of Advisors, published for public comment, and presented to the EAC's commissioners for consideration and approval. Last Spring, the EAC convened its advisory boards to review and comment on the adoption of the newest version of the voluntary guidelines, VVSG 2.0. Both boards recommended that the EAC adopt VVSG 2.0. Now that a quorum has been restored at the EAC, we anticipate that the VVSG 2.0 will soon be posted for public comment, we will hold public hearings on the proposed guidelines, and the agency has the pieces in place for final consideration.

While the EAC has been hard at work on the newest version of the VVSG, the EAC has not stopped its on-going work to rigorously review, test, and certify voting systems. These reviews are referred to as test campaigns, and in these campaigns EAC accredited laboratories test vendor-submitted voting systems against the standards contained in the VVSG. Once a system successfully completes a test campaign, the results of the campaign are transmitted to the EAC's executive director for certification of the voting system to the standard against which it was tested. If the EAC's executive director agrees that the voting system has conformed with the standard, it is certified as such and assigned a certification number. It takes the EAC approximately 8 to 12 months to certify a newly-submitted voting system. If the system has already been certified and the vendor is making an upgrade or revising a component, it may take as little as a few weeks or as much as 6 months to upgrade or change.

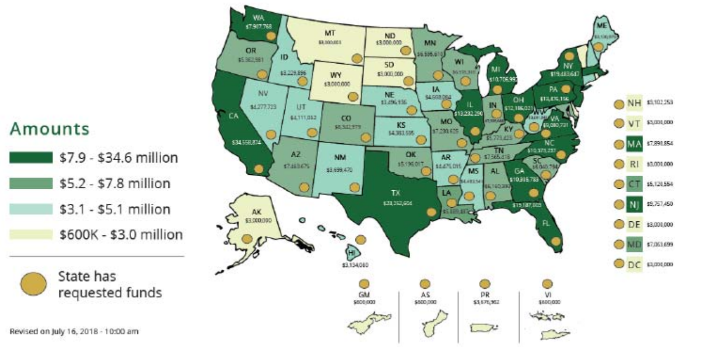
In addition to the actual certification of the voting systems, the EAC's Testing and Certification Program continually conducts quality monitoring of all EAC-certified systems and audits the quality of the EAC-accredited test labs. Monitoring of the voting systems occurs throughout the entire span of manufacturing and life of service, including manufacturing facility audits, field system review and testing, and field anomaly reporting from manufacturers and election officials.

CONCLUSION

Members of the committee, the EAC's mission includes supporting election officials across the country as they administer Federal elections, and we are committed to that work and to always seeking better ways to do it. The importance of election security and how the newly-appropriated HAVA Funds will assist States remain a primary focus and top priority for the commission. I am honored to support the important work carried out by our Nation's election administrators each and every day, and I congratulate them on a job well done in 2018. The EAC looks forward to working closely with them ahead of the 2020 Presidential Election. I welcome your feedback, and we look forward to answering questions you may have.

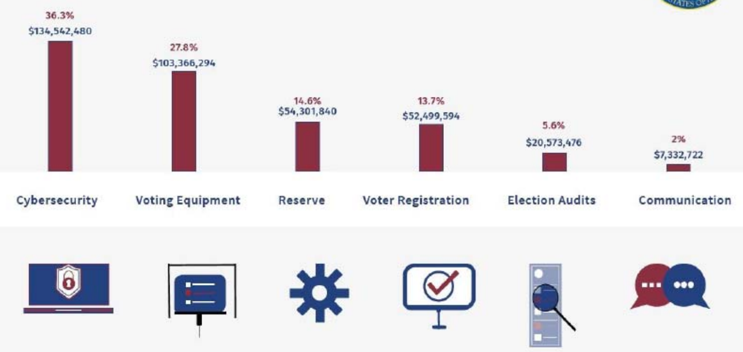


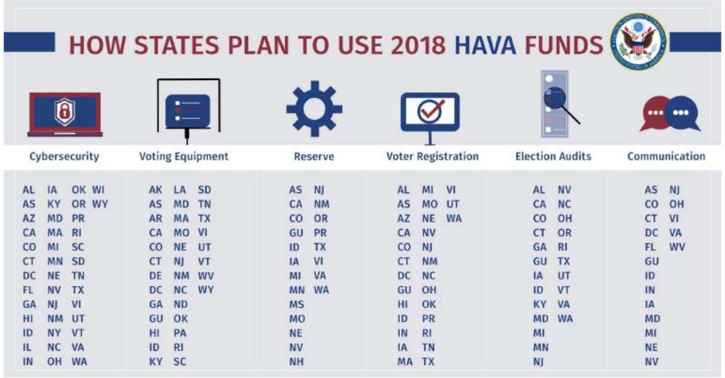
## 2018 HAVA Funds



Revised on July 16, 2018 - 10:00 am

## How States Plan To Use Their 2018 HAVA Funds





HOW STATES PLAN TO USE 2018 HAVA FUNDS

| Cybersecurity | Voting Equipment | Reserve | Voter Registration | Election Audits | Communication |
|---|---|---|---|---|---|
| AL IA OK WI | AK LA SD | AS NJ | AL MI VI | AL NV | AS NJ |
| AS KY OR WY | AS MD TN | CA NM | AS MO UT | CA NC | CO OH |
| AZ MD PR | AR MA TX | CO OR | AZ NE WA | CO OH | CT VI |
| CA MA RI | CA MO VI | GU PR | CA NV | CT OR | DC VA |
| CO MI SC | CO NE UT | ID TX | CO NJ | GA RI | FL WV |
| CT MN SD | CT NJ VT | IA VI | CT NM | GU TX | GU |
| DC NE TN | DE NM WV | MI VA | DC NC | IA UT | ID |
| FL NV TX | DC NC WY | MN WA | GU OH | ID VT | IN |
| GA NJ VI | GA ND | MS | HI OK | KY VA | IA |
| HI NM UT | GU OK | MO | ID PR | MD WA | MD |
| ID NY VT | HI PA | NE | IN RI | MI | MI |
| IL NC VA | ID RI | NV | IA TN | MN | NE |
| IN OH WA | KY SC | NH | MA TX | NJ | NV |

Chairman THOMPSON. Thank you very much. I thank the witnesses for their testimony. I remind each Member that he or she will have 5 minutes to question the panel. I now recognize myself for questions.

Director Krebs, given the 2019 World-wide Threat Assessment that warned that the U.S. adversaries and strategic competitors probably are already looking at the 2020 U.S. elections, how confident are you that our election infrastructure, as it is at this moment, is secure against cyber attacks?

Mr. KREBS. Chairman, thank you for the question. I certainly think that, just like any other I.T. system, the election infrastructure bears additional securing and resilience measures. But I will say that compared to where we were in 2016, not just from a fundamental I.T. security perspective, but from a collaboration working across the different stakeholder groups, we are light-years ahead of where we were. Most importantly, we have greater visibility both of the threats that are incoming, but also how they would work across the ecosystem and across the infrastructure.

I mentioned earlier, the Albert sensor coverage that we have, less than 30 percent in 2016, over 90 percent in 2018, that gives us near-real-time visibility in what is happening across the networks.

The last thing I will add here, the area that I think we need to invest the most as a Nation, is ensuring auditability across infrastructure. It is a key tenant of I.T. security. If you don't know what is happening and if you can't check back across the system, what is happening in the system, then you don't really have security. So, to the extent that we can focus on an outcome of auditability throughout the process end-to-end, that is the greatest area of need in my view.

Chairman THOMPSON. So, is that a matter of software or training or what?

Mr. KREBS. Yes, sir, everything. One area that we can focus on, and the good news is from my understanding and I would defer to Chairman Hicks, every State is—that is not already on a paper-type ballot, whether it is hand-marked or whatever—every State, including the 5 that are on electronic machines right now, are moving toward paper.

Paper helps that auditability process. Then you have after-election audits on the backend, but it is not just about the voting day, it is also all the way through the voter registration process, making sure that you have visibility and understanding of what is happening in those databases.

Chairman THOMPSON. Right. So, Mr. Hicks, are you concerned that so much of what we use is from international sources and the potential for supply chain compromise is there or has that issue come up in your review?

Mr. HICKS. It has come up in our reviews but I would like to say that it is difficult to function in a world economy and not have some form of components coming from overseas. I believe that that is being looked at but I believe that we can still move forward with a secure election process because the EAC certifies voting systems and that is all components within those systems for the voluntary voting system guidelines and standards and we certify the labs that do that as well. So I have very little concern in foreign components overall because I have great faith in our labs and the overall structure of our voluntary voting system guidelines to ensure that those systems are functioning the way that the American people want them to.

Chairman THOMPSON. Mr. Krebs do you want to comment on that?

Mr. KREBS. Yes, sir. So I mentioned in my opening remarks that we have three primary areas of focus for 2020. One is extending to locals but the second piece is better understanding the risk across the election infrastructure. As Chairman Hicks mentioned, supply chain concerns are certainly in that register of risk that we are looking at but I am actually at this point more concerned or focusing in on basic cyber hygiene practices.

When we looked across a range of sectors and segments what we saw was the election community still has challenges with basic cyber hygiene and so what our area of focus is helping with patching, helping implement multifactor authentication, helping on phishing campaign assessments, things of that nature.

Chairman THOMPSON. So before I run out of time, your testimony indicated that all the secretaries of state had participated in some aspect of your resources?

Mr. KREBS. Yes, sir. All 50 States have engaged with the Department in one way, shape or form. The election infrastructure ISAC for instance has all 50 States as members.

Chairman THOMPSON. Thank you, I yield to the——

Mr. HICKS. Congressman, there is one other aspect of that that I wanted to jump on, with—Under Secretary Krebs was speaking about, and one way to ensure that the systems are functioning the way that they are intended is through auditability. So once we move away from those 5 States that don't have paper trails associated with them, I believe that all States should be able to audit using some form of paper but also to ensure that we continue on with the Help America Vote Act of ensuring that those who have disabilities might not be able to use that paper can still vote independently and privately.

Chairman THOMPSON. Thank you. I yield to the Ranking Member for 5 minutes.

Mr. ROGERS. Thank you, Mr. Chairman. Commissioner Hicks in your opening statement you made reference to the fact that last spring the EAC had distributed $380 million in fiscal year 2018 funds to the States to improve their elections. To date, how many States and territories have been able to spend their allocation? I know you said 100 percent of it had been distributed but have they been able to spend it?

Mr. HICKS. All the States are spending that money now. They have up to 5 years to spend the money for—for additional things. It is basically an infrastructure grant. So if we look toward—and continuing on with infrastructure, it won't be built within 3 months but it would be carried on for the 5 years the Congress appropriated that money for.

Mr. ROGERS. You are just starting to spend it?

Mr. HICKS. Yes.

Mr. ROGERS. OK.

H.R. 1 authorizes, and this is also for Mr. Hicks, H.R. 1 authorizes—nearly $1.2 billion over the next 2 years to local election security improvements. Is it feasible for States to buy equipment, implement new security measures and poll workers, trained in time for the primaries 2 years from now?

Mr. HICKS. I missed part of your question, sir.

Mr. ROGERS. Given that $1.2 billion is to be spent, can the States take that money and buy equipment, train poll workers, and implement security measures in time for the primaries for the 2020 elections?

Mr. HICKS. I believe States can do most of that. But again we can't just—the States can't go to Best Buy and get that off the shelf so most of the States are moving toward not only purchasing new voting equipment but also other aspects of the election process in terms of voter registration, election audits, security overall so it is not just purchasing new voting equipment, they are going from registration to election night reporting.

Mr. ROGERS. My point is I just don't see how they are going to be able to get that done by the 2020 primaries and they are right—you are talking about next March is Alabama's primary; some of them are early as February or January of next year. Finally, you—for Mr. Hicks, you talked about certifying that the EAC certifies election security systems. Can you tell me more about that certification process?

Mr. HICKS. It is voting systems overall. So basically for voting systems, once the State decides they want to fall under that process of our voluntary voting system guidelines, those systems are sent by the vendors to those—to our test labs and then certified to those sorts of standards. It is the same as if computers or iPhones or other aspects of that, they are tested to a certain standard.

Mr. ROGERS. Can you have your staff to submit to my staff—for the full committee staff, what those standards are, certification standards? I would really be interested in reviewing those.

Mr. HICKS. Well there is several of them so we just certified 1.1 in 2015 but for the last 4 years since I have been at the commission, we have been working on the 2.0 voluntary voting system guidelines and there is a healthy debate going on right now between myself and the other commissioners when ensuring that those get out for public comment relatively soon.

Mr. ROGERS. Good. Mr. Krebs, can DHS and EAC complete supply chain security and other qualification mandates on vendors required by H.R. 1 fast enough for States to know that what they are buying is acceptable machines in time for the 2020 primaries?

Mr. KREBS. I am not sure. I have to think about the number of systems, the research, the requirements that would have to go into that. I may need to get back to you on the timeliness of that.

Mr. ROGERS. My final question is these 5 States that currently have audit concerns, you both made reference to the fact they are moving toward paper. Can you tell me more about what they are doing?

Mr. HICKS. So those States are purchasing—some States are already in line to purchase new voting equipment, like Georgia overall. But some States are putting bids out to other manufacturers to get some sort of paper. So it is basically little things like buying anything. There is different models out there and what works best for those States is what those States are going to purchase. But there are other aspects of voting systems that are out there—optical scan machines or just paper-based systems overall where States are looking toward getting those so that they can audit those at night—after election night and so forth.

Mr. ROGERS. Do you have a time line of when they expect to be able to get that auditability?

Mr. HICKS. It is an on-going thing. So the first purchase of voting equipment under the Help America Vote Act was more than 15 years ago and as I—when I say how much confidence folks have on computer systems that they purchase 15 years ago but the EAC gives guidance on maintaining aging voting equipment to ensure that those systems function the way they were designed to.

So I would say that it is an on-going process so it might not be, you know, fully completed in 2020. By 2022, 2024 as elections continue on, more systems will be mothballed.

Mr. ROGERS. Thank you. I yield back.

Chairman THOMPSON. Thank you. The Chair recognizes the gentlelady from New York, Ms. Rice.

Miss RICE. Thank you Mr. Chairman. Mr. Krebs, I would like to start with you if I could. I applaud the progress that you have made protecting the machinery of our elections but what I want to address now is another part of election protection, and that is protecting the campaigns and the political party committees from attack. Everyone is well aware of what happened in 2016. There was the hacking of the DNC, the DCCC, and the Clinton campaign, all hacked by Russia.

We know the subsequent use of the stolen materials have a profound effect on the election. We also know that in 2018 the NRCC was hacked, that being in the midterm cycle. Now I know that on our side the DCCC launched unprecedented cybersecurity and disinformation prevention operations. But all of that work was done by themselves. It was not done in coordination with any Federal agency—with the Federal Government at all even though these are Federal campaigns.

So I want to ask you, do you think that we should rethink how we are doing all this?

Mr. KREBS. Yes, ma'am. Thank you for the question. So during the 2018 cycle and even to today, we have worked with the major parties. RNC, we have conducted training—conducted training. DNC, we have a very good relationship with the CIO. We continue to work with the other committees so it is in our area of engagement. I take your point though that we need to expand and deepen and broaden that engagement. We continue to think about the various offerings that we have whether its capabilities, technical support information sharing, training, those are all the areas that we are continuing to push out.

I would encourage each of you, as you are coming up on another cycle, you know, please work with us, your own campaigns. We have capabilities that we can offer and it is definitely within our—it is an area of priority engagement for us going forward.

Miss RICE. So I am glad to hear you say that. I want to ask your opinion about whether you think using the Information Sharing Analysis Center, the ISAC model that you use for working with sectors like the energy and financial fields. Do you think that that would be of help here?

Mr. KREBS. In terms of political infrastructure and political campaigns?

Miss RICE. Yes.

Mr. KREBS. I don't have any reason to believe why it wouldn't work.

Miss RICE. I think that that is something that we have to look into because all of this is about sharing information when you are being hacked and what you do about getting down disinformation and all that kind of stuff. There were 3 States that did not use any part of the election assistance commission so this could be either to Mr. Hicks or to you, Mr. Krebs. Three States—Florida, Oklahoma, and Oregon chose not to use any part of the EAC's testing or certification program and they were all targeted by Russian hackers in 2016.

I guess my question is are we encouraging States to participate in the programs and I understand the tension between, you know, the State's rights over how their elections are run but there is—I guess I would ask you, do you think there is a role for the Federal Government to play and did the Government—Federal Government do enough to participate States—to encourage States to participate in the program before the 2018 cycle and how many States will be participating in this—in the 2020 cycle?

Mr. KREBS. So I wouldn't use 2016 as the baseline for how—what States engage, what local communities engage. I would instead recommend that we look at 2018. All 50 States worked with the Department of Homeland Security, and it is also important to keep laser-focused on what the Department's mission is; that is cybersecurity technical assistance. The election capabilities, that resides with the EAC and NIST and the others. We are very focused on cybersecurity capabilities. We had all 50 States, 1,400 jurisdictions, a number of election equipment vendors all playing ball with us.

The difference between 2018 and 2016 and I hope that you will hear this in the next panel was trust. In 2016 there was no relationship between the Department and EAC. There was no relationship between Secretary Padilla or Secretary Merrill. Right now, those relationships are strong and growing stronger. So I am very confident that going forward that we have the baseline of engagement and partnership in place to only continue to improve the security and resilience in the voting system.

Mr. HICKS. Thank you for the question, Congresswoman. There are two aspects that I would like to point out with—for two States that I went to last year. I went to Oregon and I did go to Florida as well. In Oregon I saw the wildfires that were going on and they were looking toward the EAC to get some sort of guidance in terms of overall aspects of running their elections. They're an all-paper State so they do everything by vote by mail. So they were—they were I think on top of things in terms of moving forward.

Florida, I had the honor of going down to visit with Bay County which was devastated by Hurricane Michael and to see their election folks basically in tears but being happy that the EAC was there to document their—their concerns and get others to see that and I hope that our staff will be able to have the videos that we took up relatively soon so folks can pay attention to that and not forget those folks as well.

I think that there are different aspects that the States have gone to, to use our services, so we do touch all 55 jurisdictions—the 50 States and the 5 territories and the District of Columbia. So I believe that, as Under Secretary Krebs talked about, there was a lack of cooperation—not cooperation but communication with Federal partners before that but I think since the EAC's founding in 2003 that we have helped States improve the process. So I think that as each election goes on that we will continually improve that process.

Miss RICE. Thank you. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much. The Chair now recognizes the gentleman from New York, Mr. Katko.

Mr. KATKO. Thank you, Mr. Chairman, and I want to congratulate you on becoming Chair of this committee and I am looking forward to working with you and Mr. Rogers and I know based on past experience with you that we will continue the fine bipartisan work on this committee that I wish the rest of Congress would engage in.

Mr. Krebs, it is nice to meet you. I am now the Ranking Member of the Cybersecurity Subcommittee and in that capacity I think we will become well-acquainted with each other going forward.

I was heartened, Mr. Krebs, about what you said in your testimony today and what you said in your written testimony, that there has been no evidence to date that any identified activities of a foreign government or a foreign agent had a material impact on the integrity or security of election infrastructure or political or campaign infrastructure in the 2018 midterms. That is a great thing.

But, I also kind-of took pause by what you said that election security has come a long way, but it bears additional measures. One of the things that you mentioned was auditability.

I want to make sure I understand a little bit more in depth, what are some of the additional measures you think we should be taking to makes sure that we do the best we can to secure our elections?

Mr. KREBS. So, I continue to believe and that—and Secretary Neilson has been consistent with this as well, but voter verifiable paper trails are critical elements of auditability. In that—after-election audit processes, and I don't want to stipulate to any specific type of audit, there are a number and variety of audits that could be implemented based on the systems that are in place, but those are two elements.

Mr. KATKO. Mr. Hicks, is there anything you want to add to that?

Mr. HICKS. I believe that the States in 2018, when they submitted their request for funds to us, allocated over $20 million to go toward the auditability of elections. There are many different ways to audit elections, and then as we move forward, the EAC has done a paper on 6 ways to do audits and I hope that States take advantage of those resources.

Mr. KATKO. Now, Mr. Hicks, you also mentioned that as part of the process of review, you wanted to look all the way through the voter registration process. Could you explain the different steps you would like to look at as far as doing your audits of the election security?

Mr. HICKS. So, it is basically to go, and it is not just depending on audits, it is basically to go from voter registration and list maintenance to ensure that the folks who are on the rolls are the people who are assigned to that.

Many States have gone toward on-line voter registration through the DMVs and other aspects. Some States have gone to automatic voter registration, and then you go toward polling places to ensure that people have access to the polls to make sure that the ramps for those who have disabilities and wheelchairs and so forth can still get in there and the height of the machines and so forth, to the poll worker training, I think that is a vital part. They are the front line of defense that we have in terms of Federal elections.

There is over a million requests for poll workers in each Presidential year that is always coming up short and I would like to see for—for more people to actually volunteer to be poll workers.

Then, toward election night reporting with the Associated Press, and other aspects as well. So, it goes from A to Z in terms of ensuring that our election process remains strong and that voters' confidence remains high.

Mr. KATKO. Is there anything you might add to that Mr. Krebs?

Mr. KREBS. No, sir.

Mr. KATKO. OK, another question I have is, what—do you—does the size of the State matter at all, as far as compliance with these issues and being active participants in them, No. 1?

No. 2, the nation-state actors, obviously we are concerned about them, the Iraqs—I mean the Irans and the Russians of the world and others. Is there other actors outside of that arena that you have potential—that have potential to disrupt around minor elections, Mr. Krebs?

Mr. KREBS. So, to your first question, we have the smallest State and the largest State engaging with us. So, I wouldn't characterize any sort of participation based on the size of the State.

In terms of the landscape of threat actors, certainly the big four or primarily, in this case, China, Russia, Iran have been active in foreign interference and influence operations.

But, generally speaking, in terms of cybersecurity issues writ large, we do see more blended operations, proxies, cutouts, things like that, so that is on the international landscape. It is just getting more complex, more of a blended environment.

Mr. KATKO. Mr. Hicks, want to add to that?

Mr. HICKS. Thank you, sir. The—I believe that it is a misnomer that think that it is the States, but it is mostly the local election officials who are running the elections and it is usually one or two individuals. It is not the large counties that are basically targeted. It is usually the person who is not only handling the election, but they are driving the school bus, they are doing payroll, they are doing nine other different things, and so they are targeted.

So, we try to offer—we try to go out to the States and offer training as I.T. managers for election officials to their State conferences, because they are not always able to come to the District of Columbia to get that sort of training.

Mr. KATKO. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much. The Chair now recognizes the gentleman from California, Mr. Correa, for 5 minutes.

Mr. CORREA. Mr. Chairman—thank you Mr. Chairman. First of all, let me congratulate you on your chairmanship, sir. Wanted to also thank you for holding this most important hearing on our Democratic institutions, our voting system, the integrity of our votes goes to the heart of our Democratic system in this country. Thank you very much, sir.

First question I have is for Mr. Hicks. That is, during the recent Government shutdown, secretaries of state across the country were notified that conversations with the Department of Homeland Security would be suspended.

Can you tell me what the effects, negative, of the Government shutdown were, in terms of harming the security of our election system, given these next elections are just around the corner?

Mr. HICKS. I think that is more appropriate question for Under Secretary Krebs, with his discussions with Homeland Security.

Mr. CORREA. Mr. Krebs.

Mr. HICKS. I would add that with the Government shutdown, we were furloughed. I was still working myself and then we have hired a CIO to ensure that our infrastructure in our office would remain high. We still had conversations with States and locals.

As I stated in my testimony, some of our delay, in terms of reporting out issues, have occurred because of the Government shutdown and our election voting administration survey, we are collecting that data to hopefully have that out to Congress by the end of June, but I am hoping that none of that will be delayed because of the shutdown.

Mr. CORREA. Thank you. Mr. Krebs.

Mr. KREBS. Sir, so during the shut—there was no question there was an impact from the shutdown. During that 35-day period we continued to share intelligence, threat intelligence, as it came in. We continued to send indicators out to those Albert Sensors I mentioned earlier on. We continue to conduct analysis based on the information we had and the intelligence that we had.

In terms of the things that we had to pause, for one, meeting with new secretaries of state that were sworn in earlier in January; that was probably my biggest regret in terms of missed opportunities. We also had to pause some of the vulnerability assessments. We have since rescheduled those, and those are back on the books.

Then just general planning, in terms of the recent National Association of Secretaries of State and the State Election Director annual conference, content development for that engagement did have to slow. My sense of things, though, was we ramped back up, I placed election security as one of the top priorities for CISA as we restarted after the shutdown.

My sense of things is that we will be back on track, if not already back on track, for instance, we are already in the planning process for another National-level tabletop exercise this June. Last year we had 44 States in the District of Columbia. This year we hope to outdo even that.

Mr. CORREA. Very quickly, cybersecurity, as it pertains to the census that exercise we do every 10 years, redistricting is based on the census, how secure do you think that data, redistricting data, census data is when it comes to cyber threats?

Mr. KREBS. We do work directly with the Census Bureau on protecting the system, particularly the 2020. So, happy to come back and provide you a little bit information and the committee——

Mr. CORREA. That is a critical issue.

Mr. KREBS. Yes, sir.

Mr. CORREA. Mr. Hicks.

Mr. HICKS. That is not one that the EAC focuses on. But I talk to our staff and get a clear answer for you sir.

Mr. CORREA. But I presume that it is something on—on your plates—something on your radar that you are looking at, again, security of our census data?

Mr. KREBS. Absolutely. Yes sir. Like I said, we do work closely with the Census Bureau on this—the 2020 census.

Mr. CORREA. Quickly, post-election audits, what would such audits look like? Would they be the same across the country?

Mr. HICKS. Those would not be the same across the country. What works in Rhode Island might not necessarily work in Washington State.

Mr. CORREA. Is that because of the paper versus no-paper situation?

Mr. HICKS. No. It is just that there is different factors to it; the number of people, the way that they run elections. Some are townships. Some are counties, and so forth. It would be more of the type of machines that they use, and other aspects of it. But I believe that it is—that all States should be doing some sort of audits to ensure that the confidence of elections remain high.

Mr. CORREA. Thank you. Just different machines, different outcomes, different standards, do you see us giving States rights here? The ability of States to choose whatever they want to purchase. Are we looking at moving toward more standardization?

Mr. HICKS. No. I think that States should purchase the machines that work best for them. I would equate it a little bit to purchasing a car. You might want a different type of car, but all of those cars should still have some sort of standards associated with it.

Mr. CORREA. Thank you. Mr. Chairman, I yield.

Chairman THOMPSON. Thank you very much. I now recognize the gentleman from Texas, Mr. Ratcliffe.

Mr. RATCLIFFE. Thank you, Mr. Chairman. Thanks for holding this hearing. Securing election infrastructure is and rightfully should be one of the central priorities of this Congress, and certainly a priority for the American people.

I will say that I don't think that Title III of H.R. 1 adequately brings forth solutions that effectively and efficiently addresses the issue of hardening election security, much less do so in a bipartisan manner.

I do want to start with you, Director Krebs. Good to see you again. One of the things that CISA is in a unique position to do now is it sits between the resources, and capabilities, and intelligence of the Federal Government, and the innovation that is happening in the private sector.

But one of the things that I have heard often over the last 4 years, as the Chairman of the Cybersecurity Subcommittee, is that the amount of actionable intelligence, or information coming from the intelligence community, being provided to the private sector through DHS is not enough, or is not good enough, or is not timely enough, or is, in some respects, stale information. You and I have talked about that. I would be curious in your perspective, now as the director of CISA. Address, for me, the progress, with respect to that issue.

Mr. KREBS. Sir, thank you for the question. It is for sure, a continuous improvement process. We are better than—today than we were a couple of years ago. I do want to say that—that this election cycle, 2018, the time between 2016 and 2018 really was a—for us, and the intelligence community and law enforcement, a forcing function to improve the way we go about doing business both, on intelligence, analysis, sharing, partnering on incident response, and other surge capabilities.

That we are going to be able to spin that out so the election community is supported, but so is every other sector; the grid, the financial sector. Every other critical infrastructure sector will benefit from the progress we have made, specific to the election community, over the last 2 years. So net-net, we—there is progress there.

In terms of the specific information sharing, the—I mentioned those Albert Sensors. One of the things that we really worked closely with the intelligence community on was helping the I.C. understand what the information—the network defense requirements were of the community—of the election community so that they could refine their collection and analysis, and then push their refinements back out into the network defender space.

We have also conducted some studies, in terms of the indicators that we share through our automated indicator sharing program. Based on those studies, 30 percent of the indicators that are shared are unique and they have a unique shelf life, about 120 days.

That is one of my areas of focus for the agency, finding where we are unique. Finding where we have value-add, and we are not competing or supplanting a private-sector capability, but really action—taking action using those intelligence community capabilities.

Mr. RATCLIFFE. So when we talk about the election infrastructure threat landscape, we talk about needing to provide our Federal partners, but also our State and local officials and private-sector vendors with the information and capabilities they need to better defend that infrastructure.

I noticed in your testimony you talked about DHS host—hosting a tabletop vote exercise, really for that purpose, in terms of identifying some of the best practices and areas for improvement on cyber incident planning, preparedness, identification, response, recovery, all of those things. What is your overall takeaway from that exercise? Was it impactful, and how so?

Mr. KREBS. So my sense of things is yes, it was impactful. I suggest you ask the next panel whether they found that useful—that exercise useful. But I think the numbers prove that it was at least a coordinating moment. That we got 44 States and the District of Columbia participating over 3 days, in the middle of primary season, that in and of itself shows that the community is participating.

We also had social media companies. We had political parties. We had the defense—the Department of Defense, the intelligence community. We believe we can do better. So, we are going to do the tabletop to vote exercise again, as I mentioned, once again this summer.

But again, it really reinforced, for us, that any small piece of information that an election official finds they should share because that—a bunch of small things can add up to a big thing. That was, kind-of, along the see something, say something line, really trying to reinforce that information sharing, both ways, can lead to better defense across the systems.

Mr. RATCLIFFE. Thank you, Director. I see my time is expired. I yield back.

Chairman THOMPSON. Thank you very much. The Chair recognizes the gentlelady from Michigan, Ms. Slotkin.

Ms. SLOTKIN. Good afternoon, and good morning. Thanks for being here, to both of you. I agree with my colleagues. I think election security has got to be one of the most bipartisan issues. We can all agree that threats to our democracy and the integrity of our democracy is a threat to our National security.

If we, as a people, do not believe in our system, all forward progress is lost. So I think it is an extremely important issue. I think that there are two pieces to it that I am worried about. One is actual election security, right? So the integrity of the actual systems and you have spoken to that.

But then, there is the perception that the elections, particularly in 2020, may not be fair and free, right? On both sides, regardless of what side you are on.

You have talked about good work that you are doing and I appreciate that but if you can just give us your sense on both issues, what is the one issue on both issues that keeps you up at night? What are you most worried about on election security actual integrity of our system and then on the perception, right, because I think for all the good work you have done, there is a huge group of people who are just ready to say, on both sides, that 2020 isn't going to be free and fair which is a deep—deeply concerning to me. So on election security and the perception that they are not secure, what keeps you up at night for both of you?

Mr. KREBS. So this question lasers right in on I think the biggest area of discussion that we need to have in the country right now. So first and foremost on the security of the systems, we have both mentioned it several times, the committee Members have mentioned it, we have got to get to auditability. That is—that is the key, understanding what is happening across the process is critically important.

On the perception, we did a lot of work throughout the 2018 cycle on education and awareness not just in the voting public. Working with the EAC and some of the election associations, we issued guidance, awareness materials, reinforcing that go to trusted sources for information on elections. Those trusted sources are the elected officials at the State and local level. Go look at the State secretary's website for information on when you vote, how to register, what the deadlines are. Go to the source. Don't listen to whatever third party, fourth party, whatever you have—whatever have you which plays into the bigger part of we have to do more awareness building in this country and introduce critical thinking and reinforce critical thinking as we are just deluged with information. It is too easy to just click like and forward on. We have got to have people thinking, where is this information coming from? Why is it being served up to me? That continue—will continue to be one of our priorities going into 2020.

Mr. HICKS. Thank you for the question, Congresswoman. I agree with Secretary Krebs but I also wanted to add a couple of other things. One, election interference is nothing new. It was mostly done, you know, since—it has been done since we have had elections. Whether or not that is pamphlets saying Democrats vote on Wednesday, Republicans vote on Thursday or other access to the polls, but the things that I would want to focus in on for our—our agency is to ensure that all aspects are taken care of. One being access and also access for three different groups. One, our military and overseas voters who—who don't always have access to ballot boxes and so forth. Two, our disabled voters who might not be able to get access inside the polls themselves and the third would be language minorities.

Ms. SLOTKIN. So I know I have a very short time and thank you as a military spouse for ensuring that our military can vote. That is a big issue for our military community. So you both mentioned this—and the perception—the concern that the perception that these aren't free and fair elections, the role of social media, of news, of third sources passing along the wrong information. Can we—can you do your jobs without the social media companies doing more—particularly social media companies doing more to identify and disclose who is actually paying for some of the ads that are coming through? Who are actually, you know, originating and spreading this information? Can you help me understand their role in making your jobs harder or easier?

Mr. KREBS. So transparency for certain is key. I will say that the social media companies deserve some credit for what they did, how they stepped up in the 2018 cycle. On Election Day we had a National situational awareness, more room, both a virtual presence where all States and local jurisdictions were plugged in but we also had a physical presence at our facility in Virginia and the social media companies participated.

Now what that allowed us to do is win election officials, identified disinformation, misinformation, or just flat-out false information that was being passed around, videos that have been edited but saying, look this machine is changing my vote. It was immediately flagged for the social media companies. Social media companies were able to get the ground truth with the election official, they were able to pull down that false information because it was in violation of their terms of service and then the election official was out and able to say, here is what really happened. Don't believe that. So they—they played a part.

There is always much more to do here and keep in mind that the adversary will continue to pivot, pivot, pivot as we raise defenses and block off avenues.

Ms. SLOTKIN. Thank you gentlemen. I am almost immediately out of time so I appreciate it.

Chairman THOMPSON. Thank you very much. The Chair now recognizes the gentleman from North Carolina, Mr. Walker.

Mr. WALKER. Thank you Mr. Chairman. Director Krebs, is there any evidence of foreign interference in the 2018 elections?

Mr. KREBS. So as I indicated in opening and my written, the statement issued by the DOJ and DHS last week indicated that there was no attributable—there was no evidence of attributable activity to a nation-state actor of material impact on the election.

Mr. WALKER. Thanks for covering that again. I just want to make sure that we are on the record with that. Is there any evidence of domestic interference in the 2018 elections?

Mr. KREBS. I would have to defer you to the Department of Justice on that.

Mr. WALKER. OK. How should we or how do we define interference? Is it just hacking and abusing voting systems or does it also include false or misleading political statements?

Mr. KREBS. Well I believe the way the 2016 intelligence community assessment broke things down, at least the way I look at foreign interference, it is consistent with that report, there is hack and lead campaigns that was targeting for instance in 2016 the DNC releasing sensitive e-mails. There is the social media campaign that disinformation trying to sow divisiveness across the community and then third is the actual technical cybersecurity operations focusing on election infrastructure.

It is important to note that anyone, any actor, could do any of those three things. It is just a matter of capability and then effectiveness.

Mr. WALKER. I want to go to Commissioner Hicks before I ask my question. I do want to say Commissioner Hicks, I think that is the best baritone voice I have heard since Lou Rawls.

[Laughter.]

Mr. WALKER. I don't know, maybe you could slow jam the election news with Jimmy Fallon sometimes, I don't know. But my question is, what separates interference from political free speech? Can you give us a line or describe the parameters there?

Mr. HICKS. That is a difficult question but thank you for the compliment by the way. The election assistance commission focused mostly in on the administration—the administration of elections. So we work with the States and local officials to help them administer the election in a way that ensures that confidence remains high, that there is no interference with the First Amendment rights of individuals or groups but to ensure that our role and we stay in our lane with that.

Mr. WALKER. So from what I am understanding, it is a hard line to call or it is hard to interpret. Who ultimately does make that decision where it crosses over in being more just somebody's right or somebody's free speech rights versus someone else who would call that interference? How do we describe that—how do—how do—in moving forward how do you interpret that?

Mr. HICKS. Domestically, that would be the Department of Justice to make that determination.

Mr. WALKER. All right, let me get a couple more—time for a couple more. Going to go back to Director Krebs, director, there were multiple reports of campaigns being hacked in 2018. What did the DHS provide in assistance in these instances?

Mr. KREBS. So, would have to defer to the Department of Justice and the FBI on any specifics of their engagements, whether they engaged in the campaigns. We provide our resources as a technical cybersecurity capability to anyone that is interested.

Any information that we had or picked up through press or through referrals from the Department of Justice, we would offer our services, that would be a vulnerability assessment, that would be an incidence response assessment and those sorts of things. Those relationships, as they come about, are sensitive, confidential, trusted relationships. But, generally speaking, we continue to provide information, incidence response capabilities.

Mr. WALKER. Sure. I am sure they appreciate the support, but this—maybe just as a yes or no, are you aware that there were campaigns in 2018 that were hacked?

Mr. KREBS. I am aware of reports of campaigns having, for instance, spear phishing and things like that——

Mr. WALKER. When you say you were aware of it, did you guys take a look at it? I know DOJ is lead on that, but from your organization, were you contacted to look into this any further or offer support on a campaign that was hacked?

Mr. KREBS. I would have to go back and look at the specifics of any campaign. We are aware of spear phishing events and things like that.

Mr. WALKER. Help me understand, when you say got to go back and look. You are not aware or you were aware of some? You just don't remember?

Mr. KREBS. What I am unclear on right now is our actual engagements with any specific campaigns. Typically on things of that nature that the FBI has direct lead on engagement. We come back—we kind-of put out the fire so to speak.

Mr. WALKER. If we provided maybe 2 to 3 weeks, is that possible? I would love to have——

Mr. KREBS. Certainly, I would follow up, yes, sir.

Mr. WALKER. I would appreciate that. Last question, to your knowledge does H.R. 1 addresses campaign security?

Mr. KREBS. I would have to go and dig into H.R. 1. I have been focusing on the election infrastructure piece. We always provide assistance to political campaigns, political infrastructure. So, whether it is included in H.R. 1 or not, we will always provide assistance.

Mr. WALKER. OK, thank you so much. Thank you, Mr. Chairman, I yield back.

Chairman THOMPSON. Thank you. The Chair now recognizes the gentlelady from New Jersey, Mrs. Watson Coleman.

Mrs. WATSON COLEMAN. Thank you Mr. Chairman. I am concerned about reports that election vendors don't fix vulnerabilities once they have been made aware of them, and then, in fact, it is not just recognizing a vulnerability and then reporting it and not having it dealt with, but even years have been involved. What role does the EAC have in making sure vendors are taking steps to remedy vulnerabilities when they find them?

Mr. HICKS. If a vendor is—thank you, Congresswoman, for the question. If a vendor is a registered vendor with the EAC, they have a certain amount of time to report errors with their machines to us and fix those vulnerabilities.

Mrs. WATSON COLEMAN. If they don't? If they don't fix them?

Mr. HICKS. Then we don't have enforcement authority, in terms of fining and so forth, but we can go toward the decertification of their voting equipment.

Mrs. WATSON COLEMAN. Does that mean that then no one can purchase their voting equipment?

Mr. HICKS. Then it would not be certified under EAC standards.

Mrs. WATSON COLEMAN. So, no one could purchase and use their voting equipment?

Mr. HICKS. If someone—since it is a voluntary system, folks could still purchase that equipment and use it.

Mrs. WATSON COLEMAN. To what extent have we knowledge of that kind of a problem?

Mr. HICKS. If they are—voting machines are basically computers. So if there are patches that need to be made, then those are acknowledged and then fixed.

Mrs. WATSON COLEMAN. But, to what extent do we know of it being a problem where a vendor has been given sufficient notice and still has neglected to fix these things?

Mr. HICKS. I have——

Mrs. WATSON COLEMAN. Is that a pervasive problem? Is that a rare problem?

Mr. HICKS. I am not aware of any issues to that degree.

Mrs. WATSON COLEMAN. Do you think that we need some kind of enforcement authority in some entity, I don't know which one it would be, that would compel those types of vendors to correct the situation?

Mr. HICKS. If Congress gave us that authority, then we would, like we have with all of the issues with the Help America Vote Act, we would act accordingly.

Mrs. WATSON COLEMAN. I know that—I know that a lot of work is being done with States and secretaries of state, I am wondering—in my State there are 21 counties and the counties are basically the entities that run the elections and the municipalities carry out.

To what extent is there this guarantee that the information sharing, the training, the cybersecurity guidance gets down to those levels? What is the mechanism to do that? Or do you deal directly with the local and county officials that deal with the elections?

Mr. KREBS. So, specific to the cybersecurity information-sharing piece and the technical assistance piece, you have highlighted an area that we recognize needs additional attention. Last year the Elections Infrastructure ISAC, the Information Sharing Analysis Center, had 1,400 local jurisdictions.

My understanding, and the number seems to change regularly, but somewhere in between 8,800 and 10,000 voting jurisdictions across the country. Some—and that is below the county, precincts, voting spots, so we are looking at scalable, repeatable ways that we can engage each and every one of them. For instance, deploying or providing information, I.T. manager training for election officials.

As Commissioner Hicks mentioned, these devices, these voting—this voting equipment, the process, the databases, they are computers. So, election officials sometimes, sole officials end up having to be I.T. managers as well.

So, it is important that we provide them the support, the training, what to look for in terms of phishing e-mails and things like that, how to apply patches, how to work with vendors and ask the right questions. But, for us, one of our top priorities in the run up to 2020 is extending out from that 1,400 and the rest of the——

Mrs. WATSON COLEMAN. So the—thank you. I am sorry. The HAVA money that was already allocated, that is allocated, it is in the hands in of the various States and jurisdictions, right?

Mr. HICKS. There were two rounds of HAVA money. One that were submitted in 2003 and then the 2018 HAVA funds. The 2018 HAVA funds have all been distributed to all the 55 jurisdictions.

Mrs. WATSON COLEMAN. So, we do we have an understanding about how much more money we need in order to ensure that the right voting machines, the appropriate voting machines that have the verifiability in them, would cost?

Mr. HICKS. The—from my travels around the country, from what I have heard from individual States in terms of replacing all the voting equipment, can run from between half a billion to $1 billion.

Mrs. WATSON COLEMAN. Thank you. I yield back.

Chairman THOMPSON. Thank you very much. The Chair now recognizes the gentleman from Louisiana, Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman. I am honored to serve on this committee again with you, sir. You are a solid patriot. With your leadership, and that of Ranking Member Rogers, I believe our committee will always move forward. Contentious, though, at times, we may be. We will be focused on the security of our homeland and we will get things done.

Mr. Krebs, the voting systems that we are discussing today, explain to America—my research says that there is somewhere over 174,000 voting precincts in America. Is that true?

Mr. KREBS. I would have to defer to Commissioner Hicks on——

Mr. HIGGINS. Is that true sir?

Mr. HICKS. Yes, sir.

Mr. HIGGINS. So you have got a lot of voting precincts. Article I Section 4 of our Constitution gives a station—States and local jurisdictions State legislature authority, specifically to the time, place, and manner of holding elections for Senators and Representatives shall be prescribed by each State by the legislature thereof.

So you are dealing with over 174,000 small communities. The voting systems we are discussing and the integrity thereof regarding cyber threat, is it true that most of these systems are—are independent? They are electronic. They are analog. They are not connected to the internet at all. They are—they are—they are in high schools and in gymnasiums across America, and cafeterias at elementary schools. They are rolled out, secured, and plugged in. They are not connected to the internet at all.

Mr. KREBS. So there is, obviously, a range of equipment out there from various vendors. The general best practice is yes, they should be air-gapped. They should not be——

Mr. HIGGINS. There you go.

Mr. KREBS. I use that term——

Mr. HIGGINS. I just wanted to clarify that. We are dealing with scores of thousands of individual voting systems, most of which are—are not actually connected to the internet. Now, the threat is real and should be—should be addressed, certainly. This committee will do our job regarding election security.

In the densely populated areas there is—obviously, a threat to a single precinct would be more significant, regarding numbers, as opposed to more rural areas. Is that correct?

Mr. KREBS. I think the threats can vary. There are certainly situations where a more densely populated—could pose a higher risk.

Mr. HIGGINS. In other words, a small percentage of error interference would have a greater affect on numbers in more a densely populated area, and a more heavily voted precinct.

Mr. KREBS. It is possible.

Mr. HIGGINS. So it is a landscape across our Nation that we must serve. In my opinion, and those of my colleagues, I believe on both sides of the aisle, we need to move forward carefully. The—the cyber threats themselves—now that we have, sort-of, categorized what we have got. Nation-states, rogue states, bad actors like Russia, Iran, China, North Korea versus a criminal element; organized crime.

How would you differentiate between the cyber attempt to interfere with an election by a nation-state versus a cyber attempt to interfere with an election by a criminal element within a nation-state?

Mr. KREBS. So at this point, I think given the way the threat environment has blended, and you have hybrid threat actors. I am not sure that there is much of a distinction between nation-states and criminal elements.

Mr. HIGGINS. Exactly. It—and in times past during the Cold War—are you familiar if you are a student of history, gentlemen? That rogue states, some of our enemies across the world attempted to influence public opinion and policy with pamphlets, and flyers, and illegal radio broadcasts into territories. Is that correct?

Mr. KREBS. Yes, sir.

Mr. HIGGINS. So wouldn't that take—wouldn't that reflect, in the modern era, using social media, and the attempt to influence public opinion, and perhaps elections in that way?

Mr. KREBS. As—as we saw——

Mr. HIGGINS. So this is nothing new, is it?

Mr. KREBS. Well, as we saw in 2016, there were technical lone network operations, as well as influence campaigns. Those activities—the influence campaigns, in particular, continue today.

Mr. HIGGINS. Right.

Mr. KREBS. It is not just Russia.

Mr. HIGGINS. It continues today, and we need to adapt to the changing time. I thank you gentlemen for doing both.

Mr. Hicks, as an American should—in your opinion sir, do you think that a voting precinct, again, of over 174,000 in our country that has never had an issue and have never had a complaint; they have the Constitutional rights to run their own elections. These—this would include local and State elections, as well as Federal, of course. Do you think a voting precinct that has never had an issue or a problem with their system should be forced by the Federal Government to spend money and invest in manpower, and change, and—and receive interference from the Federal Government? I will leave you to answer, sir.

Mr. HICKS. Thank you for the question. I wanted to clarify one quick thing, it is 8,000 jurisdictions across the country, and then the voting precincts are what you are referring to.

I wouldn't necessarily say that there has never been any issues with any of those voting precincts. There are issues with every election, as we go—move forward. That is just the nature of elections. But we need to address and adapt to each issue as they arise.

Mr. HIGGINS. Well stated, sir. I yield back, Mr. Chairman. Thank you for your indulgence.

Chairman THOMPSON. The Chair now recognizes the gentlelady from New York, Ms. Clarke.

Ms. CLARKE. I thank you, Mr. Chairman, and I thank our Ranking Member, and I thank you gentlemen for appearing before us today. As a follow-up to a question my colleague, Ms. Bonnie Watson Coleman of New Jersey, asked: How is DHS and EAC prioritizing outreach to the local governments—local level?

Mr. HICKS. Well, the former president of the National Association of State Election Directors was actually from New Jersey. We worked really closely with him, and all other States, to ensure that the process was moving forward. So it is a high priority for us. It is one we take seriously, but it is not our only priority.

Mr. KREBS. DHS's No. 1 priority; more State—more local engagement.

Ms. CLARKE. Very well. There seem to be areas where State and local election officials have not yet resolved low-hanging fruit issues of their election security; for instance, the use of wireless modems to transmit election results. These practices needlessly introduce vulnerabilities into the process.

What do you perceive as some of the low-hanging fruit in securing election operations? Might stronger, more vocal leadership from Federal partners like DHS, or EAC, or even the White House, move the needle on those issues?

Mr. KREBS. So over the last couple of years we have conducted a number of vulnerability assessments, 26 plus jurisdictions, State and local. We have also conducted remote penetration testing.

The interesting thing that we found was that, of all of those assessments, the findings were generally similar; unpatched systems, misconfigured systems, lack of multi-factor authentication.

So what happened is we took a lot of that learning across those assessments, worked with the Government Coordinating Council, which is State, local, EAC, the intelligence community, law enforcement, and put together when Congress appropriated that $300 million to the last HAVA tranche of money, and provided some expenditure guidance.

So our sense of things is that we have been pushing out those best practices. But there is certainly more to do. On the point of the modems and I used air quotes when I said air gap on a lot of the equipment.

Yes, there is equipment still out there that has modems. It is only used in very discrete circumstances. Nonetheless, absolutely that is why I used my air quotes there. It is a best practice to disable or remove that capability.

In some cases there was simply no other alternative for jurisdictions in the 2018. So that capability was limited but left in place. Auditability can also help identify and spot any irregularities.

But my sense and understanding is going forward that continues to be one of those priority actions. Low-hanging fruit as you mentioned.

Mr. HICKS. Thank you again. I think that it goes from A to Z, from voter registration all the way to election night reporting. That all aspects of election should have some sort of security to it.

We have talked a lot about cybersecurity but I also think that physical should also remain high. Also we should continue with our quest to have all elections being audited because then it remains—the confidence of the election remains high.

The way that those audits are conducted can be done by each individual State. But I believe that, in my own personal opinion, that we need to ensure that we do all we can to afford confidence of the—the system. Because what I have said in 2016 and 2018, if you don't vote then your vote definitely will not count.

Ms. CLARKE. Well, I think part of the challenge too is at the local level, just the level of proficiency of the use of the technologies of the individuals who were employed to administer these elections.

I don't know whether you are getting a true sense of that across the length and breadth and depth of our Nation. But I can tell you that there have been a lot of senior citizens that have this as a preferred profession.

Not to disparage anyone but they tend to be a little bit less concerned about cyber hygiene. So I think that there just needs to be a consistent outreach to these local jurisdictions in helping folks to really be trained and vigilant around the work that they do.

Just one more question. I know that we had talked about five jurisdictions that have paperless voting. I wanted to be corrected if I am wrong, but the only record that the votes cast on these machines is a digital record stored on the voting machines themselves, which means if the machine is hacked, election officials have no paper ballot they can count on by hand to determine how the voter really voted. Is that correct?

Mr. HICKS. It is a lot more detailed than that because all these systems have more than one redundancy for back up in their—in their systems. So——

Ms. CLARKE. But if it is hacked how would you know?

Mr. HICKS. Well, it could be stolen as well. So there is all aspects of machines could be—you do a forensic scan of those machines to ensure that the ballots are counted correctly.

Ms. CLARKE. So to the best of your knowledge, were any of these paperless voting machines used by States in 2018 elections running software that was out of date with known exploitable cybersecurity flaws?

Mr. HICKS. I would have to go to my staff to see what the actual scanning of those districts were because it is not just those 5 individual States. There are other jurisdictions around the country as well.

Ms. CLARKE. It would be good if you could get back to us with that. It is very important as you talk about auditability that we are exact in what—how these machines can be exploited.

Mr. HICKS. I would also point to the fact that a lot of these States are moving away from machines that don't have a paper component to them.

Ms. CLARKE. We want to expedite that right? Thank you. I yield back. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much. Chair now recognizes the gentlelady from Arizona, Mrs. Lesko.

Mrs. LESKO. Thank you, Mr. Chair. Thanks for calling me a young lady. I really like that.

[Laughter.]

Mrs. LESKO. I got to hang around here more often. My first question is for Mr. Krebs and thank you both for being here.

You know we have talked—hit on this a little bit with Mr. Walker but there was a lot of media—there still is a lot of media out there about how the Russians allegedly interfered in the 2016 election and I think we found out that a lot of it had to do with social media misinformation.

To Ms. Slotkin's points that a lot has to do with perception, if voters believe that their votes count and they are not being compromised. To your knowledge, was there any evidence or is there any evidence that the Russians or anybody else hacked into the actual election system and changed the outcome of the election on Election Day?

Mr. KREBS. Ma'am, I am not aware of any evidence that they had access or ability to influence the casting, counting tabulation.

Mrs. LESKO. Thank you. The reason I think that is important is because there is a lot of confusion out there and—so we need to make sure that when we talk to people that we are not talking about actual hacking into the election system is what the media is talking about.

However, we want to prevent it in the future of course. My next question is actually for Mr. Hicks and this was touched on briefly by the Ranking Member Rogers. That was about the money in this bill that is going toward certain things.

So the Democrat's Congressional Task Force on Election Security recommended $300 million for States to acquire these paper ballot systems, conduct audits, address cyber vulnerabilities, provide cybersecurity training to local and State election officials, institute cybersecurity best practices, and to make other improvements to effect Federal election security. Through the Help America Vote Act Congress appropriated $380 million in grants for fiscal year 2018 for these purposes.

This bill, H.R. 1, which we are talking about today, authorizes $1.77 billion in grants. So why do we need to give States an extra $1.77 billion to do the same thing that in this task force they said they could achieve with $300 million?

Mr. HICKS. The States—from the States that I have—I have traveled to all 50 States in the last 4 years or so and the States have all indicated that elections—Federal elections occur every 2 years and that the replacement of voting equipment from the 2002, 2003 initial HAVA funds need to be done.

The money that was put into the Help America Vote Act funds for 2018 did not just go toward machines. They went toward Title I, which gave States a lot of leeway into improving the vote—the voting process.

Whether or not that was voter registration, audits, communications, just to—and other aspects as well.

Mrs. LESKO. So, Mr. Chair, and Mr. Hicks, so I don't know if you answered do you—why—why if it—in one report it said you need only $300 million but this one is $1.77 billion. Do you know why?

Mr. HICKS. I don't know why, but I believe that they were going toward one aspect of the process in terms of—and I have to read back through the report, but I would—I am assuming that it was one aspect of what they were looking at as opposed to overall with H.R. 1. Because I believe that they were just looking toward certain machines, but I believe that maybe H.R. 1 covers a lot more than just the one aspect of it.

Mrs. LESKO. Thank you, sir. Thank you, Mr. Chair, I yield back my time.

Chairman THOMPSON. Thank you very much, as a point of clarification the $1.8 billion was for over 10 year's period of time, so it was not just 380—a one-shot deal. So it is in anticipation that upgrading will be a constant rather than just standing for one time.

Chair recognizes the gentleman from Rhode Island, former Secretary of State, Mr. Langevin.

Mr. LANGEVIN. Thank you Mr. Chairman. Director and Mr. Hicks thank you very much for being here and for your testimony and Mr. Krebs I want to thank you also—thank you for the work you are doing at CISA, I am glad that agency has been reorganized and properly tasked, and I look forward to work with you, and supporting you in your work.

Obviously this is one of the most important issues that we are facing as a country, has been securing our elections from foreign adversaries that want to try to undermine and sow discord. They have got a pretty effective, well-coordinated campaign that we have to obviously have to get even better organized and I know that we will.

So I want to thank you and Assistant Director Manfra for your support, particularly in my home State of Rhode Island. I had attended one of the final planning meetings before the election with our Secretary of State Nellie Gorbea, who testified before this committee, along with you.

Also the DHS personnel in the room made vital contributions to that discussion, and as someone who has overhauled an entire State election system, I understand the challenges of having the best equipment and making sure that it works well. When I reorganized and overhauled our election system we didn't have to deal with the issue of course of cybersecurity and threats from foreign adversaries trying to undermine us.

So let me just say, one of the topics that came out of that meeting was coordination with media. We have seen how effectively the Russians, for example in targeting Ukraine elections, went right to the media and trying to sow discord and confusion in election processes. How have you engaged with local, State, and National media outlets to ensure that unofficial voting—vote reporting is protected from malicious interference?

Mr. KREBS. So a couple examples I think that are instructive of the progress we have made, particularly with the National media, but also local and State-level media. Two things, one in advance—2 weeks in advance of the election we held a media tabletop exercise, just like what we did with the State, and local election officials we brought in a couple dozen media representatives, sat in a room, 4 hours, walked through a scenario that included both technical on-network effects as well as social media influence operations.

We walked through here is what you would see, here is what you would hear from a State or a local election official, here is what you would hear from the Federal Government and what the Federal Government would be doing whether it was DHS, the FBI, the intelligence community—and help them understand what was going on in the background.

So that, if something did happen, they would have the basis of understanding, they would know A, who to call, but also rather than say, oh there was a denial-of-service attack against an election night reporting website. We would be able to have a conversation and say, actually it is not that—instead it is simply a configuration issue and that website dropped.

The second thing we did is on Election Day every 3 hours over the course of the election we had a conference call with National media. The same thing, we would walk through issues as they popped up over the course of the day.

Oftentimes we referred them to the local or State election official to address the questions, but where we could chip in and provide some clarification. Really the important thing was getting ahead of issues and dispelling any sort of doubt, or questions about what may be happening in the background. We found it to be very beneficial in terms of getting ahead of problems before they really started.

Mr. LANGEVIN. OK, thank you. Is—another topic, as Commissioner Hicks mentioned on this testimony, I know that Representative Slotkin has touched upon this as well.

Obviously public confidence and the integrity of our elections is a vital component of our democracy and following the 2016 elections, American voters reported a decrease in confidence in the election systems, and outcomes and it is exactly playing to the hands of what our adversaries want to try to accomplish here. But election security, particularly cybersecurity, is certain an important aspect of increasing confidence, but it is not sufficient.

So who right now in the interagency has the role of coordinating protection of election integrity, and its perception thereof, and who—which cybersecurity is just a part?

Mr. KREBS. So in terms of the interagency process, the FBI and the Department of Justice have the responsibility to lead on countering foreign influence, and that is the social media campaigns, that is the direct response—the threat response piece. So as things bubble up, or pop up they work with partners to address and—immediately address head-on.

The Department of Homeland Security's role here is in terms of—is more on the lines of educating awareness, building—taking case studies that we saw in 2016—or even before that that we have seen the Russians do, that we have seen the Chinese do. Then pushing awareness and information out on—these are the sorts of things that you need to look for. Here are the things that you can do to ensure you are getting ground truth and you are getting the right information.

Again, going back to the elections, just as Chairman Hicks mentioned, it is—you need to listen to your State and local election official, they are the ones that have the official information. They are the ones that are going to tell you where to go, what day to vote. Don't listen to the text messages, don't listen to the tweets, or posts or whatever.

Mr. LANGEVIN. So do you believe that—and you talk about who the lead is, but you believe that there should be a whole-of-Government approach, or should it be silos based on experience?

Mr. KREBS. So it is certainly cliche but this is a whole-of-Nation approach. There is a specific role for a number of agencies, including the intelligence community using their specific authorities, whether it is the Bureau and their law enforcement capabilities, whether it is the Department of Homeland Security and our unique convening capabilities.

One thing I will note is that when some of the social media companies over the course of the election took action and took down, whether it was Iranian activity or whatever, we were able to work with the FBI, work with the social media companies, convene the State and local election officials in a call or even a Classified briefing and get—and have them walk through, here is what happened, here is what you need to be on the lookout for.

So there is a role in this for everyone. There is a role in this for every American, and—and it is upon us, particularly the Department, to give them the awareness, the tools to be smarter consumers of information.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much. The Chair now recognizes the gentleman from Tennessee, Mr. Green.

Mr. GREEN of Tennessee. Thank you, Mr. Chairman and Ranking Member. I extensively reviewed H.R. 1 in my previous committee hearing on Oversight and Government Reform. I certainly believe that election security is critical. Ms. Slotkin did a very nice job of saying—speaking about it, and I am impressed. I have to tell you, I am very impressed with what you have done in the 2018 cycle—essentially flawless.

There were no penetrations that we are aware of—and we have to be able to do that. We—our democracy rests on one person, one vote. But with regards to this H.R. 1, I am going to be completely upfront and say that I am disappointed by the Majority party because it seems to have disregarded our Constitution.

They claim the purpose of the bill is to protect our institutions, but they are promoting a bill that fails to improve security, all while thumbing the nose—or its nose to Federalism. Our country was not made for a few hundred people in Washington, DC to dictate to my State in Tennessee how we are going to do everything, including our elections.

Our founders, our Constitution, our electoral process have been grounded in Federalism. This bedrock is the foundation of our country, and it has to be protected. When power is concentrated in the hands of a few, tyranny inevitably follows. Our founders knew this; that is why they created, you know, three branches of Government.

They created separation between the Federal Government, the States, the local government—recall the 10th Amendment. I want to thank you again for the hard work that resulted in such success in 2018, and I, from the previous questions that were asked, assume you have not read H.R. 1. Is that correct?

Mr. KREBS. I have reviewed it, yes.

Mr. GREEN of Tennessee. You have reviewed it? OK. Can you tell me, then, in a more global sense, how far should the Federal Government be able to go in telling Tennessee how we run our elections? Considering specifically, what was read earlier from my colleague, about what the Constitution says concerning elections.

Mr. KREBS. I—so every State is different; every jurisdiction's different, every set of equipment's going to be different. I would defer to Secretary Hargett to decide what is best for the citizens of Tennessee.

But whatever I can do, as the Department of Homeland Security, to make his job easier—the thing I will note, and it has been part of the conversation throughout the morning, that the threat landscape is different today in 2019 than it was in 2001, with HAVA and even before that. Back then, we were focused on—the Department was focused on an antiterrorism mission.

Today, we have the most active nation-state adversary landscape, certainly in my lifetime. That means that individual States, individual counties, individual precincts cannot go it alone against the full-frontal assault of the Russian GRU or the Russian FSB. So I need to be able to provide whatever capabilities I can so that we can assure a collective defense across election security.

Mr. GREEN of Tennessee. Yes, but the—the—as you have reviewed H.R. 1, I am sure you know that it tells Tennessee we can't have voter identification; it tells us we—we can allow voter registration to happen on the day of the election with no way to verify it.

That seems to me to be a violation of the Constitution, as has been read and is clearly articulated in the 10th Amendment. That is more than just security; that is dictating how we run our elections in Tennessee.

Quite honestly, that is offensive to us down in Tennessee. For Mr. Hicks, I do have a question, sir. You said there is about 8,000 jurisdictions, if I understood correctly. How many of those jurisdictions are identical? They do elections identical to one or the other?

Mr. HICKS. That would be a difficult question to answer. I believe that, you know, each individual jurisdiction conducts their elections the way that they feel best for those constituents in their jurisdiction.

But the Election Assistance Commission goes to these—once invited, goes to these States and jurisdictions to offer our assistance, whether or not that is the $380 million that Congress appropriated or other aspects through our clearing house or other aspects of it, because those jurisdictions might not know techniques or things that are being done in other jurisdictions. But we bring that to them so they can run their elections effectively.

Mr. GREEN of Tennessee. Well, thank you for that answer, and I really appreciate it. My issue isn't so much with you not—with your help—we want your help; it is essential to protecting—but dictating how we run our elections in Tennessee, that is a little different. That is my point. Thank you very much.

Chairman THOMPSON. The Chair now recognizes the gentlelady from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Mr. Chairman, thank you very much for this hearing. Along with the Ranking Member, we are appreciative for a hearing that indicates one of the strongest elements of democracy is the independent right of every American to cast their vote, unimpeded, unsuppressed, and unoppressed.

Let me ask you, Commissioner Hicks—and thank you for the Election Assistance Commission. In 2016, I believe then-Secretary Jeh Johnson joined with 16 other agencies, intelligence agencies, as I recall, the fall of the election to indicate a conspicuous engagement of Russia into the elections.

Let me just read a sentence—E-Deceptive Campaign Practices Report 2010; Electronic Privacy Information Center. They are, however, talking generally about what deceptive campaigns or attempts to misdirect targeted voters, regarding the voting process, or in some way affect their willingness to cast a vote.

Deceptive election activities include false statements about polling place opening and closing times the date of the election—voter identification rules or the eligibility requirements for voters who wish to cast a vote. I think the intelligence report was focused on targeting voters, misleading information, social media, do you believe, based on those intelligence reports at that time—you are aware of that report, elective report, in 2016?

Mr. HICKS. I am aware of it.

Ms. JACKSON LEE. Do you believe the reports, first of all, Mr. Johnson joined in that report ahead of the Department of Homeland Security?

Mr. HICKS. I have no reason to believe that that was false.

Ms. JACKSON LEE. So in that—and Mr. Krebs?

Mr. KREBS. Yes, ma'am; I agree with the intelligence community assessment.

Ms. JACKSON LEE. So we know that there is, among others—and we certainly know that Russia is—looms large as having intentions to interfere with our elections. That means Federal elections, but Federal elections are held in States. We are a collective of 50 States, so we know that that—they would be impacted.

In that kind of report and the efforts that you all have, do you see States willing to accept your assistance, and in what way is the best way that you are helping States acknowledge their own plight, if you will, of susceptibility to this kind of intrusion?

Mr. HICKS. I believe State—thank you, Congresswoman—I believe States have come to the Federal Government more so than they were before because there was a little bit of a hesitation that way. But I believe that communication has improved to the point where States are giving their input through the Government coordinating council, working with vendors and other aspects of that through the sector-specific council to ensure that the election integrity remains high.

Ms. JACKSON LEE. Let me, because my time is short, go to the cybersecurity for both of you to ask or Director Krebs you can start with this. Cybersecurity involves everything from large systems to small mobile devices. My question is about a host of technologies Classified as edge devices that may have internet connections. How concerned should you be about edge devices and election technology security?

Mr. KREBS. So we——

Ms. JACKSON LEE. We could be concerned.

Mr. KREBS. Yes, ma'am. I briefly touched on some of those equipments that have modem or other telecommunications connectivity, best practice generally speaking is to disable or remove that sort of capability. In 2018 some just didn't have the time or the equipment to transition out. But it is something that across the risk profile of election infrastructure, it is something that we work on. We work with the State and local officials that have that equipment and we work on transitioning and road mapping to more secure systems.

Ms. JACKSON LEE. To each of you, do you feel, in spite of your good works, that our election systems, State and Federal, are still in jeopardy of intrusion?

Mr. HICKS. I believe that there can always be improvements to be made and I believe that the work of the EAC can help with those improvements.

Ms. JACKSON LEE. Do you feel that would be foreign intrusions——

Mr. KREBS. Yes. There is always progress that can be made.

Ms. JACKSON LEE. Let me ask the Chairman to submit into the record from the Brennan Center for Justice a study on securing elections from foreign interference, ask unanimous consent.

Chairman THOMPSON. Without objection.

[The information referred to follows:]

LETTER SUBMITTED FOR THE RECORD BY HON. SHEILA JACKSON LEE

*February 12, 2019*.

Representative JACKSON LEE,
*2079 Rayburn HOB, Washington, DC 20515.*

DEAR REPRESENTATIVE JACKSON LEE: My name is Lawrence Norden, and I am the Deputy Director of Democracy at The Brennan Center for Justice at NYU School of Law. First, please extend the Brennan Center's thanks to Chairman Thompson and the U.S. House Committee on Homeland Security for holding tomorrow's hearing on Election Security, an issue of critical national importance. For nearly 15 years, I have led the Brennan Center's extensive work on election security and foreign interference. In 2005, in response to growing public concern over the security of new electronic voting systems, I chaired a task force (the "Security Task Force") of the nation's leading technologists, election experts, and security professionals assembled by the Brennan Center to analyze the security and reliability of the nation's electronic voting machines.[1]

In the 14 years since, I have authored or co-authored numerous studies on the security, usability, cost, and design of our election systems. In 2017, with my colleague Ian Vandewalker, I co-authored *Securing America's Elections from Foreign Interference,* which looks at the key steps we must take to ensure our elections are secure, free, and fair.[2] The report begins with a foreword from Ambassador R. James Woolsey, former Director of Central Intelligence, and I have attached it to this letter.* With the 2020 elections around the corner, I believe the study will be of use to the committee. I ask that this report be placed into the record for the hearing.

In the coming weeks, the Brennan Center will be releasing a new study on the state of voting technology and the need for additional resources to ensure that our elections in 2020 are as secure and reliable a possible.

My colleagues at the Brennan Center and I are available to speak to the committee, as well as provide briefings or updates, at the committee's request.

Sincerely,

LARRY NORDEN,
*Deputy Director, Democracy Program.*

Ms. JACKSON LEE. And unanimous consent for E-deceptive Campaign Practices by the Electronic Privacy Information Center, unanimous consent.

Chairman THOMPSON. Without objection.**

Ms. JACKSON LEE. To the two witnesses just a yes or no answer. The help of this committee and legislative effort to improve your work along with funding, would that be of help to you, Mr. Hicks?

Mr. HICKS. Yes.

Ms. JACKSON LEE. Mr. Krebs.

Mr. KREBS. Yes, ma'am.

Ms. JACKSON LEE. Thank you very much. I yield back.

[1] Lawrence Norden, *The Machinery of Democracy: Voting System, Security, Accessibility, Usability, and Cost,* Brennan Center for Justice, 46, 2006, *https://www.brennancenter.org/sites/default/files/publications/Machinery_Democracy.pdf.*

[2] Lawrence Norden, *Securing America 's Elections from Foreign Interference,* Brennan Center for Justice, 2017, *https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference_1.pdf.*

* The document has been retained in committee files and is available at the website listed above.

** The document has been retained in committee files and is available at *https://epic.org/privacy/voting/E_Deceptive_Report_10_2010.pdf.*

Chairman THOMPSON. Thank you very much. The Chair now recognizes the gentleman from Texas, Mr. Taylor.

Mr. TAYLOR. Thank you Mr. Chairman. Thank you Ranking Member. I appreciate the opportunity to be here.

So in 2011, I carried the MOVE Act Compliance Legislation for the State of Texas. So in 2009 on a bipartisan effort Congress passed the law that allowed States to do—or required States to do a better job of helping men and women who were serving in uniform outside the United States be able to vote. That was—that was a 4-year compliance periods so the States had 4 years to comply with it. One of the reasons for that was that it—logistically we had to change our election schedule in Texas and so I am sure my colleagues from Texas will recall that all of the sudden they were filing instead of in January they were filing in December and that actually required a Constitutional amendment that had to be passed by the citizens of Texas.

So in working on that, again on a bipartisan basis, it took a lot of lifting on behalf of the State to comply with that piece of legislation. This legislation is far more ambitious in what it endeavors to do. Has there been—have—have you done a study Mr. Krebs of what different States' laws they would have to change or Constitutional amendments that they would have to—to comply with H.R. 1? Have you done that Mr. Krebs?

Mr. KREBS. No, sir. We are focused on the technical aspects.

Mr. TAYLOR. OK, and Mr. Hicks, have you done that? Have you analyzed what Constitutional amendments or statutory changes would be necessitated by H.R. 1?

Mr. HICKS. We have not.

Mr. TAYLOR. OK. I certainly hope if this is a serious bill, if this is something we actually think will be passed into law that we have thought about at some level what we are going to have to do at the State level because we cannot comply with this at the State level unless we have really thought about it. I—I hope this isn't a show bill.

So Commissioner Hicks, in terms of ballot stuffing of yesteryear, right? So we—we had ballot stuffing with paper ballots, is—with the paper ballot provision in H.R. 1 return us to the system of paper ballots? I mean is that—is that what we are doing? We are kind-of going back in time?

Mr. HICKS. I guess I would need to read back through it because I don't—I don't interpret it that way.

Mr. TAYLOR. So the way I read it is that it requires paper ballots. Is that—is that not what you—what you understand?

Mr. HICKS. For auditability.

Mr. TAYLOR. Right. So for time—for auditability and I think this is an important distinction that we should let out here. So time now, in my county, we have electronic machines that print out on an individual machine-by-machine basis an audit of every vote so that that can be gone through and done with an audit. So the machines are auditable through a paper trail, not of the ballot itself but of what it—of ballots that are cast on that particular machine if that makes sense.

So as I understand this bill, everybody has got to stop using those machines and start buying new machines that are all paper ballots. That is my understanding.

Mr. HICKS. That is not my understanding because there are some machines that might have a paper trail associated under glass but it would be the verifiability of the voter to verify that piece of paper.

Mr. TAYLOR. Are there enough machines that will be manufactured between now and the beginning of the primaries in less than a year that we could actually implement this bill?

Mr. HICKS. I would need to talk to the vendors to see their capabilities of manufacturing those machines.

Mr. TAYLOR. So we don't know if it could—it is even physically possible to generate the number of machines that will be required with this. I know there is funding in this legislation but I am just unclear of whether or not it is even possible to logistically have all the machines in place.

Mr. HICKS. I would have to talk to the vendors themselves.

Mr. TAYLOR. You don't know. Does anybody—Mr. Krebs, do you have any idea?

Mr. KREBS. I don't know but I assume if there is money to be made they will figure out a way to do it.

[Laughter.]

Mr. TAYLOR. Well and I think and just as a practical—on a practical level so actually in my home county in Collin County, Texas, I was actually an election judge before I was elected to the legislature and in that process I saw what happens when there are not enough voting machines.

You have very long lines, people get discouraged and they don't vote and so you have reduction of participation which is really—it is a really disappointing event.

It is a very sad thing when people show up to vote, they wait for an hour, they can't actually vote because there aren't enough machines. Is—what—what provisions do we have in this legislation that would protect from that scenario because it seems like we are setting up in this rush to try to get a bill out the door to provide funding with very limited amount of time to put it together, so to speak, that we would make sure that we have enough voting locations that we don't have people lining up and then saying I am not going to participate, I am not going to vote.

Mr. HICKS. I think States have done a great job of moving toward Election Day being the last date to actually cast their ballot. Some States have moved toward early voting or vote centers or absentee voting as well to alleviate the charge of having Election Day where 100 million people are trying to show up at the polls.

Mr. TAYLOR. Thank you. Thank you Mr. Chairman, I yield back.

Chairman THOMPSON. Thank you very much. Let me, for the record, indicate for the Members and the witnesses, we are technically here for only Section 3 of H.R. 1 bill. Some of the questions have gone to other sections of the bill and I would like for us to talk specifically about Section 3, which is our jurisdiction. Yes, so I am—I just—I understand the interest, but I don't think the witnesses are prepared to address some of the questions that have been offered by the committee at this point and that is just to make sure that we are all on track.

We now recognize the gentleman from New York, Mr. Rose.

Mr. ROSE. Chairman, thank you, and that is Staten Island, Mr. Chairman.

Chairman THOMPSON. There is a difference.

[Laughter.]

Mr. ROSE. Mr. Krebs, how you doing? I am the incoming Subcommittee Chair of Intel and Counterterrorism, so I look forward to working with you and I think you hit the nail on the head earlier, that it is clear that there are state actors, non-state actors that are probing the homeland across the board to figure out where our vulnerabilities are. As they conduct that probe, our electoral systems are one of the things that they are analyzing.

So, in line with that I want to get a sense of, when you are working with local and State actors, who are you talking to? Is it the Terrorism Task Force, is it the Fusion Center, is the secretary of state, is it the Governor, is the law enforcement entities? If it is all of the above, how do you do that and what systems are in place to coordinate that type of multifaceted action?

Mr. KREBS. It is all of the above and even more, the Homeland Security advisers and Adjutant Generals and things of that nature. My team, the Cyber Infrastructure Security Agency, which you rightly point out, this election security issue is not just about cybersecurity threats, there are also physical securities threats, there are insider threat, their access to machines, manipulation to machines on device that we need to be thinking about. So, we approach this as a cyber and physical security.

But, more broadly, form a counterterrorism perspective—the thing I have learned over the last couple years is that secretaries of state are their natural risk managers. They have to plan for the hurricane. Look at what happened in the panhandle of Florida in the last election cycle. They have got to anticipate any nature of threat, and so, as we work through, we do active-shooter training and those sorts of activities.

We have mechanisms in place, including, my team has over 140 security advisers out in the field that work day in, day out with infrastructure owner/operators, with these officials, they conduct training, they do walk-throughs, they do security facility assessments to—in a lot of cases they provide reports back to the facility owner/operator with suggested improvements.

Mr. ROSE. So, but just to push you for a second on this, my understanding then is that there—you don't have an entity that you are reaching out to, to coordinate this at the State and regional level. That it is incumbent upon you all, with these 140 folks, to be reaching out to all of these local entities and it seems, from our perspective, that this is rather disparate.

Mr. KREBS. So, specific to elections, we have developed communications protocols after some of the missteps of the 2016—post-2016 notifications where we have a coordination protocol, where we work with the State—the chief election official, the homeland security advisers, and so that is typically our point of entry for—specific to elections.

Mr. ROSE. OK, it would be great to see that.

Mr. KREBS. Yes, sir.

Mr. ROSE. Then just last, at the Federal level, you mentioned that you have convening responsibility, but who is actually in charge of this interagency process? Who's at the head of the table when all these folks are gathered together and who has that statutory authority to actually make sure that we are getting the job done here?

Mr. KREBS. So, there are a couple different levels of this conversation. There is a policy coordination piece that the National Security Council, Ambassador Bolton leads. There have been a number of convening meetings and what-not, all the way up to the principle committee meetings with the President.

Then at the operational level, there is a working group that brings together the Department of Defense, the EAC is involved, the DNI.

Mr. ROSE. Are you in charge of the working group?

Mr. KREBS. Am I? No, sir. I am in charge of the cybersecurity expertise and technical support to election officials, that is my role.

Mr. ROSE. Who would be in charge of the working group?

Mr. KREBS. There are a range of responsibilities and there is law enforcement actions, that is naturally the FBI, there is intelligence assessments, that is naturally the Director of National Intelligence, there is the cybersecurity piece, that is me. This again goes to the whole-of-Nation, the whole-of-Government approach. There is no one agency that has all of the tools and capabilities that are needed to push back on this.

Mr. ROSE. OK, all right. Thank you. I yield back my times.

Chairman THOMPSON. Thank you very much. The Chair now recognizes the gentleman from Texas, Mr. Crenshaw.

Mr. CRENSHAW. Thank you, Mr. Chairman and thank you both for being here. I am pleased that this committee is meeting to discuss the integrity of our elections and how to strengthen the cybersecurity of our election infrastructure.

I will say, that election integrity is multifaceted, there is a lot of aspects to it. It is not just the cyber side, but it is also the voter fraud side, including voter I.D. laws and how to prevent fraud by vote by mail.

I would say it is unfortunate that this is not a mark-up process and it is also unfortunate that this part of the bill, which I think we could reasonably come to a bipartisan solution on, is attached to a much larger bill that is poisonous and will certainly not make it past the Senate.

I want to ask you both, could you clarify what role you had in crafting this particular legislation?

Mr. KREBS. So, in the last Congress we certainly provided technical assistance on aspects that got rolled into it, but suggestions on what DHS needs, what DHS does.

Mr. CRENSHAW. OK.

Mr. HICKS. I spent 11 years as a House staffer. If the committee wants to come and ask my opinion, I am more than willing to give it.

Mr. CRENSHAW. OK, but you were not consulted prior to this hearing on what should be in this section of the bill?

Mr. HICKS. The committee—Chairman Thompson and then-Chairman Brady invited me to speak before their Task Force and I gave input there on various aspects.

Mr. CRENSHAW. Is there anything missing from this section of the bill that would you recommend go in it? Are there new authorities or capabilities that—and I think this is directed to you, Director Krebs, that DHS would need that are currently not in it?

Mr. KREBS. So at this point, again, I think the Department has, generally speaking, the authorities we need to engage and support the election officials.

Mr. CRENSHAW. One of the key provisions in this bill, it includes the expiration date on funds. It is asking us to spend a lot more money very rapidly; I want to get a sense of how realistic that is from you all. Given the slow pace of upgrading election infrastructure, do you think that States would need more time and flexibility on this, given your experience working with them?

Mr. HICKS. I believe that the Chairman had talked about that this would go over for 10 years and in that cycle there would be 5 Federal elections, allowing for States to make improvements overall.

If the—I believe that the provision was put in there because of the original HAVA provisions that allowed States to use those funds in perpetuity. So this gives them a deadline to actually spend the money similar to the 2018 provision, which only allowed for 5 years.

Mr. CRENSHAW. Do you have anything to add?

Mr. KREBS. Sir, our role is to help the election officials spend the money in the most risk-based and security-formed manner.

Mr. CRENSHAW. Thank you gentleman, I yield.

Chairman THOMPSON. Thank you very much. The Chair now recognizes the gentlelady from Illinois, Ms. Underwood.

Ms. UNDERWOOD. Thank you Chairman Thompson for calling this important hearing, and it is a hearing that central to protecting our democracy and I thank the witnesses for testimony here today. My own State of Illinois was a target during the 2016 Presidential elections where the information of the 76,000 Illinoisans were compromised by Russian hackers.

So while I am relieved to hear from you that there are no known harms that were caused in 2018's midterm elections by nation-state actors, for me, and I think those on this panel it is critical that State, Federal, and local governments continue to collaborate to strengthen election security and landscape of these ever-evolving threats. Now my colleague Congresswoman Slotkin pursued a line of questioning with you regarding social media and some of the threats that you all have recognized.

My follow-up question, at the end of your response sir, Mr. Krebs, is that you said that the enemy was changing tactics and so what should we be looking for in 2020 to ensure that we are continuing preparedness particularly at the State and local levels?

Mr. KREBS. That is exactly the question, what do we need to be prepared for? We have a habit of defending against the last attack, and so we can close out the last avenue of attack, we can patch vulnerabilities, we can configure systems more security. But if we have seen anything, the adversary gets ahead of us, anticipates.

So what we are working through right now is what could an advanced actor do? I—this is a personal perspective, but I tend to think that they could look back and exploit, hey, we were in that system—we are in there again. But they might not really be there.

Ms. UNDERWOOD. Right.

Mr. KREBS. So they—and one way to look at it is the Russians in some cases are living rent-free in our heads, and so how are they going to take that to their advantage without actually being on-network, but using their media—social media tools, their influence campaigns. So staying ahead of them and their ability to spread false information—it is working with social media, it is working with the traditional media in a content-neutral way.

But getting ahead and anticipating the things they may try to push, but most importantly and this again goes to that whole-of-Nation approach. What can we do to better inform the American people of the risks that are being presented to them and information that is being presented, again to make them more informed consumers?

Ms. UNDERWOOD. More concretely then, you perceive social media to continue to be a significant threat heading in to 2020?

Mr. KREBS. I see from a cost——

Ms. UNDERWOOD. OK.

Mr. KREBS. Effectiveness and risk perspective, that is probably—it is cheap to do, it is highly effective in terms of broad impact, and it is comparatively low-risk compared to on-network activity. So I think that it is going to remain a tool in their toolkit, they continue to do it to this day. What is most concerning is more actors, including the Iranians and others are getting in to that game, following the lead of the Russians.

Ms. UNDERWOOD. Sure. One of the trends that we have seen, at least in Illinois is the rise in popularity of early voting, taking advantage of vote by mail or, as we call it, vote at home. So wondering about any specific threats obviously social media is probably less relevant in that stage of voting in an election, so just wondering if you had any specific threats that you might want to make this committee aware of?

Mr. KREBS. I am not aware of any specific threats to early voting, the thing I will note though is early voting provides us earlier opportunities to spot anomalies through the auditing process and other security fall-back measures. So in some cases, it actually advantages the defender.

Ms. UNDERWOOD. In your experience every jurisdiction is engaging in that auditing process throughout the early vote period?

Mr. KREBS. I am not sure I have enough information to say that conclusively.

Ms. UNDERWOOD. Where would we go to find that out?

Mr. KREBS. In part, we would need to work with EAC through some of their mechanisms.

Ms. UNDERWOOD. OK, thank you so much. I yield back, sir.

Chairman THOMPSON. Thank you very much. The Chair now recognizes the other gentlemen from Mississippi, Mr. Guest.

Mr. GUEST. Thank you, Mr. Chairman. I will follow up a little bit to what Congressman Taylor had talked about earlier. In section 3001 of this act it says that it amends the Help America Vote

Act of 2002, to create a grant program for States to replace current voting machines with paper ballot systems, for security improvements before the 2020 general Federal election. Mr. Krebs, do you know what percentage of voting systems would have to be replaced to meet that requirement?

Mr. KREBS. Specifically no, but I know that 5 States and—83 percent of another very large State need to go through that process.

Mr. GUEST. So would the other 45 or 44 and a percentage of the State that is not in compliance—would those current voting systems comply with what we are seeking to do here?

Mr. KREBS. I would have to do a little bit deeper research on there, but I do know that of those other States that may be nominally in compliance, there are still legacy machines that are outdated and some of them may not be supported by the vendor. It is a good thing to refresh and retire legacy systems.

Mr. GUEST. OK, but as far as a percentage of systems that would need to be replaced, you do not have a percentage to give us today?

Mr. KREBS. Not—not with me sir, I would have to work with the——

Mr. GUEST. Mr. Hicks, do you have any idea?

Mr. HICKS. I could talk to our staff to figure out what the exact percentage is, but I don't have a direct percentage right now.

Mr. GUEST. Do you have an estimate on the cost to comply with section 3001, Mr. Krebs?

Mr. KREBS. No, sir.

Mr. GUEST. Mr. Hicks.

Mr. HICKS. The earlier testimony before the Senate Rules Committee, that question was asked about replacing aging voting equipment in non-compliance would be in this bill, I believe that to be between $500 million and $1 billion.

Mr. GUEST. I know there was previous testimony that at least 45 States currently used paper ballots—and this may have been testified to earlier and I may have missed it—outside of Georgia what were the other 4 States that do not currently use paper ballots?

Mr. HICKS. South Carolina, Louisiana, I believe New Jersey—and I would have to get the rest of that—and Delaware, yes.

Mr. GUEST. Then Mr. Krebs you said that there was another State that was partially in compliance with using paper ballots——

Mr. KREBS. Pennsylvania——

Mr. GUEST. Pennsylvania.

Mr. KREBS. Yes, sir.

Mr. GUEST. What percentage of Pennsylvania did you say does not currently use paper ballots?

Mr. KREBS. I would have to get back to your with specifics, it is somewhere around the 80 percent number. I will note that all 5 States that are—don't have paper trails right now, and the State of Pennsylvania are all on a path toward voter verifiable paper trail. These are good things, this is a good trend.

Mr. GUEST. Of those States that we have just talked about that are on that path, do we have any idea as to whether or not they will have paper ballots for the 2020 election cycle?

Mr. HICKS. I would—I don't know if all 5 of those will be but I know that they are on that path to comply with that. But I would also say that whatever path they take to ensure that those folks who have disabilities can still vote independently and privately as prescribed by the law in the Help America Vote Act.

Mr. GUEST. Then finally, Mr. Krebs, in your report on page 6 you say that our voting infrastructure is diverse subject to local control and has many checks and balances. Do you believe, Mr. Krebs, that elections should remain under local control?

Mr. KREBS. Yes, sir.

Mr. GUEST. Do you—do you Mr. Hicks, do you also believe elections should remain under local control?

Mr. HICKS. States and localities are the ones that run elections.

Mr. GUEST. Thank you. I yield back Mr. Chair.

Chairman THOMPSON. Thank you very much. The Chair now recognizes the gentleman from Texas, Mr. Green.

Mr. GREEN of Texas. Thank you Mr. Chairman. Thank you for your leadership and allowing me to serve on this committee under our leadership. I am a person who loves his country and I love my State but I have heard this 10th Amendment argument before. Lonnie Smith was a dentist in Houston, Texas. He wanted to vote and there was a white primary. *Smith* versus *Allwright,* 1944, went to the Supreme Court of the United States of America. Lonnie Smith prevailed; that ended white primaries.

The 10th Amendment argument has been used consistently by some States who deny rights. Texas is one such State. I love my State but Texas has been a bad actor for decades. I love my State. My State currently has a poll tax in contravention of the 24th Amendment to the Constitution of the United States of America. Talk about this photo I.D. and we will give you an I.D. if you can't afford it, if you are indigent.

Well I tested that system and voted without my proper I.D. and had some time to secure the proper I.D. The State of Texas will accord you an I.D. at no cost if you are from Texas because in my case I am from Louisiana. I had to get my birth certificate from Louisiana to get my I.D. in Texas and I had to pay a fee for that; clever ways to disenfranchise.

So I thank God for the Federal Government and the stand that has been taken over the years to protect the rights of people in States. I don't think that is in contravention of the 10th Amendment.

Now, to my question, you said Mr. Hicks that the States are moving toward some sort of paper component, I believe is the phraseology that you utilized. Paper trail is what people at my level of life would probably say, "Why are they doing that?" What is the rationale for moving to paper verification?

Mr. HICKS. It is a little bit of two things. One, I believe it is confidence to ensure that the—if there is an audit being done that there is some sort of physical trail that people can point to and do a physical count of that. The other is I believe just moving back toward confidence as well.

Mr. GREEN of Texas. Confidence and the level of confidence that we aspire or that we desire to have, is that one that would give us a belief that if there has been some sort of intervention, we will be able to detect it and that paper—verifiable paper may be of assistance?

Mr. HICKS. There could be.

Mr. GREEN of Texas. If this is the case that verifiable assistance by way of paper is something that is of value, can you give me a good reason why we would oppose having verifiable paper given that States are moving toward it and given if there is some value in it, why would we oppose it? What is a good reason to desire a system that doesn't have this type of verification?

Mr. HICKS. The biggest reason that I have heard over the years is those folks who have disabilities who may not have the dexterity functions to handle that paper and to verify it. So if I am without sight, I can't verify a piece of paper physically. I think the technology is moving toward allowing folks who have sight disabilities to be able to verify that but they still would have to physically use that paper. I believe that we have come a long way since the 2000 election in terms of technology and moving forward.

For instance back in 2000, everyone in this room probably has a smart phone. No one had those issues. So as we move forward with technology to allow for people to cast their ballots and so forth, the other aspect of that is people who live overseas and are in combat areas where they might not have access to a fax machine to fax that back or the ability to get that piece of paper back. But to ensure that our military and overseas folks still have a way to cast their ballots for the rights they are defending for us all.

Mr. GREEN of Texas. Thank you. Persons who need assistance in polling places, we currently allow that. If you need some sort of—if you are visually impaired we allow you to be assisted and there are ways to deal with our military personnel in foreign places, distant places. The empirical evidence seems to indicate that there is more value in having it than not. Is that a fair statement?

Mr. HICKS. Yes.

Mr. GREEN of Texas. All right, thank you Mr. Chairman. I yield back.

Chairman THOMPSON. Thank you very much. The Chair now recognizes the gentlelady from Florida who comes from a State that has some minor experience in voting issues. Mrs. Demings.

Mrs. DEMINGS. Thank you so much, Mr. Chairman and thank you again to our witnesses for being here with us. Everybody in this room clearly understands the deep, dark, ugly history that our great Nation has as it pertains to voter suppression and I would think that this committee would lead the effort in making sure that we have a system that allows citizens of this country to be able to exercise their right to vote. That I would believe in this country that we would ensure that race, gender, economic status, or ZIP code would never again be—to a person's right to vote. So I want to thank you—the two of you for what you do to make our process fair.

I am from Florida and let me just say I am not offended when Florida people all over this Nation question what in the heck is going on in Florida? I am not offended by it because I am committed to making sure that we get the process right. We can never underestimate the—how important the cooperation is between Federal, State, and local governments are to making sure that this process is right. In the November's election, 20 States, including my home State of Florida, elected new Governors, and while several others elected or appointed new secretaries of state.

So as we prepare for the 2020 election and using what happened in 2016 kind of as a tool that we will not forget, looking at the vulnerabilities and the experiences of 2016, I will ask both of you, what outreach have you participated in to secretaries of state, to new executive officers or Governors to make sure that they are prepared for the 2020 process?

Mr. HICKS. Thank you, Congresswoman. That is a great question. We work very closely with the National Association of Secretaries of State, and I actually participated in their winter conference 2 weeks ago, where I met several of the new secretaries myself. We also work with the National Association of State Election Directors who also had their conference a couple of weeks ago, here in the District of Columbia, where I have met several of those new folks.

We work very closely with them to find out what sort of assistance the EAC can have. In 2018, we held a summit in—at the National Press Club where it was well attended, broadcast on C–SPAN, where we talked to people about preparing for the 2018 election.

One month before the 2018 election, in October we held a—another summit in the Congressional Visitor's Center where Members of Congress and others were able to kick the tires on voting machines, and hear from election officials, themselves, about how they were preparing for the election coming up.

I believe that the EAC is looking to hold additional forums this year, and next year, with disability groups, and State election officials, and others so that we can continue our partnership. I believe that we have come a long way from when folks were not looking favorably upon the EAC. I would ask that you talk to—or ask the question to the secretaries of state.

I might be a little worried about this, but—about how we are doing, and move forward. There are other things that we can do to improve the process. But at the end of the day, this is a partnership where we hope to do what is best for the American people, and ensure that the confidence remains high.

I journeyed to your State in—in December to go down to Bay County and talk to folks, and find out what actually happened, and how they prepared for the election, since they were—things were destroyed. They were cleaning out voting equipment with toothbrushes, basically. But they still pulled the election off. We want to be able to provide them resources, not just monetarily, but advice on how to prepare for 2020, and moving forward.

Mrs. DEMINGS. Thank you. Director Krebs.

Mr. KREBS. Briefly, I have the advantage of having a field force, 140 folks out in field. Their top priority, as these new secretaries were being sworn in, was to get meetings on the books. Unfortunately, some of those meetings were disrupted by the shutdown. But those are back on the books. We are engaging full speed ahead.

Mrs. DEMINGS. Great. Thank you so much. Mr. Chairman, I yield back.

Chairman THOMPSON. Thank you very much. The Chair now recognizes the gentleman from Missouri, Reverend Cleaver.

Mr. CLEAVER. Thank you, Mr. Chairman, thank you for being here today. I—this is not a trick question, but I would like for both of you, if you could answer the question. Do you think that we have an election process that is equal in this country?

Mr. KREBS. I am sorry. Could you repeat the question?

Mr. CLEAVER. Is the—are the elections in the United States of America equal? If we have a Presidential election, are all votes equal?

Mr. HICKS. One person, one vote. So every vote counts equally.

Mr. CLEAVER. Yes.

Mr. KREBS. I would agree with that.

Mr. CLEAVER. Would you agree with that?

Mr. KREBS. Yes, sir.

Mr. CLEAVER. So, everybody who votes should have equal access to the voting booth?

Mr. KREBS. Every eligible voter should have access to a ballot. Not necessarily going into a voting booth, as well. But have access——

Mr. CLEAVER. That is good. That is fine. That is OK.

Mr. KREBS. Yes sir.

Mr. CLEAVER. OK. I don't think—I don't think elections are equal. I think I can prove it rather easily. If you live in Oregon you can vote on Sundays. You can register all the way up to the election. If you are in South Carolina—and I even think Florida, you can vote on—on Souls to the Polls, where you vote on Sundays.

In Missouri you can't do that. In the neighboring State of Kansas, you can't do that. In Iowa you can't do that. So something is not right, in terms of having equal access to the ballot—I mean, to the voting precinct. Some people have a greater opportunity to vote—vote than others. Am I wrong or am I right? Thank you. No, go ahead.

Mr. HICKS. I was going to say that I believe that there—if Congress wants to give the EAC more direction on how to improve the process, then we are more than willing to help it. I believe that States are moving toward early voting.

I believe that States are moving, with the $380 million, to refine voter registration processes. We will continually work with States to improve the process. The U.S. Postal Service does a great job, in terms of vote by mail. But I think there are other aspects that we all can improve upon.

Mr. CLEAVER. But you do understand that does some vote—some States fighting it?

Mr. HICKS. Yes.

Mr. CLEAVER. So am I right or am I wrong, Mr. Krebs?

Mr. KREBS. Sir, my job is regardless of the jurisdiction, whatever the—whatever the system is, that that vote is being cast and counted, and it is done in a secure and resilient manner.

Mr. CLEAVER. OK. I understand. I appreciate it. That is—I like that, a good American. OK, I will declare I am right.

[Laughter.]

Mr. CLEAVER. I think I can prove it, empirically, that we don't all have equal access to the voting booth. OK. The other thing—our conduct is always based on cost. We do something, there is a cost to it, or for the most part there is a cost to everything.

I am wondering, we all have been told by our intelligence agencies that Vladimir Putin ordered interference with our elections.

We have been—this is a direct quote, they will be back in 2020, FBI. In your opinion, Mr. Krebs, has—have the Russians paid a price for interfering with our elections?

Mr. KREBS. There has certainly been a significant amount of pressure and pain put upon the Putin administration, sanctions, other diplomatic actions, and a number of indictments against GRU actors. We will continue to push them, we will continue to defend.

My mission is to help State and local officials protect their networks, defend their networks and that is what we focus on every single day.

Mr. CLEAVER. Mr. Hicks.

Mr. HICKS. Our middle name is assistance and so we want to help as much as we can.

Mr. CLEAVER. OK. I am not sure that they—that they paid a high enough price for doing what they have done but my suggestion here is that they will come back again because the price wasn't high enough.

All those people who have been indicted, all they have to do to avoid going to jail is to—is never coming back to the United States or not being caught visiting another country with which we can have access to an arrest. Anyway, Mr. Chairman, I appreciate the opportunity. I yield back.

Chairman THOMPSON. Thank you very much. I thank the witnesses for their testimony. I now call up the second panel.

I welcome the second panel of witnesses. First I—let me thank all of you for being so patient. I woul like to welcome our California Secretary of State Alex Padilla to the panel.

Secretary Padilla has been a leading voice on election security and has done a number of innovative things in California to train up officials at the local level, raise public awareness about misinformation, and make the most of Federal partnerships.

Second we will hear from Noah Praetz. OK. There is an issue with a Mississippian and an Alabamian in pronunciation. Who until very recently served as the director of elections for Cook County, Illinois where he oversaw elections in one of the largest counties in the United States.

Third, I am excited to hear from Mr. Jake Braun, the executive director of the cyber policy initiative at the University of Chicago Harris School of Public Policy and also a co-founder of a DEFCON Voting Machine Hacking Village, the world's only public third-party inspection of voting equipment.

The research we have seen come out of DEFCON has been instrumental in helping us understand our vulnerabilities and help us move the conversation on election security forward.

Finally, I now recognize a Ranking Member Mr. Rogers to introduce Mr. Merrill, our minority witness today.

Mr. ROGERS. Yes, I am very happy to have Secretary Merrill with us today. He is in his second term as Alabama Secretary of State and is one of—if not one of, he is the hardest-working politician in Alabama. He has done such a fine job and I am happy to have him here with us today.

Chairman THOMPSON. Without objection, the witnesses' full statements will be inserted into the record. I will now ask each witness to summarize his statement for 5 minutes beginning with Mr. Padilla.

## STATEMENT OF ALEX PADILLA, SECRETARY OF STATE, CALIFORNIA

Mr. PADILLA. Thank you Mr. Chairman, Ranking Member Rogers, and Members of the committee. The defense of our Nation's elections must be a top priority for all of government; Federal, State, and local. After all, our democracy is under attack.

Elections officials have taken seriously the warnings from intelligence agencies. Our elections have been and will continue to be targeted by bad actors both foreign and domestic who seek to disrupt and undermine public confidence in our democracy.

We know these threats to be real because we see them every day. If we agree that defending the integrity of our elections is a matter of National security, then we must act accordingly.

Yet, despite the warnings and advice, our National response has been lacking. I have been to discuss what the Federal Government can do to help and to share what we are doing in California to better secure our elections.

I will begin by recognizing that both DHS Director Krebs and Senior Advisor Masterson are tremendously valuable partners. They have honored their commitment to timely communication with us when issues or concerns arise.

I will note that the importance of this partnership underscores the danger of unnecessary Government shutdowns. With the 2020 elections quickly approaching, our collaboration must not be interrupted. Now this partnership is only one component of a comprehensive defense strategy. We must also invest in election administration.

The last time Congress approved new funding for elections was 17 years ago through the Help America Vote Act. The investments made as a result were buying in large equipment and technology that are now 20 years old.

Today it is not uncommon for elections officials to be searching on-line for replacement parts for voting systems that are no longer supported by manufacturers. Others are stuck utilizing old operating systems that cannot be patched or updated with the latest security software.

So if we truly value our democracy, then we must commit consistent Federal funding for elections administration and security. Yes, Congress did appropriate $380 million last year in grants to States, but that wasn't new money, and it certainly wasn't enough. Last year's appropriation was the last of butterfly ballot, hanging chad, money that was never intended for modern-day cyber threats.

Next, Congress has the opportunity to make the best practices for election security the National standards. Among them, rigorous testing and certification of our voting systems, requiring logic and accuracy testing of systems before every election, requiring paper ballots and a voter-verified paper trail, requiring voting systems to be kept off-line and requiring post-election audits after every election.

This is a proven framework for securing elections and for improving voter confidence. You see, if a voter begins to think that their vote may not be counted or may not be counted as cast, and they choose to not participate in an election as a result of that doubt, that is a form of voter suppression.

Now these policies have served California well for years, but since 2016, we have done more. We have established these partnerships with DHS, FBI, the EAC, as well as State and local agencies, to better coordinate in the event of a threat or incident. We have engaged in security trainings, table-top exercises, and information sharing.

We have upgraded our State technology infrastructure and established an office of election cybersecurity and an office of enterprise risk management. We have dedicated staff to monitoring social media for erroneous information about voting. We have launched the public education campaign to raise awareness about election misinformation.

We have created a web portal with resources for voters, including the ability to verify their registration status, find their polling place and to report suspected misinformation. Finally, we piloted a voter status alert tool which notifies a voter whenever their voter registration record is updated.

We plan to deploy this tool State-wide, in time for the 2020 elections. Thankfully, the 2018 election went smoothly, but we know that those who seek to undermine our Democracy will continue to try with increased frequency and sophistication. It is not enough to keep up with nefarious actors; we must stay ahead.

This requires us to continue to work together, to implement the best standards, and to make the necessary investments. Thank you for this opportunity; I look forward to your questions.

[The prepared statement of Mr. Padilla follows:]

## Prepared Statement of Alex Padilla

February 12, 2019

Good morning and thank you Chairman Thompson, Ranking Member Rogers, and Members of the committee for the opportunity to be before you today.

And thank you for convening this hearing to discuss our Nation's election security readiness. For me, and for my colleagues in State and local government, this conversation could not be any more urgent.

The defense of our Nation's election systems and infrastructure must be a top priority for all of government—Federal, State, and local. After all, our democracy is under attack.

Elections officials throughout the Nation have taken seriously the warnings we have received from Federal intelligence agencies—that our elections have been and will continue to be a target for bad actors, foreign and domestic, who seek to disrupt our democratic process and undermine public confidence in our elections.

Elections officials know these threats to be true, because we see them every day. For example, in California, our internet-facing systems are pinged or scanned constantly. This activity is the equivalent of someone walking through a neighborhood, checking doorknobs, looking for unlocked doors. While these are not hacks or breaches, those conducting this unauthorized activity certainly have intentions.

If we agree that the integrity of our elections is a matter of National security, then we must act accordingly and recognize that elections officials are on the front lines. We are the first responders to attacks on our democracy.

Yet despite consistent warnings and evidence, our National response is severely lacking.

Most critically, we must rethink how we fund and administer elections.

In my testimony today, I will discuss what the Federal Government can do to further support States and local jurisdictions, and I will share what we are doing in California to better secure our elections.

I want to start by saying that DHS Director Chris Krebs and DHS Senior Advisor Matt Masterson have become tremendously valuable partners. They have demonstrated their commitment to quality and timely communication and coordination with State and local elections officials when issues or concerns arise.

When potential threat information has surfaced, they have reached out to us. When we read or hear of new threats, they are there to inform us of potential exposure.

The importance of this partnership underscores the danger of unnecessary Government shutdowns. During the recent shutdown, secretaries across the Nation were notified that email responses and phone contact with DHS personnel would be suspended or delayed. As the 2020 election cycle is already ramping up, we cannot afford to lose critical contact with our Federal partners.

Partnership with DHS and other National security agencies is only one necessary component of a comprehensive defense strategy.

Let's be honest, elections are underfunded and are too often a low priority for Federal, State, and local governments. The last time Congress approved new funding for elections was through the Help America Vote Act (HAVA), 17 years ago, in the wake of the 2000 Presidential election. And the investments made as a result of HAVA were by and large in equipment and technology that is now 20 years old.

Members of the committee, you would not settle for 20-year-old technology and reliability on your cell phones; our voting systems should be no different.

The lack of sustained investment has resulted in outdated election infrastructure and understaffed elections offices. Across the country there are many elections officials in counties with small populations—and therefore small budgets—that don't even have their own IT staff.

In addition to being outdated, voting equipment in many jurisdictions is at or beyond life expectancy. As we meet here today, there are some elections officials searching on eBay for replacement parts for systems that are no longer supported by manufacturers. Others are utilizing operating systems that are so old, their vendor no longer provides tech support—meaning some voting machines cannot be patched or updated with the latest security software.

Simply put, too many elections officials are ill-equipped to defend against 21st Century threats.

We often say that our budgets are a reflection of our values.

If we genuinely value our democracy, then we must commit consistent Federal support for election security and administration.

Members of the committee, respectfully, last year's appropriation of $380 million in cybersecurity grants to States was not new money, and it certainly was not enough. The $380 million was simply the final appropriation of HAVA funds. That was the last of the butterfly ballot and hanging chad money. That was not 2016, 2018, or 2020 cyber threat funding.

In addition to funding, Congress also has a tremendous opportunity to make the proven best practices for election security the National standard.

Among them:

- Rigorous testing and certification of voting systems with up-to-date security standards;
- Requiring testing of voting systems for logic and accuracy before every election;
- Paper ballots and a voter-verified paper trail, for auditing, recount, and manual tally purposes;
- Keeping elections infrastructure off-line;
- Post-election audits after every election.

I suggest to you that this is the proven framework for better securing our elections as well as improving voter confidence. Deficiencies in our election security infrastructure can jeopardize public confidence in our democracy. If voters begin to think that their vote may not be counted, or may not be counted as cast, and they decide to not participate in an election as a result of that doubt, that is a form of voter suppression.

These are just some of the best practices that have served California well since long before the 2016 election.

And in response to the 2016 election, we doubled down on our efforts.

We established intergovernmental partnerships with the U.S. Department of Homeland Security, the Federal Bureau of Investigation, the Elections Assistance Commission, the California Department of Technology, the California Office of Emergency Services, the California Highway Patrol, and county governments to ensure coordinated responses to cyber threats and incidents.

My office has engaged local elections officials in cybersecurity trainings, table-top exercises, and information sharing. And I personally visited fusion centers in all regions of California to better position ourselves to coordinate in the event of a threat or incident.

We upgraded our technology infrastructure and established both an Office of Election Cybersecurity and an Office of Enterprise Risk Management within our agency.

Another lesson I've taken to heart is that your technology is only as strong as the staff that uses it. Cybersecurity tools are just that, tools—tools for our staff to utilize. This is why we have invested in specialized staff dedicated to cybersecurity and trainings for elections staff at the State level and with our local partners.

As part of our strategies in the new Office of Election Cybersecurity, last fall we launched "VoteSure," a first of its kind in the Nation public education campaign to increase voter awareness about election misinformation on-line and to promote official, trusted election resources. The campaign included the launch of a new web portal with a variety of tools and resources for voters including the ability to verify registration status before going to vote, reliable polling place look-up tools, and a dedicated email address for voters to report suspected misinformation. And in a first-in-State history effort, we emailed official election information and resources directly to voters.

In the days leading up to the 2018 General Election, our staff identified nearly 300 Facebook posts and Tweets with inaccurate and misleading information about the voting process. We reported them to their respective social media companies for review. Ninety-eight percent of the posts and tweets we reported were promptly removed by their respective platforms for not meeting their standards.

Our office also piloted a new voter status email alert program in 7 counties—Madera, Napa, Orange, Sacramento, San Mateo, San Bernardino, and Solano—for the 2018 General Election.

This new system automatically notifies voters whenever we have received a new registration or update to their registration record through our on-line voter registration website or a paper voter registration form. We plan to expand the program State-wide ahead of the 2020 elections.

California's share of last year's HAVA appropriation was $34 million. Funds in the current year's budget is helping counties with costs of upgrading security of their connection to our State-wide centralized voter registration database, known as VoteCal, and polling place accessibility.

At the State level, we are using a portion of the funds for:

- Support of county efforts associated with cybersecurity risks and infrastructure needs related to the State-wide voter registration system, including important activities such as security assessments, penetration testing, and staff training.
- Support for county improvement of polling place accessibility and administration of elections.
- Support for county vote center implementation, which includes costs associated with new voting technology like ballot on demand, electronic pollbooks, remote accessible vote by mail systems and voting systems.
- Enhancements to VoteCal State-wide voter registration system.
- Development of security training curriculum and training of counties.
- Support and guidance for counties implementing risk limiting audits.

By all accounts, 2018 was a success. In California, voters responded with record-high voter registration and the highest voter turnout in a midterm election since 1982. And the election went as smooth as we could have hoped for.

But, the threats to our elections are ever-evolving. And those who seek to undermine our democracy will increase their efforts both in frequency and sophistication.

My colleague, Minnesota Secretary of State Steve Simon, puts it best, "Election cybersecurity is like running a race without a finish line." It's not enough to keep up with nefarious actors who seek to undermine our democracy, we need to stay ahead.

To do that, we must constantly be learning, scrutinizing, testing, and upgrading our security—and that requires Federal, State, and local entities to keep working together and to make the necessary investments.

Thank you again for your work to address these issues head on. I appreciate your leadership and look forward to answering your questions.

Chairman THOMPSON. Thank you very much. Next, we will hear from Mr. Praetz, who will—until very recently, served as the director of elections for Cook County, Illinois.

## STATEMENT OF NOAH PRAETZ, FORMER DIRECTOR OF ELECTIONS, COOK COUNTY, ILLINOIS

Mr. PRAETZ. Thank you, Chairman Thompson, Ranking Member Rogers, distinguished Members. My name is Noah, and I was director of elections in Cook County, Illinois. I speak to you from that experience today, and it is a real honor to do so.

You know, when election officials certify results, they bestow, not just power, but legitimacy that comes from the essential American belief that our elections reflect a trusted and true accounting of the votes. We secure that legitimacy by protecting two—two virtues, truth and trust, along two different fronts, infrastructure and information.

Truth can be protected with policies and practices that ensure a fair and accurate account. Trust is protected by continuing to deliver services to our voters as expected. Election officials have been security votes in voter records for a very long time. When I started, prior to 2000, we served mostly as logistics managers—kind-of like wedding planners making sure the right list of people came together at the right place with the right stuff.

After *Bush* v. *Gore,* a whole new era was foisted on us with voting technology, new rules—and we become I.T. managers. Now, since 2016, we must become cybersecurity managers. Spurred by the need to defend against foreign adversaries, Federal and State officials have been working very successfully to find a good balance of Federal involvement in elections, without trampling on authority that the States zealously guard.

State election officials who protect State-wide voter registration lists everywhere and more systems in some States and are often the spokespeople defending our institution deserve great credit, particularly their lead blocking in 2016, but also their leadership in the lead-up to 2018, when accepting the premise that we are a target and that we are vulnerable.

The Federal agency, led by Director Krebs and with Masterson's help, charged with providing direct support in this area, has also met the continuing demand for information and for services.

Election officials remain committed to the security effort even though there were no known impactful attacks against us in 2018, because we believe that good news is probably more a function of our adversaries not engaging than it is a result of our significant efforts over the last 2 years.

At the risk of being overly broad, I wish to underscore that local election officials are the ones who control, secure, and run elections. One hundred and eight in Illinois; and over 8,000 nationally are on the front lines. We deploy a variety of connected digital systems—poll books, voter registration systems, informational websites, election results websites, Election Day command centers, not to mention voting systems.

Each of these are a ripe target. Most local election officials are city or county officers, 2 or 3 people, and they are facing down shadowy, powerful adversaries; kind-of like Andy in Mayberry sent to repel an invading army. Locals need advice, support, and resources, for modern defendable technology and routine hand-counted audits, which can give confidence that the digital results are accurate.

But second, and I think more critically today, they have a pressing need for top-notch personnel with the skills to navigate the current cyber battlefield. In Cook County, we undertook significant efforts in securing the infrastructure and helping raise awareness within the ecosystem.

We concluded that, to decrease the likelihood of a successful attack, each local election official must have access to an election security officer. We suggested this be handled by a brigade of cyber-navigators, supporting local election officials. These navigators would adopt the mantra of defend, detect, recover.

They help improve defenses, following specific recommendations already out there from the Center for Internet Security or the Defending Digital Democracy program at Harvard. They establish breach detection techniques and they help develop recovery plans for when attackers do successfully penetrate the first or second line.

To accomplish this, navigators secure free support on offers from Homeland Security, State governments and companies like Google, Cloudflare, and Microsoft. They work with State and county I.T. staff, and critically, they will work with the deeply-embedded election vendors who are strategic partners that provide locals with much of their current support.

Incidentally, Illinois lawmakers spent the HAVA funds you released on a navigator program, with $7 million allocated to support each county, 108, more or less equally, with human expertise—9 navigators, each supporting about 12 counties and serving as their election security officer.

The remaining HAVA funds were to be spent with some recognition that bigger counties, like Cook County, are likely more high-value targets. Voters should feel broadly confident that we have resilient systems and that election officials are taking this problem very serious. But they should also understand that without continued investment, and people and products, the possibility of a successful attack increases.

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

The bottom line is we cannot eliminate every chance of breach. We can make sure that successful attacks are rare, and we can provide assurances that we are prepared to recover quickly when they happen. We do this with support at the local level. Thank you.

[The prepared statement of Mr. Praetz follows:]

## Prepared Statement of Noah Praetz

February 12, 2019

### BIOGRAPHY

Noah Praetz was the director of elections working under Cook County Clerk David Orr and then under Clerk Karen A. Yarbrough. He was responsible for the overall management of elections in Cook County, Illinois, one of the largest jurisdictions in the country serving 1.6 million voters.

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

Mr. Praetz currently runs an elections consulting practice. He teaches election law at DePaul University College of Law. He is an advisory board member at the University of Chicago's Cyber Initiative.

Mr. Praetz was on the executive committee of the Government Coordinating Council representing the local election officials as Homeland Security sought guidance on how best to support the election community. He was the treasurer of the International Association of Government Officials. He was also co-chair of the Election Center Cyber Security committee. He was active in the Illinois Association of County Clerks and Recorders. He has presented on election security, sustainability, election day management, on-line registration, voter registration modernization and other election-related items.

## EXECUTIVE SUMMARY

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

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

However, even as the community of election officials appreciate that election 2018 was free of any known incidents, they largely recognize that those successes are probably less a function of their efforts than they are a function of our Nation's adversaries' probable choice to hold back. The fundamentals of election security, and the investments neeeded to ensure improved security, have not changed since the summer of 2016.

Broadly, the fundamentals are these, local election officials are the ones who control, secure, and run elections. Locals—108 in Illinois and over 8,000 Nation-wide—are on the front lines of this new battlefield. Locals control almost the entire election infrastructure. Locals are the entities most in need of support and attention. Locals need help to fortify themselves, and our most important institution, against the high-probability threat actors they've been warned of. The States, with partnership from the Federal Government, are the entities that are now, and will continue to be, the leaders needed to support the security efforts to the local election officials.

While in Cook County we studied and undertook significant efforts at securing the infrastructure and helping raise awareness within the ecosystem. We concluded that to decrease the likelihood of successful attack on digital services, each local election official must have ready access to a savvy dedicated partner—an election infrastructure security officer. Most locals don't have that capacity today.

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

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

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

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

TESTIMONY

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

My name is Noah Praetz. Two weeks ago I stepped down as director of elections in Cook County, Illinois where I worked for Cook County Clerk David Orr, and recently Clerk Karen Yarbrough. I began my career in 2000 and during that time our office tried to lead on technology and security—using applied forensics in elections; creating widely-circulated cybersecurity checklists in advance of the 2016 elections; and publishing the first white paper written by election officials in the wake of the 2016 attacks. Recently, I helped the Center for Internet Security (CIS) adapt their digital security expertise to the unique context of elections and also spent a little time talking to the Defending Digital Democracy program at Harvard's Belfer Center (DDD). As co-chair of the Government Coordinating Council (GCC) that the Department of Homeland Security created to help address election security, I worked with Federal, State, and local leaders in elections, technology, intelligence, and law enforcement.

In the past 18 months I have testified before the U.S. Senate Rules and Administration committee once. On two occasions I testified before the United States Election Assistance Commission (EAC) and on two occasions I testified before Illinois legislative committees. I have presented before the numerous meetings of election officials from Illinois and from around the country. Every time, I strive to deliver the same message:

- The threats to election infrastructure are real.
- Elections are largely run and secured locally, so security efforts, let by the States and augmented by the Federal Government, need to be concentrated locally.

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

*Cybersecurity—One More Sword to Juggle*

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

Foreign governments, foreign non-state actors, and domestic troublemakers have the capacity and desire to corrode the essential public belief that our election outcomes are true and reliable. To very different degrees, this threat applies to both preliminary returns announced on election night and to official, final results. Beyond corrupting election results, the threat also reaches the large variety of systems used to run seamless elections.

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

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

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

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

*Elections are Secured Locally*

I have tremendous appreciation and respect for State election officials and their responsibilities and efforts. They are often the mouthpiece of our institution and responsible for managing the regulatory framework. For the past 16 years many have also managed their State's voter registration systems. In some States they take a far more active role in protecting other parts of the infrastructure. And it was States that were the named targets in 2016. But let there be no mistake—local election officials are on the front lines of this new battlefield: 108 in Illinois and over 8,000 Nationally. So, by and large, local election officials secure the Nation's election infrastructure. Locals install, store, monitor, test, deploy, run, and audit the voting machines and software. Locals install, store, monitor, test, deploy, run, and audit the electronic pollbooks. It is locals who manage warehouses, informational websites, voter databases, polling places, GIS Systems, results reporting systems, military voting systems, command centers, and the myriad digital services we rely upon in modern American elections. It is a local job to defend these systems, to institute controls that would detect breach, and to deploy mitigation strategies that can guarantee election processes and results that are trusted and true. It is their job to ensure recovery.

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

*Cook County Efforts*

Since the summer of 2016 we stepped up our efforts to protect ourselves and to protect the broader ecosystem: We introduced additional hand-counted audits to our State-mandated 5 percent machine re-tabulation. And we are pushing State legislation to add additional audits to election results—in the form of Risk-Limiting Audits.

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

We began installing new election equipment that will be easier to defend and will make detection and recovery significantly easier.

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

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

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

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

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

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

I co-chaired the newly-created Government Coordinating Council (GCC) set up with DHS to help drive Federal policy and resource allocation. I sit alongside the chairman of the Election Assistance Commission (EAC), the president of the National Association of Secretaries of State (NASS), the president of the National Association of State Election Directors (NASED), and from DHS deputy assistant secretary, Infrastructure Protection, National Protection and Programs Directorate (NPPD). In that role I tried to continually push for the advancement of local official's concerns.

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

*Coordinated Efforts*

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

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

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

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

*Increased Stable Investment & Short-Term Spending*

We have looked to our State and Federal funders and regulators to fortify locals on this battlefield. Given the costs of regular technology refreshes and support for human resources with cyber capacity, the needed investment is very large. And locals need a signal that they can invest now for security and not squirrel away recent money for some future episode.

Nevertheless, the recent investment is greatly appreciated. Congress just released $380 million to combat the election cybersecurity threat. And that is an important start. It may be necessary for the States, Federal Government, and locals to collectively invest that much annually. Meanwhile, Americans justly concerned about the costs need confidence this money will be spent well. In my mind there are two top priorities. First, a handful of States and counties still have paperless voting systems. These should be replaced as soon as possible.

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

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

*Illinois Approach*

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

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

These "Navigators" need to accomplish three vital goals. First, they should work to institute the election security framework—defend, detect, recover. They can help improve defenses within election offices, following the specific recommendations of CIS. We believe they'll quickly bring up the floor of the elections security ecosystem. Appropriately supported, we can see massive improvement very quickly. There is low-hanging fruit, but even low-hanging fruit needs to be plucked. They'll also work to support locals' efforts at instituting detection techniques and recovery plans. Second, the "Navigators" will do the work necessary to secure the free support being offered by public and private organizations, like the Department of Homeland Security, State resources, Google and Cloudflare, or the Elections Information Sharing & Analysis Center; they will also work with the outside vendors who provide much of the elections infrastructure and support to local officials. More importantly, they will help build a culture of security that adapts to the evolving threats we face through training and constant assessment efforts. Illinois' 108 local election offices will mature quickly with this reinforcement. As specific mitigations and upgrades are identified by Navigators, the State Board should be positioned to quickly provide that investment.

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

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

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

### *Supporting a Resilient Public*

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

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

Our public confidence is already weaker than it should be. Vacillating voting rights rules, no matter how marginal the effect, are disconcerting to many people, naturally suspect given our history. Additionally, some media, activist groups and politicians have acted in ways that ultimately prey on Americans' insecurities about their most cherished institution, either through outlandish claims of fraud, or overstated claims of suppression. Such actions have done a disservice to the institution we serve and consequently to our ability to bestow not just victory, but legitimacy. We must be very careful to calculate not just the relative effects on power that election rule changes can have, but also the relative effects on legitimacy. Or put another way—will losers be more or less likely to accept that they lost fairly.

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

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

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

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

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

## ATTACHMENT.—WHITE PAPER

### 2020 VISION: ELECTION SECURITY IN THE AGE OF COMMITTED FOREIGN THREATS

*Sponsored by: Cook County Clerk David Orr*

*Authored by: Noah Praetz, Director of Elections*

*December 2017*

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

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

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

### *Policymakers and funders must act now to ensure election security*

The new security mantra for local election officials is "defend, detect, recover."

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

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

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

### RESPONSIBILITIES OF POLICY MAKERS AND FUNDERS

### *Defend*

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

1. Supporting a digital network for all local election officials that will facilitate rapid sharing of threats and incidents, as well as supporting increased training and resiliency;
2. Financing an Election Infrastructure and Information Security Officer (EIISO) (or consultant) servicing every local and State election official in the country;

3. Ensuring that threat and incident information known to Government is shared appropriately throughout the election ecosystem.

*Detect*

Increase the catastrophic breach detection capacity by incentivizing:

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

*Recover*

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

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

### POTENTIAL APPROACH FOR ELECTION OFFICIALS AND THEIR ELECTION INFRASTRUCTURE AND INFORMATION SECURITY OFFICER

*Defend*

- Get experts into the office. Engage outside cybersecurity resources & professionals. No election offices can handle this problem on their own. Inside most elections offices, there simply is not the complete capacity to accept the threat, assess the vulnerability, digest recommendations, manage mitigations, and perfect recovery.
  - Utilize as many free local, State, and Federal (DHS, CIS, and MS–ISAC) tools as possible.
    - If Government resources are unavailable, or underwhelming, hire private firms or partner with academic institutions.
  - Collaborate with resources inside local, State, and Federal Government because we are not alone in facing this type of threat include the fusion centers.
  - Bring in outside resources to partner with information technology and information security teams, with a focus solely on election security.
    - The reality is that most election officials share their internal information technology and security resources with every other county office engaged in critical activities, such as health and public safety. It can be nearly impossible to get the attention necessary for election security unless it is the primary focus of those resources.
- Understand and limit the threat surface area; or all possible points of vulnerability for malicious attack.
- Inventory all election-related systems: e.g. voting machine and vote counting system; e-pollbook system; voter registration/election management system; mail ballot delivery and processing system; and on-line systems such as voter registration, mail ballot request tools, voter information look-up.
- Map how systems work and data flows, and mark every single point of vulnerability.
- Limit the threat surface area by making policy decisions that reduce points of vulnerability wherever possible (this is about managing risk, not eliminating it.)
- Employ defense tactics and policies for each system—on-line or not.
  - Implement the Center for Internet Security's top 20 cyber controls. Do the top 5 first. These include:

    1. Inventory of Authorized and Unauthorized Devices; 2. Inventory of Authorized and Unauthorized Software; 3. Secure Configurations for Hardware and Software; 4. Continuous Vulnerability Assessment and Remediation; 5. Controlled Use of Administrative Privileges; 6. Maintenance, Monitoring, and Analysis of Audit Logs; 7. Email and Web Browser Protections; 8. Malware Defenses; 9. Limitation and Control of Network Ports; 10. Data Recovery Capability; 11. Secure Configurations for Network Devices; 12. Boundary Defense; 13. Data Protection; 14. Controlled Access Based on the Need to Know; 15. Wireless Access Control; 16. Account Monitoring and Control; 17. Security Skills Assessment and Appropriate Training to Fill Gaps; 18. Application Software Security; 19. Incident Response and Management; 20. Penetration Tests and Red Team Exercises.
  - Employ election system-specific defense and detection tactics across specific systems.
    - These can include all the hardening options that systems may have, such as locks, seals, chain of custody, advanced authentication, etc.

*Detect*

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

*Recover*

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

## LOCAL ELECTION OFFICIALS NEED SUPPORT

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

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

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

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

And so will faith in our democracy.

Chairman THOMPSON. Thank you very much. With much excitement, we have been anticipating Mr. Braun's testimony.

## STATEMENT OF JAKE BRAUN, EXECUTIVE DIRECTOR, CYBER POLICY INITIATIVE

Mr. BRAUN. Chairman Thompson, Ranking Member Rogers, and distinguished Members of the committee, thank you for the opportunity to speak to you today on this important issue. I also want to thank my co-panelists, Secretary Padilla, Noah Praetz, Secretary Merrill, they have led this Nation in securing elections and have become a model for other election officials around the country to follow.

So with that, I am Jake Braun. I am the executive director of the University of Chicago, Cyber Policy Initiative at the Harris School of Public Policy. I am neither a technologist nor an election administrator, however, I have been working this issue for about 15 years from 3, kind-of, distinct vantage points.

A few years ago, I worked on voter protection issues for multiple Presidential campaigns. Then, during my time at DHS I worked on this issue from both the Homeland and National security perspective.

Then most recently, I co-founded the DEF CON Voting Machine Hacking Village. DEF CON is the largest hacker conference in the world and the Voting Village, as we like to call it, is the only public, third-party assessment of voting equipment on the planet that we are aware of.

One thing that has become clear to us, clear to me, as I have worked on these issues from these different—very different perspectives over the years, is that this is a National security issue. This is not, kind-of, an election administration nuisance.

What I would argue that the committee is solving for here is, they are not solving for dangling chads, they are solving for: How do we stop an existential threat to the United States from undermining our elections? So let me give you a few kind-of key findings from the most recent DEF CONs that help elucidate that point.

So thing one, the supply chain for the equipment, both the software and the machines is global. Many of these parts are made in places—nations that are unfriendly to the United States, like China.

Hackers—nation-state hacks could put malware on firmware for these machines and other devices used to implement elections, and hack whole classes of machines all across the United States, all at once and never have to leave the Kremlin. That is not something that any local election official can be expected to deal with on their own. That is a National security issue and, therefore, Congress must act to support them.

Second, both DEF CON, the Senate Intelligence Committee, and OAS, which is the National—or global head of website security, have identified nearly identical threats to website attacks across the country. On top of that, as was stated previously in this hearing, there are multiple States that don't have paper trails, much less audits in place to re-engender trust if there was an attack on their elections. So it may be simply an attack on election reporting website that undermines trust in an election, especially in States like those without paper trails and audits.

On top of that, there has been reports since 2016 that Russia has actually hacked election results-reporting websites in the United

States already. On top of that, we know that Russia did this in the Ukraine, where they coupled their attacks on the election reporting websites with fake news they put out saying that their candidate had won, when, in fact, he had not.

This—all of this together, fighting back an onslaught of attacks from both the cyber and media perspective from a nation-state is something that no local election official can be expected to do. That is a National security threat and, therefore, Congress must act to help State and locals deal with it.

Finally, the cyber industry itself is—I mean, sorry—the election industry itself is cyber immature, as we may say. Meaning that, oftentimes, even when vulnerabilities are told to vendors, they don't get fixed.

For example, back in 2007 there was a vulnerability disclosed to a vendor and—for a specific machine. This machine is used in 23 States, counts millions of ballots in a National election, often thousands of ballots locally at a particular jurisdiction. We went back and looked at that same machine at DEF CON last year, and that same vulnerability still persisted. So over a decade later, the vulnerability's still not been fixed.

To be clear, the—the attack that was used on this machine is attack to be—could be carried out remotely by foreign hackers on foreign soil. It is an attack that can jump the erroneously-named air gap, and take over a machine completely to delete or add whatever types of votes you would want.

By the way, this all may sound very hard, however, most of these attacks were done by hackers that are generalists, with no previous access to the machines, no knowledge of the machines and no specialized training on how to attack these machines.

OK. So that is all the bad news but there is—there is a few good things to highlight here. One of those things is the security measures in this bill, they are very good.

I think that my colleagues have highlighted some incredibly important things like audits, paper trails, improving cyber hygiene, money to State and locals who desperate need it to improve their cyber hygiene posture.

But there is also a few other things; No. 1, there is money for R&D. The current state of the machines Nationally is such that they are essentially un-securable and we desperately need new machines around the country. However, the market for machines is such that the margins are so slim for the vendors that they will never be able to put the money needed into R&D to create machines of the future that can secure our elections. So Congress, thus, needs to help with that.

No. 2, there is a very innovative bug bounty program in there, which I think creatively helps solve the cyber work force problem, which is a very serious problem. Then, finally, there is vulnerability disclosure component to it.

So thank you very much. I am happy to answer any questions.

[The prepared statement of Mr. Braun follows:]

## PREPARED STATEMENT OF JAKE BRAUN

FEBRUARY 12, 2019

Chairman Thompson, Ranking Member Rogers, and distinguished Members of the committee, thank you for the opportunity to speak to you today on this important issue.

I would also like to thank my co-panelists, Secretary Padilla and Noah Praetz. They have led the Nation in securing their elections and have become a model for other election officials around the country to follow.

My name is Jake Braun and I am executive director for the Cyber Policy Initiative at the University of Chicago Harris School of Public Policy.

I am also co-founder of the DEF CON Voting Machine Hacking Village. DEF CON is the largest hacker conference in the world and the Voting Village is the only public, third-party inspection of voting equipment in the world, that we are aware of.

Moreover, for the last 2 years, I have worked with leaders in the National security establishment to release an annual report on the National security implications of our findings at DEF CON. The reports have won multiple awards and our efforts have been hailed by people as diverse as President Trump's former White House Cyber Czar, Rob Joyce; then-Chairman of the Cyber Caucus, Congressman Will Hurd; and Congresswoman Jackie Speier; as well as a bipartisan group of Senators from the Senate Select Committee on Intelligence, led by Senators Harris and Lankford.

The main question relevant for this committee is whether any of our findings are useful to the legislation you are now considering. The answer, in my estimation, is emphatically yes.

To that end, I have one overarching finding I want to highlight as well as a few key vulnerabilities which clarify the importance of the finding. Finally, I would humbly like to make a couple recommendations as to how these problems can be addressed.

The overarching finding is that attacks on our election infrastructure are NOT solely an election administration nuisance but rather a National security threat. Time and again this conclusion manifests itself in our research. This threat is not about how to eradicate hanging chads. This is about our National security apparatus marshalling its resources to do what our Nation expects it to do, which is protect our country from existential threats to the United States. A county clerk or secretary of state is not equipped to defend our democracy from nation-state hackers. These nation-state adversaries may attempt to change vote totals or they may simply try and erode our confidence in the integrity of American elections. Either way, this is a National security threat and thus Congress must act.

Let me give you a few examples of specific key findings that draw us to the conclusion that this is a National security threat:

1. The voting machine supply chain is global and parts are made in nations unfriendly to the United States, like China. If an adversary were to infect the firmware made at a plant in China or elsewhere, which we know has happened with other products, whole classes of voting machines could be hacked all at once on Election Day from the Kremlin. No election clerk or secretary of state alone can defend against these global supply chain issues. This is a National security threat and thus Congress must act.
2. Second, we have highlighted well-known vulnerabilities in websites. The global leader on website security, The Open Web Application Security Project (OWASP), and the 2018 report by the Senate Select Committee on Intelligence have highlighted similar threats to election websites. The bottom line is no one can defend a website from a determined nation-state actor. Just ask the top 25 banks in the country who collectively spend billions on security but failed to stop members of the Iranian Revolutionary Guard from attacking their websites consistently over the course of 2 years. Further, since 2016, the media has reported successful attacks on election websites in the United States by Russia. Russia also executed an attack against Ukraine's Central Election Commission website in 2014, rigging the website to announce the Russian-supported candidate won. Ukrainian officials detected the breach before the election results went live, but Russian media still erroneously named their candidate the winner. In U.S. States where there are no paper audits possible, hacking a website may be all that's necessary to cast doubt on an election's integrity. Moreover, no clerk or secretary of state alone can defend themselves against a multi-layered cyber and media campaign to cast doubt on the integrity of a National election. Rather, this is a National security threat and thus Congress must act.

> 3. Finally, perhaps the most disconcerting "flaw" we found is that vendors don't fix vulnerabilities when they are disclosed to them. A significant flaw with the M650 machine, which was used in 23 States as of 2018, was disclosed to the vendor in 2007. However, to our knowledge the vendor neither told its customers about the flaw nor did they fix the flaw at the time it was disclosed. Nor did they fix it after the 2016 elections when they supposedly started taking security much more seriously. Nor did they fix it, to our knowledge, after we pointed it out again at DEF CON in 2018. To be clear, this attack would allow an attacker, through a remote hack that could be carried out from abroad, to jump the so-called "air gap" and hack into a voting tabulator processing ballots for key counties in battleground States. This attack could flip the Electoral College and determine the outcome of a Presidential election. Obviously no clerk or secretary of state alone can defend against adversaries who can change large number of votes without needing physical or network access to the machines."
>
> Clearly, this is a National security threat and thus Congress must act.

One might think these attacks sound pretty hard to carry out. However, most of these attacks and dozens of others we found were carried out by generalists with no specialized training on election equipment or previous knowledge of the machines or networks.

Some have claimed that the setting at DEF CON does not represent a real election environment, thus diminishing the utility of our findings. However, as said at the outset, DEF CON is the only public, third-party inspection of election equipment, so it's the best we have for now. Further, as former White House Cyber Czar Rob Joyce, said, "We know our adversaries have a room just like the one at DEF CON." By which he meant that our adversaries are researching all the voting equipment we have and more because they don't have to get the machines legally, like we do at DEF CON. However, they aren't doing the research 3 days a year, they are doing it 365 days a year. They also don't disclose the vulnerabilities they find, like we do. Yet they are looking for the same flaws we are: Hacks that are quick, remote, and scalable.

So what can be done about these problems?

First, I would encourage you all to study the recommendations of a new report on election security from the National Academies of Sciences, Engineering, and Medicine. Their recommendations are comprehensive and sound.

Second, pass this bill. The measures in the H.R. 1 proposed legislation provide for auditable paper trails and local implementation of at least the top 5 of the 20 Critical Security Controls, as well as funding for cyber assessments and remediation. Congress must support State and local administrators' efforts by providing funding and assistance to implement cyber best practices that reduce America's vulnerability to these clear threats to our election infrastructure.

Finally, the election industry desperately needs funding for R&D to build voting equipment that can stand up to these modern threats. The current equipment is essentially unsecurable. The vendors will never have the enough money to fund the R&D necessary to develop equipment that can defend against nation-state attackers. H.R. 1 provides R&D funding for voting technology of the future, and I would strongly encourage the committee to keep that funding in whatever version hopefully passes.

Again, not solely an election administration nuisance but rather a National security threat. Thus Congress needs to act and fund a solution. I thank you for your efforts to pass this critically important legislation.

Chairman THOMPSON. Thank you very much for your testimony.

I now recognize, Mr. Merrill, to summarize his statement for 5 minutes—or do the best you can do.

## STATEMENT OF JOHN H. MERRILL, SECRETARY OF STATE, ALABAMA

Mr. MERRILL. Thank you, Mr. Chairman, I will. I appreciate that. I am honored to be with you. Ranking Member Rogers, thank you so much for the invitation to come and share with you all today.

I am John Merrill. For the last 4 years and 25 days, I have had the privilege to serve as Alabama's secretary of state. In our State, as in 35-plus other States in the Union, the secretary of state is the person that is responsible for the election system in that particular jurisdiction.

I think it is important for you to know some of the things we have done in Alabama and some of the thoughts of some of the people that I represent that have similar positions to the one that I hold.

As far as secretary of state's role is concerned; we have pre-election, Election Day, and post-election activities that we are responsible for. We coordinate all voter registration efforts in our State, we certify the ballots, we also monitor and enforce campaign finance laws at the State level.

We ensure participation in the election's process through awareness campaigns. We have Election Day and election night reporting systems that we have created and compile and certify election results. We also engage in partnerships with our public and private partners and independent partners in different ways.

We work with our county and municipal governments as well as Federal agencies when it is appropriate including but not limited to the election's systems commission, the Department of Justice, the National Guard, the Department of Homeland Security.

Our relationship with those entities has improved over the last 3 years since we had this type situation first introduced to us. In our preparation for the 2018 election cycle, we concentrated in the areas of cybersecurity, election integrity, which also includes enforcing the laws, and we use paper ballots in Alabama. We are going to continue to do that and by Federal law, anybody has to retain the Federal ballots for a period of not less than 2 years. That is the Federal law already. Voter confidence and voter participation is extraordinarily important.

Now we have heard a lot of different things today. But one of the things I think is so important for us to remember and to acknowledge and this has come from the Department of Homeland Security most recent report that there was no breach of any incident in the tabulation that occurred in the 2016 general election.

That has been researched, it has been documented, and no breach has occurred and no tabulation change occurred in any election in any State in the Union in the 2016 cycle. I also think that it is important to know that there is some serious concerns and issues with H.R. 1 in our opinion.

No. 1, significant Federal overreach has been indicated through the introduction of this legislation and it appears to provide certain things that need to be done but the lack of resources in order to be able to do those effectively.

So they are strictly underfunded or unfunded mandates. No. 2, there are many prescriptive requirements that have been indicated that States that would accept these funds would face significant difficulty in enacting those new programs without the resources necessary to do that.

They include but are not limited to some things that are already on-going in our State and other States in the Union, which are electronic poll books, paper ballots, automatic voter registration, audits, same-day registration. Those things are strictly prescribed that they need to be adhered to regardless of what the local jurisdiction would like to do. No. 3, the amount of time that the States have to meet the requirements is not something that is going to be able to be met.

One of the questions was asked earlier is that something that is going to be able to be adhered to and the answer to that question is no. If you want to know why it is because at the Federal level and at most State levels they move at the speed of Government and if you move at the speed of Government you know why it is not going to be done. You have to create RFPs and other things but we can talk about that later if you are interested.

As far as—the most important thing that I could share with you about a good election security bill, it would be one that would create the necessary resources to the States without creating unfunded or underfunded mandates and strangling restrictions that would introduce Federal overreach. I yield back the balance of my time.

[The prepared statement of Mr. Merrill follows:]

PREPARED STATEMENT OF JOHN H. MERRILL

FEBRUARY 13, 2019

My name is John Merrill, and I am Alabama's 53rd secretary of state.

Thank you for the opportunity to appear before you today to address how we, as the States' chief State election officials, work diligently each and every day in our State, and with our counties, municipalities, and other local jurisdictions to ensure we elect our leaders in free, fair, and accessible elections. This work can be complimented by effective partnerships at the Federal level, like those we have today with the Elections Assistance Commission (EAC), and the Department of Homeland Security (DHS), the National Guard, the Federal Bureau of Investigation (FBI), and other groups and associations like the National Association of Secretaries of State (NASS).

My goal as Alabama's 53rd secretary of state is to ensure that each and every eligible U.S. Citizen that is a resident of Alabama is registered to vote and receives a photo ID.

During my time as Alabama's secretary of state, my team and I have changed the paradigm for voting in the State of Alabama. Since I took office on January 19, 2015, we have worked with notable Alabamians, local officials, interested agencies, key communicators, and interested citizens to encourage voter registration and voter participation. The results are that we have registered 1,199,909 new voters, which brings our total number of registered voters to 3,473,030. Thirty of our 67 counties use electronic poll books, which expedites the check-in process and offers greater security for the voter and greater efficiencies and accountability for the poll worker. Our stated goal is to have electronic poll books in every county in the State by 2022. As a part of our efforts to ensure voter integrity, we have worked to secure 6 convictions of criminal activity related to voter fraud and will continue to document, investigate, and prosecute those individuals' intent on disrupting our democratic institutions for personal or political gain.

All of these efforts have helped our citizens become more involved and engaged in the process to elect officials that represent them in local, State, and Federal positions. We have broken every record in the history of the State for voter participation as Alabamians have turned out to vote in record numbers. In March 2016, we set a record for voter participation in a Presidential preference primary with 1.25 million Alabamians casting a ballot. In the General Election on November 8, 2016 with 2.1 million Alabamians casting a ballot. Alabama then broke the record for participation in a Special Election during the 2017 U.S. Senate Special Election, held on December 12, 2017, with 1.3 million Alabamians casting a ballot for their choice for the next U.S. Senator from Alabama. Most recently, we broke the record for turnout in a non-Presidential general election year during the 2018 General Election with more than 1.7 million Alabamians going to the polls.

In Alabama, we are making it easy to vote and hard to cheat.

As we prepared for the 2018 General Election, we worked to ensure our systems were protected by requiring 2-Factor Authentication for any State or local user who accesses the voter registration system. We secured our networks and our election night reporting system with resources provided through the Department of Homeland Security, our local information systems team, and other third-party vendors. Our work to conduct elections efficiently and effectively is supported both by the Elections Assistance Commission and the Department of Homeland Security. The EAC provides guidance and support, as we prepare our local election officials to administer their elections. Our relationship with DHS is a relatively new one, but it is one that has been home to significant growth over the last 2 years. Prior to the Senate Special Election in December 2017, we had very little interaction with DHS. However, as that election approached, we were able to work closely with DHS to ensure our systems were secure. We wanted to make sure that any vulnerabilities that we could identify were resolved and any new issues were mitigated before they disrupted an election in Alabama. We have also hosted a team from DHS on-site with us throughout election day to ensure issues are resolved in real time.

The most significant support that the Federal Government has provided to my State has been access to Federal grants and other resources to modernize and to increase the accessibility of our State's voting systems. Additional funding is imperative to ensure voting equipment can remain up-to-date and voting systems can remain secure to protect the data of those citizens.

Another area in which I have continued to advocate is for the EAC to provide guidance, testing, and verification of vendors, equipment, and systems much like the Federal Government does for other aspects of our Nation's critical infrastructure.

The impact of the enactment of H.R. 1 could possibly damage the credible elections process we have worked hard to build in Alabama by creating a series of administrative concerns for the State to enforce.

Title I of this bill creates significant concerns for me and the people of our State. This bill makes any process currently in place in our State to update and maintain the voter registration system illegal, while expanding the process of voter registration. Empirical data shows that no State in the union has done more, per capita, in the past 4 years to increase voter registration than Alabama. This bill would create massive errors in the States' voter rolls and would be a disservice to voters that often benefit from the reminders sent from election offices encouraging them to update their registration information.

In Alabama, more than 94 percent of the eligible population is registered to vote. Therefore, our biggest responsibility when it comes to maintaining the voter registration system is to keep voter information accurate and current. Providing awareness efforts and teaching our citizens how to effectively participate in their democratic institutions is a much more effective method to get voters to the polls. That is exemplified in Alabama and was reconfirmed through a recent ruling from the Federal court on Alabama's photo voter ID law and its implementation. The judge in that case wrote that if every State in the union did what Alabama has done, then every State could have photo voter ID in their State because Alabama makes it so easy to be able to vote.

Title V of this bill is troubling, as it amends the Federal Election Campaign Act of 1971 to turn the Federal Election Commission (FEC) into a powerful, Government tool that provides a balance to big money donors and distribute resources to candidates unable to raise funds from those donors. However, this bill will not have the desired impact that the authors intend. The bill attempts to provide this balance to candidate fundraising by giving power to the FEC to redistribute tax-payer money to citizens that qualify and by providing matching funds to candidates who only accept small-dollar donations. This change would transform campaign financing and would enact into law excessive Federal intervention in a system that, is by law, to be administered by the State.

Under this bill, if the Commission finds, by themselves, that a candidate has failed to comply with any of the requirements of this program, the commission has the ability to simply revoke the certification of a candidate. This revocation could come in the middle of an election cycle allowing the FEC to become a partisan tool to be used as a weapon to completely eliminate a candidate's ability to campaign. This bill has the potential to make the FEC one of the most powerful entities in the U.S. Government.

A candidate that has been revoked by the FEC would then be unable to receive public funds and may have to repay all the resources received by their campaigns into an account the FEC controls to then use to conduct further audits or, if used improperly, to conduct unmitigated harassment of candidates they disagree with based on partisan, political, or philosophical differences. Past experiences involving the Internal Revenue Service indicate that this is not only plausible but likely.

By taking the ability to financially support a candidate away from the electorate, the most important person in our Nation—a citizen of the United States—and placing it with the Federal Election Commission, brings us one step closer toward the Federal Government dictating winners and losers in elections.

The most important feature to a good election security bill is to create one that provides necessary resources to the States without creating unfunded or underfunded mandates and strangling restrictions through Federal overreach.

United States Senators and Members of Congress that are unwilling or unable to consider the fact that each State has unique laws and circumstances with different levels of resources must understand that they are creating an ineffective system that will create additional hardships for the entities responsible for administering and conducting elections in their State, and potentially cause unnecessary damage to the credibility and security of our electoral process. State leaders must be given the opportunity to build their system around their State's laws and citizens regarding elections as is indicated in the United States Constitution.

Chairman THOMPSON. Thank you very much. Let me thank all the witnesses for their testimony and we have about 20 minutes to kind-of run this before they call votes so we are going to move very fast.

Mr. Braun, when you brought—who did you bring to the attention of that there was some vulnerabilities in equipment and you found that going back later the vulnerability was still there. Who do you make aware of that vulnerability?

Mr. BRAUN. Sir, we—we put it in a report that we released both to the press and to—we actually released it here on Capitol Hill in our building and gave it to multiple stakeholders in Government as well as the private sector. We dispersed it widely.

Chairman THOMPSON. OK. Did you make it available to DHS?

Mr. BRAUN. Yes, we sent them advanced copies as well as the final copy.

Chairman THOMPSON. OK. Did you get a comment back from them in any way?

Mr. BRAUN. I did not, sir.

Chairman THOMPSON. OK. Thank you. Mr. Merrill.

Mr. MERRILL. Yes, sir.

Chairman THOMPSON. Did you apply for any of the funds from the Election Assistance Commission?

Mr. MERRILL. Yes, sir. To get our balance from the original HAVA appropriation we did so.

Chairman THOMPSON. How much did you get?

Mr. MERRILL. About $6.2 million for the State of Alabama.

Chairman THOMPSON. Could you have done what you did without that money?

Mr. MERRILL. Well, we have. Congressman, we have not spent a dime of that money yet because the things that we are planning on introducing, the continuation of the purchase for electronic poll booths, which we have 30 of our 67 counties that are currently using it and the introduction of additional audit procedures that will be in place that will cost us some resources.

Some other things that we are doing in the area of cybersecurity where we have to provide an appropriate match for that purpose. Everything that we have done so far and we have done a number of things, as a matter of fact, if you will let me just mention some of these.

Chairman THOMPSON. No. No. You just answer my question.

Mr. MERRILL. Yes, sir. Yes, sir.

Chairman THOMPSON. You got $6.2 million right?

Mr. MERRILL. That is correct.

Chairman THOMPSON. You anticipate to spend it?

Mr. MERRILL. We going to spend it.

Chairman THOMPSON. OK. That is what—that is what I am trying—trying to get at.

Mr. MERRILL. Yes, sir.

Chairman THOMPSON. So—so you saw the need for additional resources.

Mr. MERRILL. Congressman, I always see the need for additional resources.

Chairman THOMPSON. OK. Mr. Padilla, could you tell us how much California received?

Mr. PADILLA. California's share of last year's appropriation was about $34 million. It is pretty much being spent if it is not already been spent in the current fiscal year budget. It is in a number of areas.

Some of it is in hardware; software upgrades to our VoteCal, which is our centralized voter registration database, others for security improvements and counties' access to that same database.

We have dedicated some of the funding per EAC DHS recommendation on training. Cyber training is as important as cybersecurity to make sure staff at the State and at the local level are practicing all the best cyber hygiene practices as well.

I want to make a special comment on the timing of this because I have heard this about the Q&A of the first panel. Is there enough time, is there enough time, is there enough time as if—sounds like an argument to not move forward with offering States additional resources.

There are ways to expedite how that money gets from the Federal Government to the State government down to the locals who need it the most. You know first of all, Florida 2000 triggered HAVA. HAVA was 17 years ago and the final disbursement of those dollars was just last year.

The Federal Government can move more quickly and appropriate and not just approving but appropriating the monies to States. The 2016 election kind-of revived a lot of these conversations. Yet, it wasn't until April 2018 that those final HAVA dollars were moved. So the Federal Government can move a little bit quicker. At the State level we have learned how to accelerate that—that money the investment added to local level by entering into contracts with counties to move their money to on a reimbursement basis. So the fact that the check is not in hand should not hold up counties being able to make the investments that they need to make.

Once they know that they can count on being reimbursed, a lot of counties are willing to move more quickly and bring those security benefits to the elections.

Chairman THOMPSON. So, thank you very much. Mr. Braun, supply chain is important also. I mentioned it to the last panel and I was given this assurance that we are in a global economy and everything was fine. I heard a little something from your comment. Can you elaborate on that?

Mr. BRAUN. Sure. This is kind-of a known thing that Russian hackers as well as other nation-states hack parts in the supply chain all the time. I think anybody who questions whether supply chain or remote hacks are possible just look at Stuxnet. Those centrifuges were buried in concrete vaults underground in the desert and folks were still able to get in there and take those out. Anybody who thinks that undermining our institutions and our democracy is any less of a strategic importance to Putin than taking out the Iranian nuclear program was to those who did that is very mistaken——

Chairman THOMPSON. I agree so have to on that end pay close attention to who's providing the equipment for our elections.

Mr. BRAUN. Without question there needs to be assessments of the parts and where they came from and inspections of them and a whole regime put in place for that.

Chairman THOMPSON. Thank you. I yield to the Ranking Member.

Mr. ROGERS. Thank you, Mr. Chairman. What I have been making the point in my earlier questioning and trying to emphasize is as Secretary Merrill said, he hasn't spent any of his money yet and Secretary Padilla said he started spending it. It just takes time. This money is not going to fix anything just in 1 year. It is going to be a process. In most cases it is going to take several years and that has been my only point.

Secretary Merrill, the purpose of this hearing is to review H.R. 1 even though we are not going to be marking it up. Is there anything in H.R. 1 that you can find helpful to you in securing elections?

Mr. MERRILL. No, Congressman, there are some things that we find restrictive because of what we would have to do to adhere to certain guidelines that are in the bill that are associated with the allocation that would accompany it.

Mr. ROGERS. If we were marking it up, which we are not, what would you suggest we do to improve it?

Mr. MERRILL. Well one of the things that I would encourage the Members to do is to make an appropriation that establish some level of guidelines but did not have strict adherence that had to be met so that the local State or the local jurisdiction would be able to purchase equipment or be able to purchase services or be able to purchase types of products that were necessary for them to administer their elections in a way that they saw fit and in a way that was best for them.

Because in my mind, it is always best to make those decisions at the local level as opposed to the National or the State level going down to the local jurisdiction.

Mr. ROGERS. Secretary Padilla, the same question. What would you do if we were marking up H.R. 1 to improve it, if anything?

Mr. PADILLA. I appreciate the opportunity. So there is an element to H.R. 1 that establishes not just time tables for EAC—or excuse me—DHS testing and certification of voting systems prior to their being used by States. That element fails to recognize there is a handful of States, California being one, that has established testing and certification at the State level where we statutorily require our 12 State standards to meet or exceed the Federal guidelines.

So an allowance for those States to test at the State versus requiring a duplicative Federal testing or certification and as long as the time table suits us in terms of properly administering the elections, that flexibility will be helpful as well.

Mr. ROGERS. Let me ask this, you heard Mr. Higgins earlier in the questioning and the previous panel emphasized that there are scores of thousands of voting locations around the country. When you get the HAVA funds, and this is for Secretary Padilla or Merrill, do you prescribe standards that counties must adhere to for you to fund their purchase of equipment or training?

Mr. MERRILL. Yes, sir, actually that is done, Congressman, in the legislation that was approved when HAVA was first adopted. One of the things that we discovered was that that was not always being adhered to whenever that appropriation came and it was approved at the State level. So we have made sure that we even had training and we provided training to our local jurisdictions as well.

Mr. ROGERS. You just don't write a check to the local city or county.

Mr. MERRILL. Certainly not. Certainly not.

Mr. ROGERS. You say that is a Federal requirement?

Mr. MERRILL. Yes, sir. There are certain guidelines that were established in the HAVA appropriation that said these are permissible expenses and if you go outside of that then somebody should be held liable for that. That has not happened in the past.

Another frustration that we have experienced is when those additional dollars came, they were complimenting what happened in 2003. Well what happened in 2003, and of course that—that was your first session in the Congress, was that there was no deadline on when those funds had to be expended at the State or local level.

We have a number of counties in our State that received an appropriation 15 years ago and that money is still sitting in their bank account. Now it looks good to those people that live in that county but those resources are not spent—they are supposed to be used to benefit all of the constituents that live in that county in that particular jurisdiction. In our instance in the 2,401 individual jurisdictions where we have voting precincts.

Mr. ROGERS. Mr. Braun——

Mr. PADILLA. If I may—if I may add?

Mr. ROGERS. Certainly.

Mr. PADILLA. So similarly and in agreement that the guidelines that are established at the EAC or at the Federal level as those monies move. We mentioned earlier how this contract reimbursement basis with counties allows the investments to be made earlier. It also provides to those contract reviews an additional point of compliance, if you will, or a verification that indeed the expenditure is being made or consistent with those Federal requirements.

Mr. ROGERS. Right. Mr. Braun, we all know that Russia has been meddling in our elections by disinformation for decades and just like they do countries all around the world for decades particularly in eastern and western Europe. But you made a point a few minutes ago that the Chairman addressed but you said that there have been instance—and my understanding there have been no incidents of hacking in the 2016 or 2018 elections but you said that there have been some incidents prior to that where Russia had hacked some machines in this country. Can you expand on that please?

Mr. BRAUN. It was actually a website I was referring to. Vox Media reported, I believe it was actually 2017 instance where Russian bots I think took down an election reporting website in Tennessee.

Mr. ROGERS. OK.

Mr. BRAUN. Multiple Federal sources were cited in the report.

Mr. ROGERS. Thank you very much. I yield back.

Chairman THOMPSON. Thank you very much. The Chair yields to the gentlelady from New York, Miss Rice.

Miss RICE. Thank you Mr. Chairman and thank you all for coming today. Over the past couple of weeks I have heard some people refer to H.R. 1 as a Federal takeover of our elections. But I hope that everyone on Panel II would agree that the Federal Government has a Constitutionally-protected role in advising and helping to administer elections.

I think 2016 should have established that once and for all. I think the previous panel, both Mr. Krebs and Mr. Hicks, laid out the fallacy of that claim by showing that they were able to build relationships with States and localities to work together without infringing upon the State's ultimate ability and right to set election standards in their own States.

My concern is the—what—and this is to everyone on the panel, what are States doing to work with social media companies to combat wide-spread disinformation campaigns targeting our elections? What do you think the Congress and the Federal Government can do to better prepare States and local election officials for these dynamic hybrid warfare attacks?

Mr. MERRILL. Outstanding question. I will tell you this. I don't think—well, there is nobody at this table that has had a higher-profile situation than we did in Alabama when Senator Jones was elected December 12, 2017.

I attended a presentation that was made by Facebook and Twitter in February 2018. They were talking about all they had done to help folks, and how they had made it easier for people to understand when bots were removed, and how it was helping the electoral process.

I said to them—after I waited patiently in line, I said, now friends, let me say this to you. I said, if you will tell me what you did to help us in Alabama, we will both know because they were talking about what they done in ours, specifically. They didn't do anything to help us.

Now, subsequently, we came to Washington and had a meeting with Facebook, and talked to them about what they could do, and how they could be more helpful. One of the things they have introduced now is that whenever you get ready to purchase an ad on Facebook, they communicate with you directly through a card that is mailed to a particular location so you know if that individual is making the purchase as a United States Citizen.

There are other mechanisms that they have put in place that I think are appropriate now. But we have got to have some cooperation with the people at the social media level. That will enable us to be more effective.

We were actually able to have ads removed from YouTube and Google because of the work that we did, but we had a difficult time with Facebook. Twitter was also very supportive in what they did to help us.

Mr. PADILLA. In my oral remarks I made reference to the creation of an Office of Election Cybersecurity, as well as Office of Enterprise Risk Management in California. In my written remarks, I expand on that a little bit. Some of the initiatives within the election cybersecurity effort included: We branded a voucher. We put up a specific web portal with a lot of important voter tools, the find your polling place, verify your registration status, and a dedicated email address for the public to report suspected misinformation.

In addition to that, some of our additional State funding allowed us to hire staff strictly dedicated to social media monitoring. Not to censure candidates or campaigns, but to specifically look for erroneous information about the election or the voting process.

Some are to—a lot of secretaries benefited from a mass conversation—the National Association of Secretaries of State conversation with representatives from Facebook, and Twitter, and others. I mean, we have the benefit that they are based in California. So we have a little bit quicker access to them. Creating specific protocols for being able to report to them, where these specific complaints, kind-of, jump to the front of the line for review because, you know, if you submit something on Election Day, you can't wait for 7 days for it to be addressed.

We—we ended up reporting close to 300 who we felt were misleading or inaccurate posts, tweets, et cetera, 98 percent of which the social media companies, themselves, took down because it violated their policies. So it is one example of monitoring, reporting, and relationship.

Mr. PRAETZ. If I might? We have looked at this as, sort-of, defending our institution on two fronts; one is mis- and disinformation front. It is a place where as election officials we don't have a tremendous amount of control.

Then, there is the other front, which is the infrastructure front, which is the place where we have 100 percent control on. So that is where a lot of our focus has been. But there is a bit of overlap, and it comes in the form of information about where people vote, when you vote, what you need to vote, I.D. requirements, things like that.

So, it is really key that, as election officials, as more and more folks drive voters back to the trusted sources, like us, that we remain trusted sources and are providing fully accurate information.

That means that we have got to, sort-of, up the notch again on the infrastructure that we are protecting. One other note is that we have got to expand the services we provide. I think social media steps in where they think there are gaps, in terms of driving registration outreach, or driving—showing up at the polling place outreach.

They are filling gaps that they perceive in the administration of elections. To the extent that we don't fill those ourselves, there are going to be third-party providers that continue to do so. That—that can result in challenging relationships because sometimes the information they rely upon can be inaccurate.

Miss RICE. Go ahead. Mr. Braun.

Mr. BRAUN. Congresswoman, thank you for that question because I think it hits on the head of—of how this is such a National security problem. At the University of Chicago, we spend a lot of time trying to update concepts like nuclear deterrents or cyber deterrents, which has really not happened yet in the National security world.

I think that the point that you are making, it is nearly impossible for us to stop Russia from doing something like they did in the Ukraine where—imagine election night 2020 and 12 battleground State websites are down because they have hacked the websites. Then, Russian media is announcing that their preferred candidate had won the election. It would be chaos.

We can't really stop it from happening without a strong deterrence regime. That is not in place yet. I—and it is something that, you know, the National security establishment really needs to think through, and implement. Thank you.

Miss RICE. Mr. Braun, I couldn't agree with you more. Let me just end with this thought. Everything that I have heard today over the past 3 hours and 15 minutes, I hope has established, in all of our minds, the need to address this issue from a non-partisan stance because this gets to the very heart of maintaining the democracy. That, whether you are a Republican or a Democrat, you love and you want to maintain.

I really hope that, thanks to smart brains like you, and the prior panel, and hopefully the—the commitment of everyone on this committee, and throughout this body, we recognize how important it is to maintain the integrity of our democracy. Thank you and I yield back, Mr. Chairman.

Chairman THOMPSON. Thank you. The Chair recognizes the gentleman from Louisiana, Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman. It is interesting to have my colleague, Miss Rice, mention that—the smart brain in the room mentioned by the smartest brain in the room. Gentlemen, thank you for your service. My question is going to be to both secretaries of state, Secretary of State Padilla and Merrill.

I had mentioned in an earlier round of questioning that there were over 174,000 precincts, Mr. Chairman, voting precincts in America. My brilliant staff has advised me the actual number is 178,217 in the 2016 voting cycle. That is just—this is a tremendous endeavor.

Our goal here in this committee is—is shared on—from both sides of the aisle, we want every legal vote to have access to the poll, easy and fair access to the poll and we want their vote to be accurately counted, whether they are Democrats, Republicans, or anything in between. We have that same goal. You, gentlemen, have the incredible task of ensuring that that happens in your individual States.

The—your colleague from the State of Texas, secretary of state has stated that in Texas it has been identified 58,000 non-U.S. citizens who are illegally in the country voted in one way or another in elections over the last two decades.

May I remind all of us that sometimes even Federal elections are determined by very, very few number of votes. Our colleague Will Hurd from Texas 23rd district, his election was determined by 926 votes. So to say that it is a—that it is a small problem is not a—I don't think it is intellectually sound, when—when that is—when that response is measured against elections that are determined by very few votes.

So Secretary of State Padilla, is seems to me, since we are dealing with Title III, election security. That is our jurisdictional authority in this committee. Security has—as it—to establish a perimeter. That you want to control access to that perimeter first and then control action within that perimeter.

So how do you, good sir, in California, how can—how do you guarantee the citizens of your State that access to a controlled voting environment or precinct is limited to a legal vote? I—and, sir, I will be asking you the same question.

This is—this is a spectrum beyond the control of the action. We spent a lot of time talking about how we confirm the accuracy of a vote and cyber interference, et cetera. How do we control legal access to that voting perimeter, good sir, in your State?

Mr. PADILLA. I very much appreciate the question. I know Congress at times deals with public safety issues and debates about the balance between public safety and civil liberties. I put that out there just as a framework to consider when it comes to elections. We value security and we value accessibility, right? Those two are not mutually exclusive.

Mr. HIGGINS. They are difficult, yes.

Mr. PADILLA. So when it comes to the security of the voting process and the actions taken within, just look at the data. I mean, there have been numerous reports, numerous studies, numerous investigations that, when it comes to the baseless allegations of massive voter fraud, show that voter fraud is exceedingly rare.

So the safeguards are working, by and large. Does that mean that we should not take it seriously? No, we do take allegations very seriously. But the measures that have been—technology and otherwise——

Mr. HIGGINS. Intelligent response. So let me give time to your—to your colleague from Alabama. Before he answers, let me state that what we seek is reassurance at the State and the local level as we are dealing with 178,000 precincts that legal access to that voting environment is recognized as a security concern, if we are talking about jurisdiction over the security of the—and the sanctity of our elections in America. This is certainly—any reasonable man or woman would recognize this. Sir, in Alabama, how would—how would you handle that?

Mr. MERRILL. Congressman, 2,401 of those are in Alabama and I want to share this with you, too. I want to be perfectly clear about this——

Chairman THOMPSON. You have 10 seconds.

Mr. MERRILL. OK. The only people that need to be voting in U.S. elections are United States citizens.

Mr. HIGGINS. Well, that would—that indentify the legal access.

Thank you, gentlemen, for your service to your country. Mr. Chairman, I yield.

Chairman THOMPSON. Thank you very much. The reason I said that, Mr. Secretary of State, they have called votes and we trying to finish——

Mr. MERRILL. Yes, sir.

Chairman THOMPSON. That is the good news. The bad news is all the questions going forward will be yielded to 2 minutes.

Mr. Correa.

Mr. CORREA. Mr. Chair, just a quick question. Mr. Padilla, Mr. Merrill, H.R. 1, help or not help with voter system integrity?

Mr. PADILLA. Help. Additional resources on the table that are desperately needed, we have offered under our previous question some specifics on how to maybe improve upon the language to make it even more strategic for State investment.

Mr. MERRILL. Congressman, it has a potential to, but not in the current form.

Mr. CORREA. Thank you.

Chairman THOMPSON. Thank you.

Chair yields to the gentlelady from Arizona, Ms. Lesko.

Mrs. LESKO. Thank you, Mr. Chair.

Very quickly I am just going to ask one of the questions and it will be to you, Mr. Merrill. Section 1302 of this bill H.R. 1 criminalizes false statements or misinformation regarding elections and candidates.

Much of how, in this bill it determines if a person is in violation of these provisions is to their intent. The penalty written in the bill is a fine of up to $100,000 or up to 5 years in prison, or both.

I guess, my question is and—how are we going to determine—who's going to be the arbitrator and determining if something is misinformation or not? I know, I can tell you in my election, my opponent did a lot of misinformation about me. Are they going to be a criminal now as well?

Mr. MERRILL. Well, Congresswoman, I want to make sure that—that you know this. We take voter fraud, which that would be a part of voter fraud, very seriously in our State.

Since I have been the secretary, we have had 6 convictions and we have had 3 elections that have been overturned. Prior to the time that I became the secretary, we had not had an incident of occurrence that was reported, identified, investigated, and prosecuted.

I brought a sheet, if you would like to have it I will be happy to share it with you, we have had 874 unique instances reported in our office since we have been there and all but 4 have been fully taken care of in one way or the other. I have got a way to show you what we have done on that.

I think it is important to know that we have a number of prosecutors in our State that are not really interested in advancing investigations into voter fraud because they think the penalties are too stiff. So the penalties that are outlined in the code section that you just identified, I don't know that they are really commensurate with what the crime may be.

So I think there is a number of people who may be concerned about the implementation of that at any level.

Mrs. LESKO. Thank you, Mr. Chairman, perhaps I had got misinformation. The information I got was on that particular section. It also included like misinformation like you would put out on Facebook or something like that, and it would criminalize it. So perhaps I am wrong, because that would be concerning to me. Thank you.

Chairman THOMPSON. Thank you very much. Will the gentleman provide that——

Mr. MERRILL. Oh, yes——

Chairman THOMPSON. Document for the—for the committee.

Mr. MERRILL. I can be—I can do so, sir.

Chairman THOMPSON. Thank you very much. I yield 2 minutes to the gentlelady from California, Ms. Barragán.

Ms. BARRAGÁN. Thank you, Mr. Chairman. I first want to thank everybody for being here. I have a bias here; I am from California. Thank you, Secretary Padilla, for everything you are doing. In 2016, several media reports claim that 21 States had been targeted or hacked. Was California one of them, and if so, what happened?

Mr. PADILLA. So California was not hacked, if you are talking about a hack or a specific type of breach. You know, the question brings to mind another valuable lesson that to think all secretaries have learned and local elections officials have learned in our partnership with DHS and others.

We talk cybersecurity and we reference cyber hygiene earlier, but cyber vocabulary is also critical. When there is an incident, it is important to be specific and precise about what has or has not happened, right. We don't want to downplay incidents because that would be irresponsible for, you know, accountability to the public, but we also can't blow it up either.

So, the stories that came out in 2016, about 21 States, from my understanding, California was on the list of States that were "scanned" by entities that trace back to agents of the Russian government. So what is scanning? You know, scanning has been described in lay terms as the equivalent of somebody in the neighborhood shaking doorknobs to see if the doors are locked, right.

You are looking for vulnerabilities that scan in and of itself; it is not compromising a system—it is not flipping votes—it is not a theft of data. So, frankly, scanning is very, very common in this day and age, given the technology that we all depend on now, not just in the election space, you know, across industries. So that is a long way to answer your question. California was on that list, but we know what it was; we know what it wasn't, and our integrity of our missions are intact.

Ms. BARRAGÁN. Thank you. I will yield back, given the short time.

Chairman THOMPSON. Thank you very much. I am sure Congressman Cleaver appreciates it. You have 2 minutes.

Mr. CLEAVER. Thank you, Mr. Chairman. Mr. Merrill——

Mr. MERRILL. Yes, sir.

Mr. CLEAVER. Gave us a short answer, if you can. You kind-of confused me. Were you—were you suggesting that there were a lot of—much more voter fraud in the State of Alabama, but you didn't—that was another attempt to prosecute because it was this—the penalties were too stiff?

Mr. MERRILL. Yes, sir. We have some; actually, I have two incidents that I could share with you just briefly. One, 119 absentee ballot applications were mailed to one location and nobody lives in that home. In another jurisdiction, 109 absentee ballot applications were mailed to the mayoral candidate's mother's home, and neither one of those had been prosecuted yet.

Mr. CLEAVER. Were there many—many more?

Mr. MERRILL. Sir?

Mr. CLEAVER. Were there many more of such cases?

Mr. MERRILL. Oh, yes sir. Yes, sir; we have them frequently. They are not just related to certain parts of our State either.

Mr. CLEAVER. No, that was just interesting, because most of the——

Mr. MERRILL. Yes, sir.

Mr. CLEAVER. Studies showed that we didn't have a lot of mass votes in——

Mr. MERRILL. Yes, sir. The main instances kind-of that we see are in the area of absentee balloting, not in walk-up, in-person voting.

Mr. CLEAVER. OK. But my final question; I want you to tell me whether or not I am right. Our elections equal—we have 8,000 voting jurisdictions—8,000. Forty-three States use electronic voting machines—and I go on to list a lot of different things that are different. So, you can't—I am having difficulty. I went to—somebody already tried to—you have—when you do—you have to make things match.

So, I can't fit it. If all these things were having—all these different States and territories are doing things differently, how can we all be equal? Anybody? Am I right or am I wrong? Am I right or wrong?

Mr. PADILLA. If your premise is, look, this is the United States of America, and if you are 18 years or older and a citizen with minimal exceptions, you have the right to vote, exercise that right vote without any—without any unnecessary obstacles, then it is, how we achieve those in each State?

Do some States have easier ways to be a registered voter if you are eligible? Yes, some have better than others. Do some States offer more options for when, where, and how to cast a ballot? Unfortunately, yes; some States do better than others. My work in California is to try make California, you know, the leader of the pack when it comes to, yes, being secure, being as accessible and voter-friendly as possible.

Mr. CLEAVER. Thank you.

Chairman THOMPSON. Thirty seconds for the gentleman from Alabama.

Mr. MERRILL. Yes, sir. Congressman, one of the things that I wanted to share was that, since January 19, 2015, we have registered 1,199,909 new voters; we now have 3,473,030 registered voters.

We have exceeded and surpassed any voter registration and voter participation records in the history of our State. In that period of time, we have done more per capita than any State in the union, to ensure that all of our eligible citizens are registered to vote and have an I.D.

Chairman THOMPSON. Thank you very much. Thank you, gentleman from Missouri, for his question.

Let me thank all of the witnesses for your expert testimony. We will probably have some additional questions for you—for you to respond back to us. I would like unanimous consent to—to the record, that final report on a Democratic Congressional Task Force*** on

*** The document has been retained in committee files.

election security and article on voting participation. Without objection.

[The information follows:]

ARTICLE, WWW.VOX.COM, "CIVIL RIGHTS LEADERS FOUGHT TO MAKE VOTING EASIER. AN ALABAMA REPUBLICAN DIDN'T GET THE MEMO"

*John Merrill thinks guaranteeing people the right to vote "cheapens" the civil rights movement's fight to, well, vote.*

*By Victoria M. Massie, @vmmassie, Nov 3, 2016, 5:10pm EDT*

Alabama Secretary of State John Merrill says that automatically registering people to vote "cheapens" civil rights leaders' efforts to maximize people's rights to, well, vote, Slate reported.

In an interview published Wednesday by Answering the Call, a voting rights initiative, Merrill was asked to explain why he opposes automatic voter registration, a move that could help fix America's paltry voter turnout rate.

Merrill didn't waver. First he name-dropped "civil rights pioneers" like Dr. Martin Luther King Jr. and Rosa Parks, noted his friendship with Rep. John Lewis (D–GA), and touted the fact his daughter interned for African-American Congress member Terri Sewell (D–AL). Then Merrill argued that granting people the right to vote "cheapens" these people's work by rewarding folks who are "too sorry to get up off of their rear to go register to vote":

> "These people fought—some of them were beaten, some of them were killed—because of their desire to ensure that everybody that wanted to had the right to register to vote and participate in the process. I'm not going to cheapen the work that they did. I'm not going to embarrass them by allowing somebody that's too sorry to get up off of their rear to go register to vote."

To make his point abundantly clear, Merrill compared automatic registration to "giving [people] a trophy because they've played on the ball team."

For Merrill, automatic voter registration feeds into the taboo notion of entitlements, rewarding people with services when they didn't put in the initiative to earn them.

There's just one problem: American citizens who are at least 18 years old should be entitled to the right to vote if they meet the age and citizenship requirement.

Rather, the major barrier standing between people and the polls tends to be policies trying to keep select groups far away, as civil rights leaders demonstrated half a century ago.

Despite having the constitutional right to vote, African Americans in Southern States like Alabama faced insidious Jim Crow-era policies like poll taxes and literacy tests that were damn near impossible to pass. In 1965, a 25-year-old Lewis and other civil rights activists of the time were brutally beaten by Alabama State troopers for attempting to March from Selma to Montgomery for that right.

The slew of voter ID laws passed to the fix nonexistent voter fraud that dubiously suppresses voters of color is one of the latest 21st-century examples. Others include some States like Alabama denying felons and people with mental disabilities the right to cast a ballot.

Historically, the right to vote has never been about effort. It's been about access, and is likely one of the reasons Lewis has been a fierce advocate for automatic voter registration—even if he's allegedly Merrill's pal.

Merrill's dog-whistle politicking about "entitlements" doesn't change that.

Chairman THOMPSON. I thank the witnesses for their valuable testimony and Members for their questions. The Members of the committee, as I indicated, may have additional questions for the witnesses, and we ask you respond expeditiously, in writing, to those questions.

Hearing no further business, the committee stands adjourned.

[Whereupon, at 1:30 p.m., the committee was adjourned.]

# APPENDIX

## Questions From Chairman Bennie G. Thompson for Christopher C. Krebs

*Question 1.* You testified that disabling or removing wireless modems from voting systems is a best practice recognized by DHS. Has DHS communicated this best practice in writing to election administrators? Can DHS share any written material on this?

Answer. Response was not received at the time of publication.

*Question 2a.* You testified that all 13 States that currently use paperless voting systems as their primary voting equipment in at least one jurisdiction are on a path to transition to voter-verified paper ballots throughout their States.

Please confirm this is accurate.

Answer. Response was not received at the time of publication.

*Question 2b.* Please provide an estimated time line (rough) for each State to complete the transition to paper ballots.

Answer. Response was not received at the time of publication.

## Questions From Honorable Sheila Jackson Lee for Christopher C. Krebs

*Question 1.* Are we taking a fail-safe approach to determining which election systems or processes are critical to the successful conduct of a public election?

Answer. Response was not received at the time of publication.

*Question 2.* Would you consider State-wide Centralized Voter Registration Databases a critical system to the administration and conduct of any public election?

Answer. Response was not received at the time of publication.

*Question 3.* What fail-safe measures are in place to assure that if the voter registration database is compromised and thereby make data records untrustworthy; or rendered unavailable for early voting or on election day the casting of ballots will continue?

Answer. Response was not received at the time of publication.

*Question 4.* How many States have plans in place to hold or continue an election should their voter registration databases become compromised?

Answer. Response was not received at the time of publication.

*Question 5.* How many States and jurisdictions within each State use electronic poll books?

Answer. Response was not received at the time of publication.

*Question 6.* Are there instances when electronic poll books have failed to operate as intended?

Answer. Response was not received at the time of publication.

*Question 7.* What recovery plan is in place should a polling location's electronic poll books fail or for periods of time not function?

Answer. Response was not received at the time of publication.

*Question 8.* How well does same-day voter registration during early voting and on election day create meet fail-safe objectives for the successful conduct of a public election?

Answer. Response was not received at the time of publication.

*Question 9.* Are you providing any guidance on security and wireless non-voting system technology?

Answer. Response was not received at the time of publication.

*Question 10.* Do election administrators plan for 100% voter participation during early voting or on election day? If not, why not?

Answer. Response was not received at the time of publication.

*Question 11.* Are there best practices that should be used to determine the number of ballots and ballot marking technology, or voting machine that should be provided to support voting?

Answer. Response was not received at the time of publication.

*Question 12.* Are there best practices to address when a natural or man-made event makes a polling location unavailable for voting?

Answer. Response was not received at the time of publication.

*Question 13.* How does allowing voters to vote at locations other than at a single voting location impact the ability of election services to serve voters in a county or State?

Answer. Response was not received at the time of publication.

### Questions From Honorable James R. Langevin for Christopher C. Krebs

*Question 1a.* How have you engaged local and State media outlets to ensure that unofficial vote reporting is protected from malicious interference?

How many affiliates has CISA worked with?

Answer. Response was not received at the time of publication.

*Question 1b.* How have you coordinated defense or information sharing related to the defense of State and local media outlet networks?

Answer. Response was not received at the time of publication.

*Question 1c.* How have you coordinated dissemination of information regarding attempts to interfere with other aspects of elections?

Answer. Response was not received at the time of publication.

*Question 2a.* Have you observed any change in public confidence as a result of efforts to increase election security?

How does DHS/CISA assess confidence in election integrity?

Answer. Response was not received at the time of publication.

*Question 2b.* What outcomes does DHS/CISA use to determine success in protecting elections?

Answer. Response was not received at the time of publication.

*Question 3a.* Does DHS have any outstanding requests for risk and vulnerability assessments from States or local election officials? Is there a wait for new assessments?

Have States/localities been implementing the policies that DHS recommended based on these assessments?

Answer. Response was not received at the time of publication.

*Question 3b.* How often does DHS/CISA conduct reassessments of jurisdictions? How often does CISA recommend refreshing RVAs?

Answer. Response was not received at the time of publication.

### Questions From Honorable Dina Titus for Christopher C. Krebs

*Question 1.* In my home State of Nevada there have been thousands of attempts by various actors to breach our voter registration database. Fortunately, our State and local election officials have managed to thwart every single one of these attacks. They have utilized Albert sensors to identify suspicious IP addresses and known malware signatures and alert the appropriate authorities. How important is it that each State deploy these Election-system sensors?

Answer. Response was not received at the time of publication.

*Question 2.* Acknowledging the importance of coordinating Federal, State, and local election security efforts, what kind of barriers exist that slow or prevent the Multi-State Information Sharing and Analysis Center from coordinating with local and State IT personnel to inform them about the types of attacks that occur and where they came from so local officials can better prepare for future attacks?

Answer. Response was not received at the time of publication.

*Question 3.* What sort of obstacles have you experienced when trying to share sensitive information about imminent threats with State and local election officials?

Answer. Response was not received at the time of publication.

*Question 4.* H.R. 1 aims to create channels for interagency collaboration by, among other things, requiring DHS, EAC, the intelligence community, the State Department, and other Federal partners to develop a comprehensive National strategy to protect our elections and our democratic institutions, perhaps through broad initiatives around media literacy or studying the effects of influence campaigns. Who is responsible for convening and coordinating interagency efforts to secure elections, and to what extent is there leadership from the White House?

Answer. Response was not received at the time of publication.

### Questions From Honorable Yvette D. Clarke for Christopher C. Krebs

*Question 1.* In November 2018, Senator Ron Wyden wrote to DHS, asking the agency to "forensically examine paperless voting machines used in the November 6, 2018 general election for signs of tampering or other manipulation by foreign governments or other malicious actors." On December 18, 2018, DHS responded to Senator Wyden, stating that "under our existing authorities, DHS cannot mandate that States submit to comprehensive forensic examinations of their voting machines." But last week, the DOJ and DHS issued a public statement saying there was "no evidence to date that . . . a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political/campaign infrastructure used in the 2018 midterm election." If DHS didn't have the authority to examine paperless voting machines used in the November 2018 election for evidence of hacking, which is what you informed Senator Wyden in your letter, what is the basis for your public statement last week saying there is no evidence that foreign governments hacked our election infrastructure?

Answer. Response was not received at the time of publication.

*Question 2.* Last year, the FBI uncovered that a Russian oligarch, with close ties to President Putin, had acquired an ownership interest in a vendor which hosted State-wide election data for Maryland.[1] Until the FBI alerted them, State election authorities were unaware of the vendor's ties to Russia. Even if no tampering occurred, this raises important questions about foreign ownership of firms providing election-related services. To the best of your knowledge, is the Federal Government undertaking any efforts, other than the CFIUS process, to assess potential existing foreign ownership of firms that produce voting machines or provide other election-related services? If so, please describe these efforts. If not, do you believe foreign actors may seek to invest in this sector with the intent of interfering in our elections?

Answer. Response was not received at the time of publication.

## QUESTIONS FROM HONORABLE MICHAEL T. MCCAUL FOR CHRISTOPHER C. KREBS

*Question 1a.* Foreign states, including Russia and other malicious actors have and will continue to attempt to interfere with U.S. elections. In fact, I encouraged, in a Classified space, both the Obama administration and the Trump administration to call out Russia for their targeted attacks on our Nation. Their activities have injected chaos and doubt into foundation of our democracy. An issue of this gravity requires Congress to act in a deliberate and bipartisan manner. Now, all eyes are on 2020.

What do you see as the major vulnerabilities in our election security as we look to the future? How do we address these?

Answer. Response was not received at the time of publication.

*Question 1b.* Can you outline the major lessons learned and the steps your agency has taken to effectively provide Federal assistance to the local election level?

Answer. Response was not received at the time of publication.

*Question 2a.* Last Congress, my bill, the Cybersecurity and Infrastructure Security Agency Act, was signed into law to streamline National Protection and Program's Directorate's (NPPD) efforts to execute cybersecurity and critical infrastructure missions and establish it as the Cybersecurity and Infrastructure Agency (CISA).

How has CISA been effective at combatting cyber threats? What are the major successes?

Answer. Response was not received at the time of publication.

*Question 2b.* What do you anticipate are the upcoming roadblocks and how can Congress be helpful?

Answer. Response was not received at the time of publication.

## QUESTIONS FROM CHAIRMAN BENNIE G. THOMPSON FOR THOMAS HICKS

*Question 1a.* In response to questioning from Congresswoman Clarke, you testified that it is possible to audit a Direct Recording Electronic (DRE) voting machine to determine if the system has been hacked. Yet that appears inconsistent with the findings of research performed by the National Institute of Standards and Technology (NIST) at the request of the EAC.

Is there new research that suggests it is possible to audit DREs?

Answer. All voting systems certified by the U.S. Election Assistance Commission (EAC) to meet the Voluntary Voting System Guidelines (VVSG) are required to have redundant memory. All voting systems, including Direct Recording Electronic (DRE) voting machines, are required to have two, separate sources for memory. A comparison audit of these two separate sources of memory, including a DRE's internal mem-

[1] *https://www.baltimoresun.com/news/maryland/politics/bs-md-election-russia-20180713-story.html.*

ory that stores voting results, could identify discrepancies, and thus reveal that a system had been compromised.

With that stated, because both sources of memory for DREs without VVPATs are electronic, it is fathomable that a sophisticated attack could alter both sources of memory to make them identical and cause alterations to the data to be undetected. The EAC recognizes the possibility of this threat is real, which is why the VVSG 2.0 has Principles and Guidelines requiring software independence. At the moment, paper is the best way to audit a voting system, but all systems utilizing paper must comport with HAVA's mandate for all voters to be able to cast their ballot privately and independently.

The EAC is not aware of new research to this point, however the Commission is aware that jurisdictions have in the past conducted parallel audits with DREs to ensure votes are being tallied accurately.

*Question 1b.* What is the source of that information?

Answer. Vendors have identified this process, and the EAC is aware that the University of Connecticut's Center for Voting Technology Research has numerous post-election audit reports that utilize such data.

*Question 1c.* Should this new research override NIST's findings?

Answer. No. This research should not be depicted as contrary to the findings of NIST. In order to meet the National standard set by the Voluntary Voting System Guidelines (VVSG), all tabulators, including DREs, are required to have redundant memory that can be independently verified in order to meet the National standard set by Voluntary Voting System Guidelines (VVSG). However, it is also feasible that such a system could be compromised via a significant attack that would alter both sources of electronic data. This is why the VVSG 2.0 recommends software independence. It is also why election offices customarily follow the principle known as "Defense in Depth" by building in multiple layers of security to prevent such an attack from happening, assess damage created by such an attack, and mitigate the fallout if a system was compromised.

*Question 2a.* You testified that you had little concern regarding the risk of corruption of voting systems through the supply chain because of the EAC Testing and Certification program. But the EAC Testing and Certification program which lacks Full Formal Verification (FFV) or full source code review. Moreover, the EAC Testing and Certification Program does not evaluate voter-registration systems, e-poll books, election night reporting systems, and other critical components that run elections.

Can you elaborate on how the EAC Testing and Certification Program is capable of detecting supply chain corruption in voting systems without FFV?

Answer. When the Help America Vote Act of 2002 established the U.S. Election Assistance Commission, it also created the EAC's Testing & Certification Program to certify, decertify, and recertify voting system hardware and software, as well as accredit test laboratories. The Testing & Certification Program has a very specific mandate that defines its work as helping to develop guidelines for, and certifying, voting equipment. This mandate does not include voter registration systems, e-poll books, and election night reporting systems.

To the question of risk management in the supply chains of systems, the EAC test labs review the source code, hardware, and software components of all voting systems tested under the EAC's Testing and Certification Program. The EAC maintains an on-going Quality Monitoring Program to identify and correct issues in the field. Additional details on these programs are included below.

The EAC's Testing and Certification Program conducts a full review of vendor-developed hardware, software, and source code for every system it certifies. Also required by the VVSG is a technical data package (TDP) that includes an approved parts list and/or the bill of materials documentation.

After a voting system is certified, there is a process for on-going validation and verification through the Quality Monitoring Program. This is an audit and analysis of issues reported from the field, issues discovered by the vendors from their internal testing, and quality audits that are performed on the voting system manufacturers. Also, as manufacturers have hardware that reaches the end of its useful life, they are required to submit engineering change orders to update the approved parts list and/or bill of materials. In accordance with the system certification, these engineering change orders must be approved by the EAC before the vendor can implement the new parts into their manufacturing process.

That being said, the EAC's Testing and Certification Program cannot mitigate all supply chain threats. As with all security, including cybersecurity, there is not one mechanism that can thwart all threats. This is why the election community should focus on building resiliency and security through the principle of "Defense in Depth."

The EAC's Testing and Certification Program does, however, provide built-in layers of security for supporting the methodology of "Defense in Depth" for mitigating the supply chain threats for EAC-certified voting systems via the mechanisms previously described. The EAC also recommends and assists jurisdictions in working with Federal partners so they can benefit from the "whole of Government" approach to securing our Nation's election systems.

For example, the EAC has played an instrumental role in providing opportunities for State and local election officials, as well as election vendors and other key stakeholders, to interact with Department of Homeland Security (DHS) officials following the designation of elections as part of the Nation's critical infrastructure. The Commission led the establishment of the Government Coordinating Council for the Election Infrastructure Subsector (GCC) and the Sector Coordinating Council (SCC). Both councils were functioning within 1 year of the critical infrastructure designation. OHS has said that the GCC was formed faster than any other similar critical infrastructure sector council to date.

Since then, the GCC has launched an Information Sharing and Analysis Center (ISACs) that allows election officials to receive timely notifications of potential threats, real-time monitoring of malicious activity on their networks and access to cybersecurity experts. Such working groups are exemplary proof-points of how local, State, and Federal governments can work together toward the shared goal of protecting our Nation's election systems.

*Question 2b.* Please explain how the EAC Testing and Certification Program is capable of detecting potential corruption by vendors servicing and programming systems that have already been certified.

Answer. The EAC's Testing and Certification Program cannot mitigate all supply chain threats; not even for threats to the one system of the elections process it oversees, which is the voting systems. As with all security, including cybersecurity, there is not one mechanism that can thwart all threats, which is why election officials should focus on building resiliency and security through the principle of "Defense in Depth." The EAC's Testing and Certification Program does, however, provide built-in layers of depth for mitigating the supply chain threats for EAC-certified voting system via the mechanisms detailed below.

All voting systems tested under the EAC's Testing and Certification Program go through a full review of all vendor-developed source code. The software and hardware, as certified, has been validated and verified to be programmed for its intended use. Also required by the VVSG is a technical data package (TDP) that includes an approved parts list and/or the bill of materials documentation.

Additionally, after a voting system is certified, there is a process for on-going validation and verification through the Quality Monitoring Program. This is an audit and analysis of issues reported from the field, issues discovered by the vendors from their internal testing, and quality audits that are performed on the voting system manufacturers. Also, as manufacturers have hardware that becomes end of life, they are required to submit engineering change orders to update the approved parts list and/or bill of materials. In accordance with the system certification, these engineering change orders must be approved by the EAC before the vendor can implement the new parts into their manufacturing process.

*Question 2c.* Please explain how the EAC Testing and Certification program is capable of protecting voter-registration databases, election night reporting systems and e-poll books from supply chain corruption?

Answer. These particular systems are outside of the scope of the EAC's Testing and Certification program as detailed in the Help America Vote Act. It should be noted that a number of States have independent certification programs for electronic poll books and provide their own certification testing requirements for e-poll books and voting systems. In addition, States and local election agencies have resources to protect voter registration databases and other technology, including servers. For example, voter registration databases are periodically audited by State or independent experts.

## Questions From Honorable Sheila Jackson Lee for Thomas Hicks

*Question 1.* Are we taking a fail-safe approach to determining which election systems or processes are critical to the successful conduct of a public election?

Answer. State and local election officials would likely tell you that each of their election systems and processes play a critical role in the administration of successful elections, which is why they invest time and resources into contingency planning and establishing practices that ensure eligible voters have the ability to successfully cast their ballot. For example, the availability of provisional ballots at the polls is the ultimate fail-safe step that election officials offer on Election Day to ensure that eligible voters impacted by unforeseen circumstances or issues are able to cast their ballots and have them counted. In addition, election officials often have contingency plans in place that include roving technicians who are able to quickly identify and resolve issues with voting equipment or provide replacement voting systems if there is a failure. Another example of State and local election leaders creating fail-safe processes is the usage of audits to verify election results and confirm that election systems functioned properly to produce an accurate result.

*Question 2.* Would you consider State-wide Centralized Voter Registration Databases a critical system to the administration and conduct of any public election?

Answer. Yes. Voter registration databases play a critical role in the administration of elections. State and local election leaders secure these systems by implementing controls to maintain confidentiality, integrity, and availability of the system and its data. Each election office has its own procedures and requirements for how these systems are managed, but the EAC does provide best practices regarding these systems.

*Question 3.* What fail-safe measures are in place to assure that if the voter registration database is compromised and thereby make data records untrustworthy; or rendered unavailable for early voting or on election day the casting of ballots will continue?

Answer. The availability of provisional ballots at the polling place is a key fail-safe measure to ensure that voters have the ability to participate in an election should voter registration databases not be available for any reason. In addition, jurisdictions frequently conduct a back-up of their voter registration database so, if a problem detected, the administrator is able to retrieve the back-ups to a specific date and time to review and began remediation if necessary.

*Question 4.* How many States have plans in place to hold or continue an election should their voter registration databases become compromised?

Answer. State and local election leaders across the Nation have contingency plans in place for events that could impact Election Day, including a compromised voter registration database. The availability of provisional ballots at the polls is a safeguard that ensures an election can still take place under these circumstances. In addition, election jurisdictions typically have a back-up of their voter registration list at the local level, and many election officials provide paper back-ups at polling places or election offices.

*Question 5.* How many States and jurisdictions within each State use electronic poll books?

Answer. According to the 2016 EAC's Election Administration and Voting Survey (EAVS), from 2012 to 2016, there was a significant increase in the use of electronic poll books Nation-wide. The number of in-person voters checked in with e-poll books more than doubled during this time span, increasing 110 percent from 19.7 million to 41.4. million voters. The EA VS also found that 32 States, the District of Columbia, and U.S. Virgin Islands reported using e-poll books in at least one jurisdiction in the 2016 election. Five States used e-poll books State-wide.

*Question 6.* Are there instances when electronic poll books have failed to operate as intended?

Answer. The EAC is aware of some specific instances reported in the media, but the Commission does not track such data related to electronic poll books. State and local election administrators are better positioned to provide detailed responses to this question.

*Question 7.* What recovery plan is in place should a polling location's electronic poll books fail or for periods of time not function?

Answer. Typically, as part of election officials' on-going contingency planning efforts, jurisdictions using electronic poll books prepare a paper back-up system in the event of an issue with the electronic poll books. Some jurisdictions may send the paper back-up to the polling place with the e-poll books, while others send them only if needed. The issuance of provisional ballots is one way that election officials ensure that voters have the ability to cast their ballot when electronic poll books fail. State and local election administrators develop and implement their own recovery plans and are better positioned to provide detailed responses to this question.

*Question 8.* How well does same-day voter registration during early voting and on Election Day create meet fail-safe objectives for the successful conduct of a public election?

Answer. Same-day voter registration is a policy choice made by the States. Its potential impact on the successful administration of an election is a question better posed to the election officials charged with carrying out elections.

*Question 9.* Are you providing any guidance on security and wireless non-voting system technology?

Answer. The EAC, often in conjunction with DHS, provides election officials training on election technology and security. In that training, the EAC highlights the best practice of disconnecting all portions of the voting system from the internet. Further, that training highlights best practices for securing systems that are networked, such as two-factor authentication, implementing integrity checks such as digital signatures and hashing, as well as the utilization of encryption.

In addition, the EAC has issued best practices and checklists for securing networked systems, such as election night reporting systems, as well as how to protect data that is on network systems. These resources include the EAC's Checklist for Securing Voter Registration Data and other handbooks, playbooks, and best practices documents.

*Question 10.* Do election administrators plan for 100 percent voter participation during early voting or on Election Day? If not, why not?

Answer. Election administrators forecast turnout across advance voting sites, by mail, and at polling locations. This forecasted mix allows election administrators to ensure proper resources are applied. Overall, election administrators plan to ensure that each and every voter is provided the ability to cast a ballot. In addition, States have laws and regulations to guide the number of pre-printed ballots required for election day, and many States also have in-house or polling place ballot-on-demand systems to provide additional ballots as needed.

*Question 11.* Are there best practices that should be used to determine the number of ballots and ballot-marking technology, or voting machine that should be provided to support voting?

Answer. State election offices often create guidance and procedures for local jurisdictions to follow. The EAC provides tools that can be used as part of this process, most notably the EAC's Election Administration and Voting Survey interactive portal that allows jurisdictions to compare their own election data with that of jurisdictions with similar characteristics. In addition, there are on-line tools available to assist election officials seeking to identify the number of voting systems and check-in stations they need to mitigate the chance of lines.

*Question 12.* Are there best practices to address when a natural or man-made event makes a polling location unavailable for voting?

Answer. Yes. Contingency planning is a key function of election administration. Election officials must prepare for the unexpected and have plans in place to conduct elections when disaster strikes. The EAC is committed to helping election officials prepare for everything from wildfires and hurricanes to terrorist threats and electricity outages. In fact, the Commission has launched a new initiative to more rigorously engage election officials who can help to shape the Commission's more robust suite of services and resources for election administrators who face natural or man-made disasters.

*Question 13.* How does allowing voters to vote at locations other than at a single voting location impact the ability of election services to serve voters in a county or State?

Answer. The impact of these procedures is different in the States and jurisdictions that may offer these services, and, therefore, the State election offices would be the best source to answer this question.

## Questions From Honorable Dina Titus for Thomas Hicks

*Question 1.* In my home State of Nevada there have been thousands of attempts by various actors to breach our voter registration database. Fortunately, our State and local election officials have managed to thwart every single one of these attacks. They have utilized Albert sensors to identify suspicious IP addresses and known malware signatures and alert the appropriate authorities. How important is it that each State deploy these Election-system sensors?

Answer. Every State and local election official has the duty to securely protect their election systems. Nevada's election officials have availed themselves to many security-focused services provided by the OHS. The EAC recommends that it all States use the Federal resources available—including those provided by the OHS and those that might be funded as part of the $380 million in HAVA Funds passed last year by Congress and administered by the EAC—to address election security threats.

*Question 2.* Acknowledging the importance of coordinating Federal, State, and local election security efforts, what kind of barriers exist that slow or prevent the Multi-State Information Sharing and Analysis Center from coordinating with local and State IT personnel to inform them about the types of attacks that occur and where they came from so local officials can better prepare for future attacks?

Answer. Because OHS manages the Election Infrastructure Information Sharing and Analysis Center (EI–ISAC), this question would best be answered by OHS.

*Question 3.* What sort of obstacles have you experienced when trying to share sensitive information about imminent threats with State and local election officials?

Answer. For the most part, the EAC has not experienced obstacles when charged with sharing information about imminent threats with State and local election officials. This is something the EAC did even ahead of the 2016 election and prior to DHS's decision to designation elections as part of the Nation's critical infrastructure. That said, the delay in issuance of security clearances for the EAC Commissioners remains an issue that hopefully will be resolved quickly to allow the EAC to receive and share sensitive information when necessary.

*Question 4.* H.R. 1 aims to create channels for interagency collaboration by, among other things, requiring DHS, EAC, the intelligence community, the State Department, and other Federal partners to develop a comprehensive National strategy to protect our elections and our democratic institutions, perhaps through broad initiatives around media literacy or studying the effects of influence campaigns. Who is responsible for convening and coordinating interagency efforts to secure elections, and to what extent is there leadership from the White House?

Answer. The DHS Government Coordinating Council (GCC), of which the EAC Commissioners are members, is the primary body to share information related to securing elections. Aside from that body, under the Help America Vote Act, the EAC is the only Federal agency authorized to assist election officials with all aspects of elections, including security.

### Question From Honorable Yvette D. Clarke for Thomas Hicks

*Question.* Last year, the FBI uncovered that a Russian oligarch, with close ties to President Putin, had acquired an ownership interest in a vendor which hosted State-wide election data for Maryland. Until the FBI alerted them, State election authorities were unaware of the vendor's ties to Russia. Even if no tampering occurred, this raises important questions about foreign ownership of firms providing election-related services. To the best of your knowledge, is the Federal Government undertaking any efforts, other than the CFIUS process, to assess potential existing foreign ownership of firms that produce voting machines or provide other election-related services? If so, please describe these efforts. If not, do you believe foreign actors may seek to invest in this sector with the intent of interfering in our elections?

Answer. The EAC agrees that the question of foreign ownership is an important one. As such, foreign interference in elections should always be treated as a credible threat. That's why the Commission's Testing and Certification Program provides built-in layers of security and quality assurance on voting system manufacturers, including a registration process that requires disclosure of ownership and on-going quality monitoring audits. Since the EAC cannot mitigate all threats from its registered voting system manufacturers, it recommends that election officials focus on building resiliency and security through the principle of "Defense in Depth" and by taking advantage of resources offered by Federal partners.

As a clearinghouse of information on best practices in election administration, the EAC has also provided officials with real-life examples of how to mitigate threats potentially posed by foreign ownership. For example, the EAC has posted security language from a Request for Proposal requiring voting equipment vendors, and their parent and holding companies, to be based in the United States. Our office, in conjunction with the Department of Homeland Security (DHS), has also offered election officials training on election technology and security, including best practices for contracting and the selection of vendors.

### Questions From Honorable Michael T. McCaul for Thomas Hicks

*Question 1.* Voting machine challenges remain a chronic problem. How can local officials who are the center of gravity for running and securing elections ensure electric voting machines are secure?

Answer. The goal of every election official is to ensure not only voting machines, but the entire election system, is secure. Security has always been at the heart of what election officials do. Each State and jurisdiction has measures in place to ensure security in all phases of the election process. Every jurisdiction is different. This is one of the great strengths of our election system—that there is no one central point of access that could render the system vulnerable to a massive attack.

Since the EAC's inception, our HAVA-mandated Testing & Certification Program has been a critical first step in the process of maintaining the reliability and security of the voting systems used in our Nation's elections. The Commission also produces guidelines and checklists, posts Requests for Proposals, elevates best practices and administers an IT Management course to help election officials take a holistic approach to securing their election systems. Through our partnership with the National Institute of Standards and Technology (NIST), the EAC has also maintained the Voluntary Voting System Guidelines (VVSG), which sets the National standard for voting equipment around the country.

However, as stated above, the EAC is not the only security solution for election officials. As secure voting systems must have many layers of security and resiliency built into every component, election officials must also have a "Defense in Depth" in terms of partnerships and resources they can draw from to secure their systems.

*Question 2.* What incentives are in place for election equipment companies to improve their security?

Answer. The best incentive for election equipment companies to improve security is in response to a requirement by their customers, State and local election officials who administer elections. The EAC produces guidelines and checklists, posts on-line sample Requests for Proposals, elevates best practices, and administers an IT management course to help election officials take a holistic approach to securing their election systems, including making sure best practices are required of their contractors and vendors in addition to their own election staff.

Another incentive for election equipment vendors is the EAC's Testing and Certification Program. In order for a voting system vendor to have the ability to submit a voting system to be tested and certified by the EAC, it must first become a registered manufacturer. This requires disclosure of ownership, as well as on-going quality monitoring audits. The Testing and Certification Program also oversees the Voluntary Voting System Guidelines (VVSG), which the EAC maintains with our partners at NIST. The VVSG are a set of standards against which voting systems can be tested to determine if the systems meet those standards. Some factors examined under these tests include functionality, accessibility, accuracy, auditability, and security capabilities. These principles, and the best practices disseminated as part of the EAC's Clearinghouse function help set and maintain the standard for voting equipment around the country.

### Questions From Honorable Sheila Jackson Lee for Alex Padilla

*Question 1.* Are we taking a fail-safe approach to determining which election systems or processes are critical to the successful conduct of a public election?

Answer. Response was not received at the time of publication.

*Question 2.* Would you consider State-wide Centralized Voter Registration Databases a critical system to the administration and conduct of any public election?

Answer. Response was not received at the time of publication.

*Question 3.* What fail-safe measures are in place to assure that if the voter registration database is compromised and thereby make data records untrustworthy; or rendered unavailable for early voting or on election day the casting of ballots will continue?

Answer. Response was not received at the time of publication.

*Question 4.* How many States have plans in place to hold or continue an election should their voter registration databases become compromised?

Answer. Response was not received at the time of publication.

*Question 5.* How many States and jurisdictions within each State use electronic poll books?

Answer. Response was not received at the time of publication.

*Question 6.* Are there instances when electronic poll books have failed to operate as intended?

Answer. Response was not received at the time of publication.

*Question 7.* What recovery plan is in place should a polling location's electronic poll books fail or for periods of time not function?

Answer. Response was not received at the time of publication.

*Question 8.* How well does same-day voter registration during early voting and on election day create meet fail-safe objectives for the successful conduct of a public election?

Answer. Response was not received at the time of publication.

*Question 9.* Are you providing any guidance on security and wireless non-voting system technology?

Answer. Response was not received at the time of publication.

*Question 10.* Do election administrators plan for 100 percent voter participation during early voting or on election day? If not, why not?

Answer. Response was not received at the time of publication.

*Question 11.* Are there best practices that should be used to determine the number of ballots and ballot marking technology, or voting machine that should be provided to support voting?

Answer. Response was not received at the time of publication.

*Question 12.* Are there best practices to address when a natural or man-made event makes a polling location unavailable for voting?

Answer. Response was not received at the time of publication.

*Question 13.* How does allowing voters to vote at locations other than at a single voting location impact the ability of election services to serve voters in a county or State?

Answer. Response was not received at the time of publication.

### Questions From Honorable James R. Langevin for Alex Padilla

*Question 1.* Our system is only as strong as its weakest link, and we need to ensure everyone has this "cyber hygiene" knowledge. Have you found that there's a general lack of knowledge of security vulnerabilities and best practices at the staff level?

Answer. Response was not received at the time of publication.

*Question 2a.* Have the trainings you've conducted for staff been productive?

Answer. Response was not received at the time of publication.

*Question 2b.* What are some lessons learned from these trainings?

Answer. Response was not received at the time of publication.

*Question 3.* The risk and vulnerability assessments offered by DHS can be extremely valuable for States and localities. Have you found these assessments for States and local election officials to be useful as you work to secure your election systems, and have you implemented DHS's recommendations?

Answer. Response was not received at the time of publication.

*Question 4.* Do you have the resources you need to implement the recommendations, and if not, what more do you need to do so?

Answer. Response was not received at the time of publication.

### Question From Honorable Dina Titus for Alex Padilla

*Question.* When speaking with State and local election officials in Nevada, I have heard that while urban areas like Las Vegas may have the IT workforce available to recruit individuals to implement new cybersecurity measures like Albert sensors, rural areas have been struggling to find trained personnel. Have you experienced this shortage in other parts of the country, and do you believe further investment in STEM education is necessary to effectively mitigate this skills gap and secure our most vulnerable election sites?

Answer. Response was not received at the time of publication.

### Questions From Honorable Yvette D. Clarke for Alex Padilla

*Question 1a.* Last year, the FBI uncovered that a Russian oligarch, with close ties to President Putin, had acquired an ownership interest in a vendor which hosted State-wide election data for Maryland.[1] Until the FBI alerted them, State election authorities were unaware of the vendor's ties to Russia. Even if no tampering occurred, this raises important questions about foreign ownership of firms providing election-related services.

To the best of your knowledge, does your State have any election-related contracts with vendors backed by Russian or Chinese investors?

Answer. Response was not received at the time of publication.

*Question 1b.* What measures, if any, does your State undertake to assess foreign ownership of election vendors prior to signing contracts with them?

Answer. Response was not received at the time of publication.

### Question From Honorable Michael T. McCaul for Alex Padilla

*Question.* Foreign states, including Russia and other malicious actors have and will continue to attempt to interfere with U.S. elections. In fact, I encouraged, in a Classified space, both the Obama administration and the Trump administration to call out Russia for their targeted attacks on our Nation. Their activities have injected chaos and doubt into foundation of our democracy. An issue of this gravity requires Congress to act in a deliberate and bipartisan manner. Now, all eyes are

[1] *https://www.baltimoresun.com/news/maryland/politics/bs-md-election-russia-20180713-story.html.*

on 2020. How has the cooperation with DHS and Director Krebs strengthened California's election security?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE SHEILA JACKSON LEE FOR NOAH PRAETZ

*Question 1.* Are we taking a fail-safe approach to determining which election systems or processes are critical to the successful conduct of a public election?

Answer. Most election systems and processes are managed at the local level and therefore the fail-safe approach is often determined and implemented locally, though often State-wide guidance is provided. Election officials do try and ensure business continuity and therefore they do build in redundancies to many processes. However, there are large variations in the degree to which election officials are able to identify critical path systems, prioritize efforts, and build in sustainable redundancies.

Prioritizing the most critical systems is incredibly important. Most foundationally people need to be able to vote and administrators need to be able to count those votes accurately. Voter Registration System and Voting Systems are therefore the two most critical systems, without which elections could not be run. However, within those two umbrella systems, and around the edges, election officials rely on a variety of other system to aid in the seamless efficient administration of elections. Successful attacks on any of those systems can have a detrimental effect on the voter experience—and therefore in their level of trust. Some of these others connected systems that election officials rely upon to deliver expected services include:

- Voting Systems for casting and counting votes, as noted above
- Voter Registration Systems for managing the list of voters and what they are—entitled to vote upon, as noted above
- Election Management Systems for handling data necessary to facilitate the two above and to facilitate the various other duties
- Electronic Pollbook Systems
- Ballot Printing Systems
- Ballot Envelope Scanner
- Election Day Command Centers
- Election Information Websites
- Election Service Websites—registration—ballot requests w/ or without marking—sample ballots
- Election Night Reporting Websites
- Election Auditing Tools
- Other miscellaneous tools.

*Question 2.* Would you consider State-wide Centralized Voter Registration Databases a critical system to the administration and conduct of any public election?

Answer. Yes, I consider a State-wide voter registration database to be a critical system to the administration of elections. However, the particular level of criticality can vary depending upon whether the State has a centralized singular top-down voter database construction, or a diffuse, bottom-up construction. In Illinois the system was considered "bottom-up" meaning each county had their own primary database.

*Question 3.* What fail-safe measures are in place to assure that if the voter registration database is compromised and thereby make data records untrustworthy; or rendered unavailable for early voting or on election day the casting of ballots will continue?

Answer. One fail-safe operation available Nation-wide is the use of provisional ballots that can be counted after the election in the event voter data in the over registration database is not 100% accurate at point of service. Additionally, some States, like Illinois, offer same-day registration (SDR) options. SDR as a service offering and fail-safe process also offers a significant amount of resiliency. There are policy decisions that can impact business continuity when the software is not operating as expected. However, there is wide latitude and variance in how these fail-safe programs are managed and consequentially in how impactful such a major event would be. For example, in Cook County we implemented a registration process that was only marginally longer than a normal check-in process and believed we could have managed a significant data problem without equally significant impacts on lines and voter expectations. However, to do so we relied on electronic pollbooks (e-pollbooks). Were the e-pollbooks rendered inoperable entirely, the tertiary paper-based backup would have had a significant negative impact on the amount of time voters would have had to wait in line to check-in.

*Question 4.* How many States have plans in place to hold or continue an election should their voter registration databases become compromised?

Answer. I do not know how many places have a specific detailed plan for this type of occurrence. But every State and local election official knows how to administer provisional ballots and many times in large numbers. Whether most are outfitted for wholesale failure of the primary voter registration system is unlikely. In Cook County we could have likely handled a wholesale data failure given our use of electronic poll books and streamlined registration process. However, should we have had to revert to our back-up paper provisional and registration system there would have been significant service impacts.

*Question 5.* How many States and jurisdictions within each State use electronic poll books?

Answer. I do not know Nation-wide. In Illinois there are between 20 and 30 election jurisdictions that have electronic poll books, including all counties with over 100,000 voters. This accounts for over 83% of the State's registered voters.

*Question 6.* Are there instances when electronic poll books have failed to operate as intended?

Answer. I'm sure there are many cases of them not operating as expected or intended. They are computers operated by humans. And while the root cause most often comes back to user issues, the effect on a voter is the same. We certainly had sporadic episodes of having to revert to our back-up systems and even our paper registration books. This occurred in far fewer than 1 percent of our precincts and the issues was resolved at some point during the day in almost every case; the digital services and data became reliable once again.

*Question 7.* What recovery plan is in place should a polling location's electronic poll books fail or for periods of time not function?

Answer. Recovery plans are different everywhere. In suburban Cook County we had a number of back-ups. First, if the specific primary e-poll book software was inoperable, but the device worked, we utilized a redundant digital file of voters. We were able to do this because we capture actual signatures for every voter on paper and kept a full paper record. If the device failed entirely or workers felt most comfortable with paper back-ups we had a printed version of the poll book for emergency use. And finally, there was a process for Election Day Registration or Provisional Voting which guarantee all voters cast a ballot.

*Question 8.* How well does same-day voter registration during early voting and on election day create meet fail-safe objectives for the successful conduct of a public election?

Answer. Same-day voter registration relieved a tremendous amount of pressure in Cook County on election day and during early voting. It allowed for instant correction of operational voter registration mistakes (things like typos, and jr/sr problems, which always occur at some small rate) and provided a large fail-safe process for malicious activities.

*Question 9.* Are you providing any guidance on security and wireless non-voting system technology?

Answer. Cook County issued no guidance to other election officials other than the white paper that was attached to the testimony I delivered. It did not include a prohibition on wireless. In fact, Cook County used wireless technology in different contexts. While there was increased marginal risk Cook County accepted it because of the significant operational & voter list maintenance advantages. Ultimately the team believe that it had the ability to mitigate the potential security consequences through back up plans and solid audits.

The e-poll books communicated wirelessly with the central servers. Aside from embedded security like encryption, because Cook County had same-day registration, the team believed that the downside risk increase due to this communication method was covered for, and therefore Cook chose to allow wireless communications between e-pollbooks and the central office.

Cook County also transmitted encrypted unofficial election results from the precincts. However, before publishing those results Cook County validated that the results were not being systematically altered in any way during the transmission process. And before certifying the official results Cook County validated that the transmitted results matched the precinct printed results 100% of the time. In an environment where there are audits and auditable materials, the level of acceptable risk changes. It was the team's judgment that the decision to utilize technology to solve some operational and trust problems was acceptable even if they increased risk marginally to other areas. But it was only acceptable because Cook County believed they would find and be able to correct exploitation of those risk areas.

*Question 10.* Do election administrators plan for 100% voter participation during early voting or on election day? If not, why not?

Answer. In Cook County voters voted early on touch screens with audit trails and Cook County could accommodate 100% turnout, technically. However, Cook understood that they only had to outfit themselves for around a 30% voting in that early voting time period. With respect to printing paper ballots and resourcing with machines and staff, some officials do plan for complete turnout. Others do not. In Illinois officials are technically required to print ballots for 110 percent of the registered voters on election day. Many don't however, because they subtract the number of people using vote by mail and early voting, and they also rely on historical numbers as a valid offset. Finally, the ability to vote people on the ADA touchscreen devises offers some bandwith protection if turnout is full. Paper ballots are not cheap and in odd-year local elections or in even-year primary elections, with an expected turnout of maybe 30 percent, it has historically not been viewed as imprudent to try to do some surgical targeting of ballot printing numbers.

*Question 11.* Are there best practices that should be used to determine the number of ballots and ballot-marking technology, or voting machine that should be provided to support voting?

Answer. Yes. The best practice is to guarantee you can meet the highest foreseeable demand at any location during any election. There are available wait time calculators to maximize the resource allocations. The Presidential Commission on Election Administration collected and published these resources.

*Question 12.* Are there best practices to address when a natural or man-made event makes a polling location unavailable for voting?

Answer. The Election Assistance Commission (EAC) provides some clearinghouse information in this area. More would be valuable. And I believe it is an upcoming effort of the agency. These are problems we have been dealing with since the beginning of the republic. And taking "Super Storm Sandy" as an example it is evident that election officials have been exceedingly resourceful during this type of event.

*Question 13.* How does allowing voters to vote at locations other than at a single voting location impact the ability of election services to serve voters in a county or State?

Answer. Increasing voting locations opportunities increases the inherent resiliency of a system by distributing the available access points such that there is no single point of failure that would absolutely disenfranchise any one individual. But there are certainly some voter costs associated with travelling further than expected to vote on election day. Its also important to note that there are marginal tradeoffs with changing the voting model away from precincts. Some advocates and election officials believe that strong local oversight at the precinct level provides the best election day assurance against nefarious behavior by the very rare but committed bad acting campaign or voter. Further, some security activists believe they have the best chance of validating data and monitoring voting behavior when elections are managed in digestible chunks, like in the precinct unit.

## Questions From Honorable James R. Langevin for Noah Praetz

*Question 1.* Our system is only as strong as its weakest link, and we need to ensure everyone has this "cyber hygiene" knowledge. Have you found that there's a general lack of knowledge of security vulnerabilities and best practices at the staff level?

Answer. In the past 2 years the overwhelming majority of the profession has grown to fully accept the premise that we rely on technologies and people that are inherently vulnerable. This has been a sea change in our industry. However, there remains a tremendous disparity in the degree to which election officials and their staff will, or can, make the changes necessary to increase their security posture to the highest levels. While there remains plenty to learn, the biggest issue will always remain the operationalization of best practices.

*Question 2.* The risk and vulnerability assessments offered by DHS can be extremely valuable for States and localities. Have you found these assessments for States and local election officials to be useful as you work to secure your election systems, and have you implemented DHS's recommendations?

Answer. The Risk and Vulnerability assessment conducted by DHS at Cook County was tremendously valuable. Though Cook took the security issue seriously for a long time we were still very surprised by what committed, skilled, security tradespeople were able to accomplish on the networks. The findings set the table for years of modernization and transformation. It is critical to note that even with their findings, Cook County was forced to layer the optimal situation on top of the election calendar, resource constraints, probability of a successful attack, and the consequences/risks of operational disruption due to change and regression testing oversites. There are many risks, and election administration is a matter of risk management, cyber and otherwise.

*Question 3.* Do you have the resources you need to implement the recommendations, and if not, what more do you need to do so?

Answer. There were certainly resource deficiencies in Cook County. Those deficiencies are worse almost everywhere else. The demand is not just for modern defensible technology, though that is in short supply. There is a dearth in human skill necessary to operationalize recommendations. Cook County long argued that every election official should have access to an Election Infrastructure Security Officer. For giant counties like Cook, they could hire their own. But that would cost nearly a billion dollars a year to replicate Nation-wide—an impossible and unnecessary investment. A huge security leap could be accomplished by providing the same single human resource across multiple local election official agencies. In Illinois this was handled by a team of "cyber navigators" who have essentially adopted a dozen counties and are helping them mature their election security. The navigators are helping them operationalize the recommendations, not just form DHS, but also from CIS and Belfer. They are helping them procure free services and manage vendors. The key is to do the basics now and utilize the best available shared resources and free resources from the private and public sector.

### Question From Honorable Dina Titus for Noah Praetz

*Question.* When speaking with State and local election officials in Nevada, I have heard that while urban areas like Las Vegas may have the IT workforce available to recruit individuals to implement new cybersecurity measures like Albert sensors, rural areas have been struggling to find trained personnel. Have you experienced this shortage in other parts of the country, and do you believe further investment in STEM education is necessary to effectively mitigate this skills gap and secure our most vulnerable election sites?

Answer. There is no question that there is a skilled professional gap between the workforce needed and that available. This runs not simply through elections Nationwide, but through the all sectors of country. There are millions of jobs in the field unfiled because the workers are not yet available. The demand will continue to grow. And the supply must grow to meet the demand. Given that the cyber risk is top of list from a National security perspective, it would seem appropriate to throw everything including the kitchen sink at it.

### Questions From Honorable Michael T. McCaul for Noah Praetz

*Question 1a.* Mr. Praetz, I share your assessment that we must expect the attackers' methods aimed at our election system will evolve. You described the large role that local officials play in running and securing elections and the critical public partnership.

How can the Federal Government best support these efforts without the all-too-common Federal overreach?

Answer. Overly proscribing tactics and specific actions to be taken can create overreach or the perception thereof; and can lock in actions that won't likely remain necessary or valuable over time. However, the Federal Government could provide investments in the area to the States and local election officials while simultaneously demanding some set of measurable progress to prove the investment is worthy of the taxpayers' sacrifice. I laid out my navigator program support. The Federal Government could invest in such a program without proscribing how the States do it—the model can be different everywhere—and the laboratory effects of those differences highly valuable overtime. However, there are some areas where prescription is more important, particularly around ballot audits. Some level of hand-auditing seems necessary to prove up that the machines are reading them correctly. That's not to exclude additional audits that may be superior to a small hand-counted audit in a vacuum.

*Question 1b.* How will Federal mandates from Washington address the problems you outlined and not just add more bureaucracy?

Answer. A program initiated by the Federal Government which aims to support the protection of the critical infrastructures is necessary. As you rightly note, finding the right balance is critical. Investing in principles is important. My top three principles are (1), sustained, skilled human partnerships with local election officials; (2), investment in technology that is easier to defend and provides the services voter expect; (3), investments in audits that can prove conclusively that trusted and true results are attainable even in the event of software failure. Providing some administrative autonomy to the States and local election officials in satisfying the principles can help those Government bodies own the principles and the management of the project. Retaining some requirements and measurements ensures that the States are accountable for the Federal tax investment.

QUESTIONS FROM HONORABLE SHEILA JACKSON LEE FOR JAKE BRAUN

*Question 1.* Are we taking a fail-safe approach to determining which election systems or processes are critical to the successful conduct of a public election?

Answer. No.

*Question 2.* Would you consider State-wide Centralized Voter Registration Databases a critical system to the administration and conduct of any public election?

Answer. Yes. It is also important to note that the local jurisdictions' voter registration databases are nearly as important as those at the State level.

*Question 3.* What fail-safe measures are in place to assure that if the voter registration database is compromised and thereby make data records untrustworthy; or rendered unavailable for early voting or on election day the casting of ballots will continue?

Answer. To my knowledge, there are no fail-safe technology measures to accomplish this. Many election officials regularly back up their systems and/or use an auditing regime to increase the likelihood that they will be able to detect an attack and restore data that were deleted or changed. However these procedures are not foolproof and their implementation at the local level is just as important as at the State level, yet far from uniform. That being said, same-day voter registration would likely be a sound defense against this attack.

*Question 4.* How many States have plans in place to hold or continue an election should their voter registration databases become compromised?

Answer. I do not know. However, local laws are, in general, unequal to the threat State and locals are facing.

*Question 5.* How many States and jurisdictions within each State use electronic poll books?

Answer. According to the Brennan Center for Justice, at least 34 States plus Washington, DC used electronic pollbooks as of 2017.[1] While it is is possible that some of those States have chosen to discontinue their use due to the 2018 DEF CON report, our preliminary research suggests the opposite. With updated information from State action taken over the last 2 years, there are now at least 41 States that have implemented the use of electronic pollbooks, conducted a pilot program for their use, or approved funds to purchase them for future use. There is no up-to-date accounting for how many jurisdictions within each of those States uses electronic pollbooks, as of 2018. The Brennan Center reports that 5 of the 34 States using electronic pollbooks in 2017 were using them State-wide.

*Question 6.* Are there instances when electronic poll books have failed to operate as intended?

Answer. Yes. In our research at DEF CON, untrained hackers (with no specialized skills or previous access to the machines) found that such devices are vulnerable to hacks via wireless networks, bluetooth, or cellular connections. These vulnerabilities give hackers the ability to compromise such connections and intercept communications between the jurisdiction's main database and a cloud backup service, such as Amazon Web Service (AWS). If attackers can gain access to this cloud backup, they can view the database and potentially control functions along the line of communication. As a result, a single compromised connection in a single polling place could result in unrestricted access to the entire jurisdiction's voter registration database—thereby compromising names, birth dates, addresses, social security numbers, driver's license numbers, addresses, and voting history linked with the individual's signature. In 2017, just such a security lapse was discovered in Illinois when a cybersecurity analyst discovered a database containing sensitive information for more than 1.8 million Illinois voters that was downloadable from a publicly-available AWS storage site controlled by ES&S, one of the major election equipment vendors in the United States.[2]

In addition, software vulnerabilities have been discovered by DEF CON researchers in a line of Diebold electronic poll books, ExpressPoll 5000, which was purchased and is currently operated by ES&S. Investigators at DEF CON discovered that not only were administrator and root passwords to the pollbook's system stored without

[1] "VRM in the States: Electronic Poll-books." *Brennan Center for Justice,* February 6, 2017. Accessed March 14, 2019. *www.brennancenter.org/analysis/vrm-states-electronic-poll-books.*

[2] O'Sullivan, Dan. "The Chicago Way: An Electronic Voting Firm Exposes 1.8M Chicagoans," Upguard (blog), December 13, 2018, *https://www.upguard.com/breaches/cloud-leak-chicago-voters.*

encryption, but they could directly access and modify election parameters using a free, widely available program called SQL Lite.[3]

The biggest concern with compromising these devices is not just corrupting data but also the multi-hour long lines for Election Day and early voting it could cause as confused poll workers try to sort out who can vote and who can't. These lines would further add to a sense that the system doesn't operate properly or is "rigged" against the voter's preferred candidate.

*Question 7.* What recovery plan is in place should a polling location's electronic poll books fail or for periods of time not function?

Answer. To my knowledge, such recovery plans vary dramatically across jurisdictions. In previous elections, we advocated strongly to have paper-based back-up poll books kept on-site in case there was a problem with the machines. However, we often met strong resistance in adopting even this simple fix.

*Question 8.* How well does same-day voter registration during early voting and on election day create meet fail-safe objectives for the successful conduct of a public election?

Answer. Same-day voter registration may be the only nearly fail-safe option available today for mitigating voter registration database and e-poll book attacks.

*Question 9.* Are you providing any guidance on security and wireless non-voting system technology?

Answer. I am sorry, I do not understand the question.

*Question 10.* Do election administrators plan for 100% voter participation during early voting or on election day? If not, why not?

Answer. No. Election administrators use several methods to predict voter turnout, including looking at past voter history; consulting turnout tables, which calculate a probability that an individual will turn out to vote, based on her age and previous voting history; and building regression models.[4]

*Question 11.* Are there best practices that should be used to determine the number of ballots and ballot marking technology, or voting machine that should be provided to support voting?

Answer. Yes. There is a tool maintained by MIT (here) that can help an election administrator determine the optimal assets needed for a precinct to administer an election.

*Question 12.* Are there best practices to address when a natural or man-made event makes a polling location unavailable for voting?

Answer. Not to my knowledge. However, in past elections we encouraged election administrators to treat as an "emergency" any polling place with a line over 30 minutes long.

*Question 13.* How does allowing voters to vote at locations other than at a single voting location impact the ability of election services to serve voters in a county or State?

Answer. Multiple locations provide voters various options to increase ease of voting. It has worked well with early voting but would provide challenges for Election Day voting, especially as it may necessitate more internet connections to devices being used to find people in the registration database.

## QUESTIONS FROM HONORABLE JAMES R. LANGEVIN FOR JAKE BRAUN

*Question 1.* What can be done to improve the relationship between the cybersecurity research community and the election system vendors and ensure that the work of voting security researchers is not ignored by vendors?

Answer. First, vendors can eliminate restrictions on third-party security testing from their contracts. It's ridiculous that in order to buy election equipment, local election officials have to sign away their rights to have independent audits of equipment that they own. It also creates significant risk for security researchers who want to work with election officials, all of which is unnecessary.

[3] University of Chicago Harris Cyber Policy Initiative. *DEF CON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure.* Chicago: The University of Chicago Harris Cyber Policy Initiative, 2017. Accessed February 26, 2019. *https://www.defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf*, The University of Chicago Harris Cyber Policy Initiative. *DEF CON 26 Voting Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure.* Chicago: The University of Chicago Harris Cyber Policy Initiative, 2018. Accessed February 26, 2019. *https://www.defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf.*

[4] Malchow, Hal. "Predicting Turnout in a Presidential Election." Campaigns & Elections 25 (2004): 38–40.

Second, vendors could donate or sell voting equipment for us to inspect at DEF CON and other such events. Fortunately some of the vendors now seem interested in participating in events like DEF CON. Further, there are many local election officials who have expressed interest in holding cyber assessments of their systems, including machines and software from the vendors but have not pursued such efforts from fear of lawsuits from the vendors. Vendors should allow and even facilitate this type of activity instead of quash it. The industry needs all the help it can get with security and as NSA's Rob Joyce said, "Head-in-the-sand security is not security at all."

Possibly the best way to improve relations with the vendors and research community is to fund the development and piloting of open-source voting software. Open-source voting software would allow all interested security researchers to audit and suggest security improvements to our election systems 365 days a year, not just the 3 days of DEF CON. In fact, DHS recently posted an RFP for grants to vendors and researchers, requesting bids for building a "voting system of the future," which could have included open-source voting equipment. Unfortunately, for an undisclosed reason, that RFP was taken down and no one was allowed to bid on it. DHS should repost that RFP and solicit bids to build an open-source voting system.

Further, I applaud DARPA's recent announcement of significant grant dollars being disseminated to researchers to build a secure, open-source voting system. In a welcome departure from the stance of current vendors, the firms who received the DARPA funds have already reached out to DEF CON attendees to engage us early in the process.

*Question 2.* Our system is only as strong as its weakest link, and we need to ensure everyone has this "cyber hygiene" knowledge. Have you found that there's a general lack of knowledge of security vulnerabilities and best practices at the staff level?

Answer. As of 2017, there was a 350,000-person shortage in cyber professionals Nationally.[5] That number is projected to grow to more than 3.5 million world-wide by 2021.[6] It is nearly an impossible task to hire the cyber professionals necessary to put in place the basic cyber hygiene necessary to protect a network much less train the lay people on staff as to their basic hygiene. Moreover, misconceptions as to election officials' relative security, caused in part by words erroneously used by the vendors like "air-gapped," further lead to confusion or a false sense of security.

*Question 3.* The risk and vulnerability assessments offered by DHS can be extremely valuable for States and localities. Have you found these assessments for States and local election officials to be useful as you work to secure your election systems, and have you implemented DHS's recommendations?

Answer. I think these assessments have been invaluable in assisting election officials to understand the depth and breadth of their risk. The assessments also help dispel misconceptions promulgated by industry as to the level of security each jurisdiction has achieved. The most important improvement to make in the assessments is to increase the number of them for local election jurisdictions, as they are the ones who administer elections.

*Question 4.* Do you have the resources you need to implement the recommendations, and if not, what more do you need to do so?

Answer. I believe this question is for the election officials. However, in general, I believe the EAC money was an order of magnitude lower than what is needed to begin to effectively mitigate this problem. All the voter registration databases in the country should be moved to one or more secure, American-owned and -operated clouds like AWS, Google, or Microsoft (among others). Second, touchscreen voting machines should be banned (except for use by the disabled) in favor of paper ballots counted by secure optiscan machines. The DHS assessment teams should be quintupled so that all 50 States and the top 30 largest local jurisdictions (which vote nearly 85% of the U.S. population) can be assessed biannually, and the other nearly 8,000 jurisdictions can get at least a remote assessment once every other year. Further, these teams should help train local IT staff to plan and implement remediation plans based on the DHS assessments, especially including election night reporting website security and breach protocols. Finally, funding should be allocated for DHS to disseminate grants for research and development on building the voting machines of the future.

[5] "Cybersecurity Jobs Report 2018–2021." Cybersecurity Ventures, May 31, 2017. Accessed March 13, 2019. *https://cybersecurityventures.com/jobs/*

[6] "Cybersecurity Jobs Report 2018–2021." Cybersecurity Ventures, May 31, 2017. Accessed March 13, 2019. *https://cybersecurityventures.com/jobs/*

### QUESTION FROM HONORABLE DINA TITUS FOR JAKE BRAUN

*Question.* When speaking with State and local election officials in Nevada, I have heard that while urban areas like Las Vegas may have the IT workforce available to recruit individuals to implement new cybersecurity measures like Albert sensors, rural areas have been struggling to find trained personnel. Have you experienced this shortage in other parts of the country, and do you believe further investment in STEM education is necessary to effectively mitigate this skills gap and secure our most vulnerable election sites?

Answer. As of 2017, there was a 350,000-person shortage in cyber professionals Nationally.[7] That is projected to grow to more than 3.5 million world-wide by 2021.[8] It is a LITERALLY impossible task to hire the cyber professionals necessary to put in place the basic cyber hygiene necessary to protect an election system. They simply can't compete with industry and the Federal Government for the workforce. Moreover, misconceptions as to election officials' relative security, caused in part by words erroneously used by the vendors like "air-gapped," further lead to confusion or a false sense of security. While further investment in STEAM is undoubtedly critical to solving this problem long-term, those investments could take a decade to bear fruit. We should still make the investments.

However, we must find creative ways to "hack" the work force problem for election officials. HB1 has a creative solution with its provision for a bug bounty program, akin to "Hack the Pentagon," that crowdsources security for local election officials. Further, specifying that some of the R&D funding in HB1 be allocated for development of open-source voting equipment, would enable thousands of security experts to audit the code of voting equipment and suggest fixes. Open-source equipment offers an inexpensive, persistent, and adaptable opportunity to dramatically increase the cyber workforce without local election officials being required to recruit, hire, and retain cyber professionals. Finally, outsourcing voter registration database security by providing State and local election administrators grants to migrate their data to a secure, American-owned and -operated cloud like AWS, Google, or Microsoft would remove database security burdens from local election officials and assign it to organizations who can afford to recruit and retain the best security professionals in the business.

### QUESTIONS FROM HONORABLE SHEILA JACKSON LEE FOR JOHN H. MERRILL

*Question 1.* Are we taking a fail-safe approach to determining which election systems or processes are critical to the successful conduct of a public election?

Answer. No. The Alabama Secretary of State's Office believes that the only effective method to determine which election systems are critical to the process is with direct guidance and input from the Secretaries of State.

*Question 2.* Would you consider State-wide Centralized Voter Registration Databases a critical system to the administration and conduct of any public election?

Answer. State-wide Centralized Voter Registration Databases are the most critical component to the current democratic institutions that we have created for the people of this country to voice their political preferences. These provide detailed information that allows Secretaries of State to effective plan an election for the people of their State, county, or local municipality.

*Question 3.* What fail-safe measures are in place to assure that if the voter registration database is compromised and thereby make data records untrustworthy; or rendered unavailable for early voting or on election day the casting of ballots will continue?

Answer. There is no true fail-safe to ensure that a compromise does not occur; however, a systematic approach to augment any system or user data damage can only be accomplished with daily system back-ups, additional layers of security including two-factor authentication, and verification that even in the event of total loss of access or systems locally would not eliminate the existence of those records and that can be restored to a system without any down time.

*Question 4.* How many States have plans in place to hold or continue an election should their voter registration databases become compromised?

Answer. Alabama does.

I am unable to answer this question, but I am hopeful that each and every State has a plan in place should their voter registration databases be compromised.

[7] "Cybersecurity Jobs Report 2018–2021." Cybersecurity Ventures, May 31, 2017. Accessed March 13, 2019. *https://cybersecurityventures.com/jobs/*

[8] "Cybersecurity Jobs Report 2018–2021." Cybersecurity Ventures, May 31, 2017. Accessed March 13, 2019. *https://cybersecurityventures.com/jobs/*

*Question 5.* How many States and jurisdictions within each State use electronic poll books?

Answer. As Alabama's Secretary of State I can only speak for Alabama and at this time there are 30 of 67 Alabama counties utilizing the electronic poll book systems.

*Question 6.* Are there instances when electronic poll books have failed to operate as intended?

Answer. With a few minor exceptions electronic poll books have worked as intended. Those minor exceptions have involved age-related camera issues where the camera used to scan barcodes was not strong enough to pick up the driver's license barcode in low light and another issue occurred when a county employee failed to complete all of the steps to load a voter's list onto the system.

*Question 7.* What recovery plan is in place should a polling location's electronic poll books fail or for periods of time not function?

Answer. The Secretary of State's Office recommends that every county retain a paper copy of that precinct's poll list at each polling site, but ultimately that is left up to the discretion of the Judge of Probate in each county.

*Question 8.* How well does same-day voter registration during early voting and on election day create meet fail-safe objectives for the successful conduct of a public election?

Answer. In Alabama it does not meet or create fail-safe objectives, it simply creates a system without security mechanisms and attempts to pass it off as a solution.

*Question 9.* Are you providing any guidance on security and wireless non-voting system technology?

Answer. We provide guidance and require cybersecurity and ethics training to all the State and county users that work in the Secretary of State's Office or have access to the voter registration system.

Additionally, Alabama's system utilizes paper ballots which once voted are retained for at least 22 months following an election, as required by Federal law.

*Question 10.* Do election administrators plan for 100% voter participation during early voting or on election day? If not, why not?

Answer. In Alabama, electronic voting machines must be placed at each polling location based on the number of voters assigned to that polling place (2,400 voters per machine). So, pertaining to machines, there is no projection involved. It is a set number.

Regarding the printing of ballots and ballot styles, some counties choose to print the exact number of ballots for voters assigned to that polling location, and some counties prefer to project the turnout, obviously leaning towards the highest projected turnout number to ensure enough ballots. The reason some counties would not print one ballot per voter is due to the cost of ballots.

It is also important to have an understanding with the local ballot printing vendor that they will deliver, in-person on election day, additional ballots to any polling place that is getting low. This has happened in the past in Alabama, and the vendor has done their part to ensure enough ballots. Some States may not have the ballot printing vendor in their State and would be forced to print one ballot per voter.

*Question 11.* Are there best practices that should be used to determine the number of ballots and ballot marking technology, or voting machine that should be provided to support voting?

Answer. In Alabama according to State law and administrative rule, an electronic voting machine must be assigned for every 2,400 voters in each polling place. Working with vendors to determine the number of voters that should be associated with a machine for proper flow on Election Day is a must, as well as the number of ballots and ballot styles should be printed for that polling place.

*Question 12.* Are there best practices to address when a natural or man-made event makes a polling location unavailable for voting?

Answer. The best practice is preparation. In Alabama, County Commissions should identify emergency back-up polling locations in each area in the case that one or more assigned polling locations is damaged. In the case in which a polling place must change, the county would need to hold an emergency meeting, designate the new polling place(s) to be used and the electronic voting machines to be placed in those polling places, and provide the list of new polling places to the judge of probate and board of registrars. Immediately upon changing the polling place, the county must notify all affected voters and publicize the change via newspaper and any/all other effective means of communication including social media.

*Question 13.* How does allowing voters to vote at locations other than at a single voting location impact the ability of election services to serve voters in a county or State?

Answer. Alabama State law requires voters to vote at the polling place assigned to them. Also, in Alabama, electronic voting machines must be placed at each polling location based on the number of voters assigned to that polling place (2,400 voters per machine).

The preparation and planning for the number of voting machines, ballots, ballot styles, poll books and electronic books, election workers, election supplies, parking and disabled ballot marking devices per polling place is one of the most important aspects of an election. Understanding the number of voters assigned to a specific polling place and planning resources around that number is vital in our election preparation.

### Questions From Honorable James R. Langevin for John H. Merrill

*Question 1.* Our system is only as strong as its weakest link, and we need to ensure everyone has this “cyber hygiene” knowledge. Have you found that there’s a general lack of knowledge of security vulnerabilities and best practices at the staff level?

Answer. No. We have an outstanding team here at the Alabama Secretary of State’s Office, however, it is difficult to hire staff that we can compensate based on the current salary schedule that is available from the private sector.

*Question 2.* The risk and vulnerability assessments offered by DHS can be extremely valuable for States and localities. Have you found these assessments for States and local election officials to be useful as you work to secure your election systems, and have you implemented DHS’s recommendations?

Answer. We have utilized the assessments from DHS on more than one occasion to review our system and to ensure that any vulnerabilities that existed were resolved prior to an election.

*Question 3.* Do you have the resources you need to implement the recommendations, and if not, what more do you need to do so?

Answer. In all of the instances reported to the Secretary of State’s office we have had the resources to implement the recommendations that were made from the cyber assessments. However, many of those would not have been possible without the grant funds already allotted to the Secretary of State’s office.

Additionally, recently DHS has begun to undertake a review of county offices. Many of those recommendations will be for things that are much more expensive, and many are hesitant to schedule their review because they know they will be made aware of a large number of issues.

### Question From Honorable Dina Titus for John H. Merrill

*Question.* When speaking with State and local election officials in Nevada, I have heard that while urban areas like Las Vegas may have the IT workforce available to recruit individuals to implement new cybersecurity measures like Albert sensors, rural areas have been struggling to find trained personnel. Have you experienced this shortage in other parts of the country, and do you believe further investment in STEM education is necessary to effectively mitigate this skills gap and secure our most vulnerable election sites?

Answer. Investment in education in rural areas is something that would benefit the people of those locations but that would help solve the problem in the long term. Short-term solutions to this problem require additional resources and smart hiring processes.

### Questions From Honorable Yvette D. Clarke for John H. Merrill

*Question 1a.* Last year, the FBI uncovered that a Russian oligarch, with close ties to President Putin, had acquired an ownership interest in a vendor which hosted State-wide election data for Maryland.[1] Until the FBI alerted them, State election authorities were unaware of the vendor’s ties to Russia. Even if no tampering occurred, this raises important questions about foreign ownership of firms providing election-related services.

To the best of your knowledge, does your State have any election-related contracts with vendors backed by Russian or Chinese investors?

Answer. To the best of my knowledge the State of Alabama does not have any vendors backed by Russian or Chinese investors.

*Question 1b.* What measures, if any, does your State undertake to assess foreign ownership of election vendors prior to signing contracts with them?

Answer. The Alabama Secretary of State’s office reviews all the financial documentation associated with each company before entering into a contract with them.

[1] *https://www.baltimoresun.com/news/maryland/politics/bs-md-election-russia-20180713-story.html.*

Additionally, we require all business that do business with us to be registered with the State of Alabama before we enter into an agreement for services. The contract for Alabama's current voter registration system is about to be put up for bid again and will include requirements for all companies to disclose any foreign ownership or investment in their company before they are considered by the office for use in Alabama.

### QUESTION FROM HONORABLE MICHAEL T. MCCAUL FOR JOHN H. MERRILL

*Question.* Foreign states, including Russia and other malicious actors have and will continue to attempt to interfere with U.S. elections. In fact, I encouraged, in a Classified space, both the Obama administration and the Trump administration to call out Russia for their targeted attacks on our Nation. Their activities have injected chaos and doubt into foundation of our democracy. An issue of this gravity requires Congress to act in a deliberate and bipartisan manner. Now, all eyes are on 2020. How has the cooperation with DHS and Director Krebs strengthened California's election security?

Answer. The Alabama Secretary of State's Office has benefited from the increased relationship with the Department of Homeland Security. This relationship has allowed us to secure our systems by implementing a multitude of security equipment and tools to strengthen the States' election systems. Additionally, DHS has provided a team from the Department of Homeland Security that has been present with our IT staff on election day to provide direct contact in the event of a breach or other system problem.

○