SECURING U.S. ELECTION INFRASTRUCTURE AND PROTECTING POLITICAL DISCOURSE

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY

OF THE

COMMITTEE ON OVERSIGHT AND REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

MAY 22, 2019

Serial No. 116–28

Printed for the use of the Committee on Oversight and Reform

Available on: *http://www.govinfo.gov*
http://www.oversight.house.gov or
http://www.docs.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

36–662 PDF WASHINGTON : 2019

COMMITTEE ON OVERSIGHT AND REFORM

ELIJAH E. CUMMINGS, Maryland, *Chairman*

CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
JAMIE RASKIN, Maryland
HARLEY ROUDA, California
KATIE HILL, California
DEBBIE WASSERMAN SCHULTZ, Florida
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont
JACKIE SPEIER, California
ROBIN L. KELLY, Illinois
MARK DESAULNIER, California
BRENDA L. LAWRENCE, Michigan
STACEY E. PLASKETT, Virgin Islands
RO KHANNA, California
JIMMY GOMEZ, California
ALEXANDRIA OCASIO-CORTEZ, New York
AYANNA PRESSLEY, Massachusetts
RASHIDA TLAIB, Michigan

JIM JORDAN, Ohio, *Ranking Minority Member*
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
VIRGINIA FOXX, North Carolina
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
JODY B. HICE, Georgia
GLENN GROTHMAN, Wisconsin
JAMES COMER, Kentucky
MICHAEL CLOUD, Texas
BOB GIBBS, Ohio
RALPH NORMAN, South Carolina
CLAY HIGGINS, Louisiana
CHIP ROY, Texas
CAROL D. MILLER, West Virginia
MARK E. GREEN, Tennessee
KELLY ARMSTRONG, North Dakota
W. GREGORY STEUBE, Florida

DAVID RAPALLO, *Staff Director*
DAN REBNORD, *Subcommittee Staff Director*
AMY STRATTON, *Clerk*
CHRISTOPHER HIXON, *Minority Staff Director*
CONTACT NUMBER: 202-225-5051

SUBCOMMITTEE ON NATIONAL SECURITY

STEPHEN F. LYNCH, Massachusetts, *Chairman*

JIM COOPER, Tennessee
PETER WELCH, Vermont
HARLEY ROUDA, California
DEBBIE WASSERMAN SCHULTZ, Florida
ROBIN L. KELLY, Illinois
MARK DESAULNIER, California
STACEY E. PLASKETT, Virgin Islands
BRENDA L. LAWRENCE, Michigan

JODY HICE, Georgia, *Ranking Minority Member*
JUSTIN AMASH, Michigan
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
MARK MEADOWS, North Carolina
MICHAEL CLOUD, Texas
MARK E. GREEN, Tennessee

C O N T E N T S

INDEX OF DOCUMENTS

The document listed below is available at: https://docs.house.gov.

SECURING U.S. ELECTION INFRASTRUCTURE AND PROTECTING POLITICAL DISCOURSE

Wednesday, May 22, 2019

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY,
Committee on Oversight and Reform,
WASHINGTON, D.C.

The subcommittee met, pursuant to notice, at 2:03 p.m., in room 2154, Rayburn House Office Building, Hon. Stephen Lynch presiding.

Present: Representatives Lynch, Cummings, Cooper, Welch, Rouda, Wasserman Schultz, Kelly, Sarbanes, Hice, Jordan, Amash, Gosar, Foxx, Meadows, and Green.

Also present: Representative Sarbanes.

Mr. LYNCH. The subcommittee will come to order.

Without objection, the Chair is authorized to declare a recess of the committee at any time.

This hearing is entitled, "Securing U.S. Election Infrastructure and Protecting Political Discourse."

I now recognize myself for five minutes to give an opening statement.

Today we will examine the security of our Nation's election infrastructure systems, as well as how the Federal Government is working with private-sector partners to respond to malicious attempts to unduly influence public opinion, sow discord, and undermine confidence in our political institutions.

The purpose of today's hearing is not to re-litigate the outcome of the 2016 Presidential election. Rather, our goal is to safeguard the fundamental democratic principles underscored by President Abraham Lincoln when he said that "Elections belong to the people." Indeed, no less than the integrity of our democracy is now at stake.

In January 2017, the intelligence community released an assessment that our democracy had come under attack by foreign adversaries. With high confidence, our Nation's 17 intelligence agencies unanimously found that "Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. Presidential elections." The Russian effort included clandestine intelligence operations coupled with blatant meddling by Russian government agencies, state-funded media organizations, third-party intermediaries, and paid social media users, or trolls.

Special Counsel Robert Mueller's report, which followed his nearly two-year independent investigation into Russian interference, confirmed and augmented the intelligence community's high con-

fidence judgment. According to the Special Counsel, "The Russian Government interfered in the 2016 Presidential election in sweeping and systematic fashion."

Thanks to the Special Counsel, we know that Russia's interference campaign involved so-called "active measures" led by the St. Petersburg-based Internet Research Agency designed to sow discord in the U.S. through information warfare. Its primary components included the creation of fictitious social media accounts, the purchase of online ads to promulgate divisive political material, the deployment of automated bots to amplify content, and the organization of political rallies in the U.S. At the same time, Russia's military agency, the GRU, perpetrated a hacking operation targeting U.S. individuals, political committees, state election boards, state secretaries of state, county governments, and private manufacturers of election-related software and voting machines. In response to these malign activities, the Special Counsel criminally indicted 13 Russian nationals, 12 military officers, and three Russian companies.

In its post-election review, Facebook alone estimated that accounts controlled by the IRA may have reached 126 million people prior to their deactivation in August 2017, including nearly 30 million Americans.

Russian interference in U.S. elections has continued beyond 2016, with Iran, China, and other hostile state actors following suit. In September 2018, the midterm elections, the Department of Justice charged a Russian national with conspiring to interfere in the 2018 midterm elections in connection with her work as a chief accountant for "Project Lakhta," a social media influence campaign funded by the same Russian oligarch already indicted by the Special Counsel for financing the Internet Research Agency. On the eve of the midterms, Facebook announced that it had suspended over 100 Facebook and Instagram accounts due to their potential affiliation with the Internet Research Agency.

In submitting a classified intelligence community report on foreign interference in December 2018, Director of National Intelligence Dan Coats stated: "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."

As we approach the 2020 Presidential election cycle, U.S. intelligence officials and security experts have warned that malign foreign influence operations will continue to evolve.

According to FBI Director Christopher Wray, Russia likely viewed its influence activities in 2018 as a "dress rehearsal for the big show in 2020." In his 2019 Worldwide Threat Assessment, DNI Director Coats added: "We expect our adversaries and our strategic competitors to refine their capabilities and add new tactics as they learn from each other's experiences, suggesting the threat landscape could look very different in 2020 and future elections."

The nonpartisan Brookings Institution predicts that foreign state actors will increasingly rely on artificial intelligence to conduct political warfare in the form of disinformation campaigns that are almost impossible to detect. To this end, our adversaries are refining the use of so-called "deep fakes." These are synthetically doctored

audio, photos, and videos that are highly believable, inexpensive to produce, and have unlimited potential to go viral. Foreign influence campaigns are also trending toward subtler and harder-to-detect tactics, including by targeting specific audiences and amplifying divisive organic content over the creation of fake news and accounts, which are easier to identify.

In light of these threats, we must undertake a frank and bipartisan assessment of the vulnerabilities that remain in our electoral process.

While the Department of Homeland Security has established multiple task forces to combat foreign election interference, the DHS Inspector General reports that their effectiveness has been undermined by dramatic staffing cuts, leadership turnover, and a lack of coordination with state election officials. Meanwhile, the Election Assistance Commission, which is responsible for administering the $380 million in state grant funding that Congress appropriated for election security in 2018, is experiencing a shortfall of technical expertise, including the recent departure of its top technology official in charge of testing and certifying voting systems.

Information sharing among intelligence agencies, state and local governments, and private-sector technology companies has markedly increased since 2016. However, there is still significant room for improvement. The FBI's recent notification to state and local officials in Florida that Russian operatives had successfully hacked voter registration files in two counties in 2016 came nearly three years after the breach and over six months after the 2018 midterms.

Social media companies and Federal law enforcement agencies also must continue to improve their ability to communicate specific threat information and potential vulnerabilities in real time.

Securing the integrity of our electoral process will require a collective and renewed commitment on the part of the public and private sectors to address these and other challenges. Only then can we be confident that future elections in the United States truly reflect the will of the American people.

I now yield to the Ranking Member, the gentleman from Georgia, Mr. Hice, for his opening statement.

Mr. HICE. Thank you very much, Mr. Chairman.

We all know that voting is a bedrock of our republic. It is grounded in the principle of federalism and a fundamental right we as Americans enjoy and take pride in. It is imperative that our election systems are secured so that Americans can have full confidence that their vote is heard on election day.

Not only are we here to discuss the importance of ensuring the security of our election systems but also how we protect political discourse on the social media platforms like Facebook, Twitter, and YouTube leading into Americans casting their vote.

The Federal agencies on our first panel, along with others, play an important role in aiding state and local election officials who are ultimately responsible for administering the elections.

In January 2017, in order to reduce both cyber and physical risk to state and local election systems and facilities, the Department of Homeland Security designated our election systems as a critical

piece of our country's infrastructure. As a result, state and local election officials can now receive a wide range of services to reduce both cyber and physical risk to their election systems and facilities.

Additionally, in March of last year, President Trump signed the Consolidated Appropriations Act which provided another $380 million for grants disbursed by the Election Assistance Commission to state and local election officials to improve election administration. So I look forward to hearing from Chairwoman McCormick more about the EAC's partnership with state and local election officials and how they are putting that money to good use.

Later this afternoon we will hear from Facebook, Twitter, and Google representatives to understand the role of these private-sector companies in safeguarding our political process. These three entities have become such a centerpiece in the discourse of our Nation and our politics. I think we are all aware of that. Think about the presence and reach of social media platforms today. Facebook has over 2.3 billion monthly users, Twitter over 330 million, and Google over 2 billion. These platforms obviously have a massive audience. Accordingly, it is vital that these companies are fully transparent on their platforms. These platforms should advance freedom of speech, not censor it. Yet, we find again and again that some accounts are suspended or banned for unclear reasons. So I look forward to discussing how some accounts are banned or suspended for bad content and who is making that determination, and why.

Additionally, social media companies should play an active role in securing their platforms by limiting the spread of misinformation, providing transparency of political advertising, while also blocking and removing fake accounts seeking to manipulate the public.

It is no secret that Russia, Venezuela, Iran and other foreign adversaries seek to interfere in our political process. These bad actors have and will likely seek to challenge the credibility of our election system, the very fundamental part of our republic. We must safeguard our systems and our platforms and deter future attempts by all foreign adversaries. It is my understanding that during 2018, Twitter challenged about 425 million accounts that were suspected of engaging in spam or platform manipulation. Of that amount, roughly 75 percent have been suspended or removed. Between October 2017 and March 2018, Facebook disabled 1.27 billion fake accounts.

I think it is important to note that there is a clear distinction between content from foreign adversaries versus content with which people disagree.

So we have a lot to unpack this afternoon. I look forward to hearing from our witnesses on their roles and responsibilities to safeguard and protect the integrity of our elections, and I thank the Chairman, and I yield back.

Mr. LYNCH. The gentleman yields back.

Without objection, the gentleman from Maryland, Mr. Sarbanes, who is a full committee member and author of H.R. 1, the For the People Act, which seeks to address some of the issues that we raised today, shall be permitted to join the subcommittee on the dais and be recognized for his questions of the witnesses at the appropriate time.

Today we are joined by the Honorable Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security; Adam Hickey, Deputy Assistant Attorney General, National Security Division, U.S. Department of Justice; the Honorable Christy McCormick, Chairwoman, U.S. Election Assistance Commission; and the Honorable Ellen Weintraub, Chairwoman, U.S. Federal Election Commission.

If the witnesses would please rise, I will begin by swearing you in. Please raise your right hand.

[Witnesses sworn.]

Mr. LYNCH. Let the record show that the witnesses answered in the affirmative.

Thank you, and please be seated.

The microphones are sensitive, so please speak directly into them. And without objection, your written statements will be made part of the record.

With that, Mr. Krebs, you are now recognized to give an oral presentation of your testimony.

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

Mr. KREBS. Chairman Lynch, Ranking Member Hice, and members of the subcommittee, good afternoon and thank you for the opportunity to testify regarding the Department of Homeland Security's efforts to secure the vote.

Cyber threats, particularly from nation-state actors, remain one of the most strategic threats to the United States. Perhaps the highest profile threats we face today are attempts by nation-state actors to interfere in our democratic elections.

Our goal has been for the American people to enter the voting booth with confidence that their vote counts and is counted correctly. I want to update this committee on the progress made in working with the election community. Our agency, the Cybersecurity and Infrastructure Security Agency, or CISA, our mission is clear: to support election officials and their private-sector partners consistent with the Constitution, existing law, and electoral tradition.

At its core, elections are run at the state and local level, but those officials shouldn't have to defend themselves from nation-states on their own.

Since 2016, we have learned quite a bit. We have done after-action reviews, the Department of Justice conducted an investigation and issued indictments in some cases, Offices of Inspectors General and the General Accountability Office and multiple committees in Congress have or are investigating what happened and how we can improve our efforts to secure elections.

Over the last two years, in focused and oftentimes humbling engagements, we have become partners with the election community. For the 2018 election, alongside the Election Assistance Commission, we worked with all 50 states, over 1,400 local and territorial election offices, six election associations, and 12 election vendors.

Our approach is three-fold: first, making sure the election community has the information they need to defend their systems; sec-

ond, making sure they have the technical support and tools they need to defend their systems; and third, building enduring partnerships to advance security efforts together.

In 2018, we focused on building scalable, repeatable mechanisms to dramatically grow our information-sharing capabilities. The Election Infrastructure and Information Sharing and Analysis Center, or EI-ISAC, was established. By election day, the EI-ISAC had over 1,400 members, including all 50 states. This is the fastest growing ISAC of any critical infrastructure sector. That ISAC now has over 1,600 local jurisdictions participating.

We shared contextualized threat intelligence and actionable information through our close partnerships 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 of malicious activity. By election day 2018, those sensors offered protection to election infrastructure in voter registration data bases for more than 92 percent of registered voters. For reference, during the 2016 election, we were below 30 percent of coverage. That is real improvement.

Second, we provided technical support and services to election officials and vendors. Initially, we offered the standard services, including vulnerability assessments that we offer Federal agencies and other sectors. As we refined our understanding of election official requirements, we shifted the capabilities quicker, less intrusively, and can scale to more jurisdictions.

This scalability is critical, because while our initial efforts in 2016 were primarily targeted at state election officials, we recognized 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.

While on the surface it seems simple, this initiative provided no-cost, tailored information on cyber risks and a checklist of cyber security action items.

The final area of focus has been on building enduring partnerships toward a collective defense. It may seem mundane, but governance, communications, coordination, training, and planning are the critical foundational elements of our efforts to secure the Nation's elections. These efforts and others contributed to a secure 2018 election.

While 2018 is behind us, the 2020 election season is already underway. We are clear-eyed that the threat to our democratic institutions remains, and we must continue to press for increased security and resilience of our election systems. Over the next two years, CISA will focus on expanding engagement at the local level. We will also continue to work with election officials to improve both their and our understanding of risk. With a better understanding of risk, we can support efforts by election officials to obtain the resources they need to secure their election systems.

We at CISA are committed to working with Congress to ensure our efforts cultivate a safer, more secure and resilient homeland.

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

Mr. LYNCH. Thank you, Mr. Krebs.

Mr. Hickey, you are now recognized.

STATEMENT OF ADAM HICKEY, DEPUTY ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. HICKEY. Good afternoon, Chairman Lynch, Ranking Member Hice, and distinguished members of the subcommittee. Thank you for the opportunity to testify on behalf of the Department of Justice concerning our efforts to ensure the safety and security of our Nation's election infrastructure and to combat malign foreign influence.

By malign foreign influence, I am referring to covert actions by foreign governments intended to affect U.S. political sentiment and public discourse, sow divisions in our society, or undermine confidence in our democratic institutions. These can range from computer hacking that targets election infrastructure or political parties to state-sponsored media campaigns.

This issue, protecting the Nation's democratic processes, has been and remains a top priority of the Department. Our principal role here is the investigation and prosecution of Federal crimes. But malign foreign influence efforts extend beyond efforts to interfere with elections, and they require more than mere law enforcement responses alone.

Recognizing that, we approach this issue the same way we approach other national security threats, by using our own legal tools, as well as supporting the tools and authorities of others. And to the best of our ability, we try to prevent crimes from occurring or disrupt them in progress, in part by sharing information that enables people to protect themselves.

Reflecting the priority of these issues, last year the Attorney General's Cyber Digital Task Force analyzed the types of foreign influence operations that exist and lays out a framework to guide our responses. Since the 2016 election, the Department has taken a number of steps to combat malign foreign influence and support secure elections.

First, as an intelligence-driven organization and member of the intelligence community, the FBI can pursue tips and leads, including from classified information, to identify, investigate, and disrupt illegal foreign influence activities. To that end, the FBI established the Foreign Influence Task Force to lead its response to ensure information flow, resource allocation, and coordination both within the Department and among the Department, other Federal partners, and the private sector.

Second, together with other agencies, through a series of outreach and education efforts, we have been helping public officials, candidates, and social media companies to harden their own networks and platforms against malign foreign influence operations.

Third, we have improved enforcement of the Foreign Agents Registration Act, one of the statutory tools that helps ensure transparency in the activities of foreign entities and individuals. FARA

enforcement makes it more difficult for those entities and individuals to hide their role in activities occurring in the United States.

Fourth, our investigations have led to a number of criminal charges and other enforcement actions that have exposed malign influence efforts by foreign states and their proxies. While we work with other nations to obtain custody of foreign defendants whenever possible, just the charges themselves help educate the American public about the threats that we face.

Fifth, our investigations have supported the actions of other U.S. Government agencies such as financial sanctions imposed by the Secretary of the Treasury.

Finally, even outside the context of criminal charges, we have used the information from our investigations both to warn and to reassure potential victims and the general public alike about malign foreign influence activities. Victim notifications, defense of counterintelligence briefings, and public safety announcements are traditional Department activities, but they must be conducted with particular sensitivity in the context of foreign influence and elections. In some circumstances, exposure can be counter-productive or otherwise imprudent.

Given those countervailing considerations, the Department has adopted a public policy for evaluating whether and how to disclose malign foreign influence activities, and among its first principles, partisan political considerations must play no role in our decisions.

Our adversaries will undoubtedly change their tactics as technology changes, and we will need to be nimble in our response. But the framework we developed last year will aid us to respond, and I believe it will have staying power.

As you can see, the Department plays an important role in combatting foreign efforts to interfere in our elections, but there are limits to our role and the role of the Federal Government more generally in combatting malign foreign influence. Doing so effectively requires a whole-of-society approach that relies on coordinated actions by government agencies at various levels, support from the private sector, and the active engagement of an informed public.

Thank you again for the invitation to testify today, and I look forward to your questions.

Mr. LYNCH. Thank you, Mr. Hickey.

Ms. McCormick, you are now recognized for five minutes.

STATEMENT OF CHRISTY MCCORMICK, CHAIRWOMAN, U.S. ELECTION ASSISTANCE COMMISSION

Ms. MCCORMICK. Good afternoon Chairman Lynch, Ranking Member Hice, and members of the subcommittee. Thank you for the opportunity to testify before you to detail the important work of the U.S. Election Assistance Commission, better known as the EAC, and our role in helping election officials secure elections.

While 531 days remain until the 2020 Presidential election, the first Federal Presidential primary is just seven months away, and election officials across the Nation are administering state and local elections now. As you know, the EAC and its vital mission were established under the Help America Vote Act of 2002. The EAC is the only Federal agency solely devoted to supporting elec-

tion officials in their work. It is as needed today as it has been at any other time since it was established.

One of the Commission's primary focuses is election security, and I am pleased to have this opportunity to provide more detail about our efforts in that regard. Before I do, however, it is important to put that work into context.

Election security is only one component of election administration. To demonstrate this, the EAC has developed a wheel of competencies in which each section represents a similar level of expertise and effort. The Election Administrator Competency Wheel visualizes ongoing duties, election preparation work, as well as responsibilities stemming from election night and beyond. The 20 areas of competency represented on the wheel are each important and require support from our team, and many of these competencies play a direct role in election officials' work to secure elections.

The EAC has worked diligently to help states secure their elections, especially in the 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.

As the agency best positioned to communicate directly with election officials across the country, the EAC also played an early and leading role in establishing trust and open lines of communication between state and local leaders and the Federal Government entities that work on election security. The EAC drove the development of the Election Security Working Group that eventually became the subsector's Government Coordinating Council, GCC, and played an integral role in establishing the Sector Coordinating Council, SCC, comprised of private election equipment manufacturers and vendors.

Beyond the GCC and SCC, the Commission has taken a multifaceted approach to helping state and local election officials strengthen their election security. This work includes testing and federally certifying voting systems, providing hands-on security and post-election audit trainings across the country, producing security-focused resources, disseminating security best practices information and checklists to state and local election officials, as well as hosting widely attended forums that feature security experts as speakers.

The distribution of HAVA funds is another example of the EAC's work related to election security. Last year, Members of Congress provided $380 million in much needed and much appreciated financial support to the states and territories through the EAC. We know from state plans and expenditure reports that most states are spending these funds on items that will directly improve election security. In fact, at least 90 percent of the funds have been devoted to technological and cyber security improvements, the purchase of new voting equipment, and improvement to voter registration systems.

Through our more recent conversations with all 55 states and territories that receive these funds, we believe that as of April 30th, 2019, states have spent at least $108.14 million, or 29 per-

cent of the $380 million in grant funds. This represents a 262 percent increase in spending from the last reported spending levels in September of last year.

As states seek to invest these funds in purchasing new voting equipment, election leaders are continuing to turn to the EAC's testing and certification program as a key resource in ensuring the Nation's voting systems are tested to confirm the secure and accurate tabulation of ballots. This includes seeking information about when the EAC will implement the next iteration of the Voluntary Voting Systems Guidelines, which will be known as VVSG 2.0.

The VVSG has historically consisted of principles, guidelines, and requirements against which voting systems can be tested to determine if the system meets required standards. These guidelines are voluntary, and states may decide to adopt them entirely or in part. Last year, the EAC's Technical Guidelines Development Committee, as well as the EAC's Board of Advisors and Standards Board recommended adoption of the proposed guidelines and principles. Unfortunately, when one of the commissioners left the EAC, we lost our quorum and were not able to vote to move the guidelines forward. After Commissioner Palmer and Commissioner Hublin were confirmed and a quorum was restored, our first official act was to unanimously vote to publish the principles and guidelines in the Federal Register for a 90-day public comment period.

In April we held public hearings in Memphis and Salt Lake City, and on Monday we held our third hearing at our office in Silver Spring. The public comment period on the principles and guidelines concludes on May 29th.

It is important to note that the EAC's participation in critical infrastructure activities and its own security work was a direct result of the personal involvement and direction of the EAC's most senior staff, as well as the efforts of our talented team of professionals. The EAC does not have full-time employees devoted to these new components of providing election security support.

As we provide for 2020 and beyond, the EAC looks forward to working with Congress as we continue our efforts to help America vote, including work to secure elections.

I am happy to answer any questions you may have following today's testimony. Thank you.

Mr. LYNCH. Thank you, Ms. McCormick.

Ms. Weintraub, you are now recognized for five minutes.

STATEMENT OF ELLEN L. WEINTRAUB, COMMISSIONER, U.S. FEDERAL ELECTION COMMISSION

Ms. WEINTRAUB. Thank you. Chairman Lynch, Ranking Member Hice, and members of the committee, thank you for inviting me to testify before you today, and thank you for convening this hearing in this subcommittee, because the integrity of our elections is a matter of national security. I welcome the committee's forward-looking approach to the ongoing cybersecurity and disinformation threats to our election infrastructure, especially as we head into the 2020 elections. I share your concerns about foreign threats to the integrity of our country's elections.

And I bring some good news. The Commission yesterday approved an advisory opinion that will allow Federal campaigns to ac-

cept extensive cybersecurity assistance from a project called Defending Digital Campaigns. They are bipartisan, national security and tech savvy, and they can help protect campaigns from foreign and domestic cyber and information attacks. It is a big step for the FEC to allow a group like this to assist campaigns. We allowed it because of the grave dangers facing campaigns from hackers, and I hope every campaign will take advantage of it.

I am also introducing a proposal at the FEC tomorrow to allow the party committees to use their building funds to pay for cybersecurity for themselves and their candidates. There is a bill on that, but we could do it without legislation, and I hope we will.

We know what happened in 2016. We know that our foreign adversaries can and will repeat their cyber warfare if the U.S. Government does not act boldly and decisively to defend this Nation from such attacks. And make no mistake, our adversaries do not seek partisan advantage. They seek chaos and discord. They seek to undermine our democracy. Just because Russia's attack involved ports on Facebook servers instead of a port in the middle of the Pacific Ocean makes it no less of an attack on our country.

Other witnesses today have and will tell you about how we need to protect the physical infrastructure of our elections, the brick and mortar electoral apparatus run by state and local governments, and it is vital that we do so. But from my seat on the Federal Election Commission, I work every day with another kind of election infrastructure, the foundation of our democracy, the faith that American citizens have that they know who is influencing our elections, and that faith has been under malicious attack from our foreign foes through disinformation campaigns. That faith has been under assault by the corrupting influence of dark money that may be masking illegal foreign sources. That faith has been besieged by online political advertising from unknown sources. That faith has been damaged through cyber attacks against political campaigns ill-equipped to defend themselves on their own.

That faith must be restored, but it cannot be restored by Silicon Valley. Rebuilding this part of our elections infrastructure is not something we can leave in the hands of the tech companies, the companies that built the platforms now being abused by our foreign rivals to attack our democracy. Don't let the guys on the next panel tell you they got this; they don't.

The U.S. Government needs to be the one who steps up to meet this threat. I am doing what I can at the FEC. I revived the Commission's efforts to clarify the rules about Internet advertising disclosure. I have highlighted the dangers of foreign election spending through corporations, LLCs, and dark money groups. The Commission recently obtained record penalties against a Super PAC and a domestic subsidiary that was funneling money into our elections at the behest of foreign owners. So this risk is not hypothetical.

But there is only so much I can do from my seat on the Commission. Congress has more powerful tools available to it, and I urge you to use every tool in your toolbox. There is legislation already drafted that could help, bills like the Honest Ads Act, the Deter Act, the Secure Elections Act. I implore all Members of Congress, regardless of party and regardless of chamber, to speak up now.

Speak up, legislate, pressure leadership to bring those bills to the floor.

And I urge you most of all to do something outside the realm of election law, something that the FEC absolutely cannot do. Congress and the White House must make it abundantly clear to our foes that the costs of attacking America's elections far outweigh the real or perceived benefits. If those who attack our democracy pay no price for doing so, the damage they will continue to wreak will swallow up any other reform we could possibly enact.

In the best of all possible FEC worlds, I could crack down on dark money. In the best of all possible FEC worlds, I could provide greater transparency for online political debate. But nothing that I do will matter unless Congress and the White House convey with unmistakable clarity and unity that our democracy is not to be messed with. We need to put partisanship aside and speak with one voice, not as Democrats or Republicans but as Americans. I hope this hearing will be a positive step in that direction.

Thank you.

Mr. LYNCH. Thank you.

I will now yield myself five minutes for questions.

Chairwoman McCormick, given the critical role that the Election Assistance Commission plays in our democratic process, your agency has been given a renewed sense of purpose and urgency and attention. The Commission is finally back to having a quorum after lacking one between December 2010 and January 2015, which is a sad statement in itself; and then again since March 2018. The Commission was integral in distributing the $380 million in funding that the Help America Vote Act provided during the last few years. However, I do remain concerned that the EAC may not be able to fill its important role in a timely fashion as we approach the 2020 elections.

Last week, on May 15, you did speak before the Senate Committee on Rules and Administration and testified that in 2009, the last time the EAC had a quorum—and this is a quote—you said, "Our budget was double what it is now." You also testified that the EAC had 49 employees back then, and you have 22 right now.

So this is against the backdrop where I think the pressure on you and the work that needs to be done has risen exponentially, and you are trying to do this with less resources and less people, and I know some of your tech people left a short while ago and you are trying to in-board some technical help.

I am worried. I am worried. I talked to some of my state and county officials around the country, and they are nervous about making the necessary improvements, getting the necessary equipment and funding, training the necessary people on the new systems, and having all that happen in a fluid fashion before the elections in 2020.

So how are things going?

Ms. MCCORMICK. Obviously, we are a very small agency and quite underfunded, but I give a lot of kudos to our staff, who work 80 hours a week each on all of the projects that we are doing. We are stretched very thin, but we have met our mission, and we have met it well. We have hired some new security and technical people, and we are very excited to on-board them. The person that we

hired as our Director of Testing and Certification is one of the country's experts on post-election audits, and we have two more people starting who have between them 26 years combined experience in testing and certification of voting systems.

We have also hired last year a CIO who has expertise in cybersecurity, and so we are rebuilding that team. We are doing the best we can with the resources we have, but we have asked for more appropriations, and we hope we will get them.

Mr. LYNCH. I don't doubt that you are doing the best you can under the circumstances. But if 2016 and 2018 are indicators, and I think they are, you are going to face a ramped-up assault in the coming months before the election.

What do you need? What do you need specifically, as specifically as possible? I will hold my other questions until later. But what do you need? What can we do to help you?

Ms. MCCORMICK. People. We need people. We need more staff. Our staff is strained to the breaking point at this point, and we need depth. We have, in some cases, one person with no back-up holding down jobs that need back-up in case something happens. So we are asking for money so we can hire more staff to meet the demands.

The EAC's mission has expanded since it was created under HAVA. We didn't have the cybersecurity needs at the time. We always worried about election security, but, of course, since 2016, this is an additional mission for our agency, and we have stepped up in every way possible that we can, given the resources that we have. But we would like to step up even further.

Mr. LYNCH. All right. There is some common ground here between Democrats and Republicans. Can I ask you to work with your top people and give me a budget of what you need to get your job done? I know there are wider issues, but just narrowly look at 2020, what you need to get your job done, the number of people you need, to the degree possible a dollar figure that will get it done. Think about technology, the equipment you need, the whole shebang.

Ms. MCCORMICK. Yes, we can do that. We already have given that to Appropriations, so I can give that to you.

Mr. LYNCH. We have to strip it down just to that, what you actually need. I know there are a lot of other issues that are out there, but my focus is the 2020 elections because of the consequences. If we have a close election, God forbid, and people are skeptical of the process, I have seen that happen in other countries and it undermines the legitimacy of the government that gets put in place, and I don't want to be one of those countries in January 2021.

Ms. MCCORMICK. I agree with you completely.

Mr. LYNCH. Okay, I am going to yield to the Ranking Member, Mr. Hice, for five minutes.

Mr. HICE. Thank you very much, Mr. Chairman.

Mr. Krebs, you are aware of the situation in Florida, the voter registration breach in 2016?

Mr. KREBS. Yes, sir, I am aware of the incident in 2016 in Florida.

Mr. HICE. As much as you can, to the extent that you can, walk us through what happened.

Mr. KREBS. So I think the majority of this conversation would require the FBI to be a part of the conversation as well. The FBI was lead on briefing down in Florida, and I would defer to Mr. Hickey as well.

Ultimately, I think what we at my agency are focusing on is ensuring that any victim has the information they need to secure and address the issues with their systems so that we can understand what is happening within those systems and share the techniques that the adversary may be using across those systems.

Mr. HICE. Okay. I want to go there, but first let me go to Mr. Hickey.

Can you just real briefly, a 30,000-foot view, tell us what happened?

Mr. HICKEY. Thank you, sir. The most I think I can say in this forum without deferring to the FBI is that there were two counties that experienced intrusions into their systems, and we are confident based on what they have told us and our own work that there is no evidence that we have seen that that had any impact on the tabulation or counting or reporting of votes.

Mr. HICE. Okay. But the fact that the breach took place obviously is concerning to every one of us in here.

So going back, Mr. Krebs, to you, between the FBI and DHS, what steps are being taken to try to prevent this from happening again?

Mr. KREBS. So, as I mentioned, the run up to 2018, we made it a priority to work with every single state and as many of the local jurisdictions as possible. I have to say that Florida and Governor DeSantis just issued a press statement I think earlier today about his review of the state's election systems. But what we are finding is that Florida is probably one of our best partners of any state in the union right now.

Of their 67 counties or their 67 election supervisor jurisdictions, they are all working with us in one way, shape, or form. The Albert sensors I mentioned, those intrusion detection systems, 66 of 67 counties have them configured and deployed right now, and the 67th is in the process of doing so right now.

Mr. HICE. So with that, are you confident, relatively confident, that that vulnerability is going to be removed for 2020?

Mr. KREBS. Well, the specific vulnerability or the issue associated with the 2016 incident was addressed. What we are doing is taking——

Mr. HICE. Was it addressed to the point that the problem has been resolved?

Mr. KREBS. That is my understanding.

Mr. HICE. Okay.

Mr. KREBS. So what we have been doing is really focusing on what happened in this case. We have made a significant investment in outreach and engagement, best practices sharing. Spear phishing campaign assessments are one of our top priorities and just pushing awareness that with email come potential risks. It is really educating supervisors and election officials that there are things that they can do to truly minimize their risk surface.

Mr. HICE. Why has the FBI not released or disclosed the identity of the two counties?

Mr. KREBS. Again, I defer to the FBI on that, sir.

Mr. HICE. Mr. Hickey, any idea? I am just curious.

Mr. HICKEY. I think what they would say is they are following the process we follow any time you respond to the victim of a computer intrusion, which is that we are there to help them, and we leave it to them to make the decision about who they are accountable to and how to report that information. So whether it is a company or a county or a state, we are there to provide assistance, and then they need to make decisions about who they need to disclose that to.

Mr. HICE. I get that, but we have a right to know too. This is something that took place in 2016. We are talking three years ago. Evidently the issue has been addressed, the vulnerability is being closed. We have the right to know. I believe Congress has the right to know who was involved in that as far as counties, and the American people need to know. So I expect you to get back with us on this as best you can.

Ms. McCormick, let me go to you real quickly. Regarding the money, I brought this up a little bit in my opening statement, the $380 million that is available to help in the states, 80 percent of that is going to be spent. In what kind of concrete ways or how are the states going to use this?

Ms. MCCORMICK. About 58 percent of the money has been used for hardening cybersecurity, hardening the infrastructure. About 34 percent has been used to purchase new voting systems, where needed. And then about six percent, seven percent used for voter registration systems. So that adds up to a little over 90 percent of the money so far. We expect that the states will, straight-line projection, spend 85 percent of that money by 2020.

Mr. HICE. Okay.

And one five-second question, Mr. Hickey. What do you believe is our greatest threat to the election security? Is it hacking? What is the greatest threat?

Mr. HICKEY. It is how we respond to reports of hacking. Hacking, sir, I think is inevitable. It is how we react to it. Systems that are connected to the Internet, if they are targeted by a determined adversary with enough time and resources, they will be breached. So we need to be focusing on resilience, and resilience is not just a matter of what Mr. Krebs can tell you about the importance of auditing votes and the like. It is also how we as a people respond when there is a rumor or there is a report that there has been a breach. We need to take a breath, we need to let the states evaluate it, we need to let investigators respond, and we need to have confidence in our elected representatives and our state officials that they have this, because they deal with contingencies and elections all the time.

If we undermine ourselves, the confidence in our systems, we will be doing our adversary's work for them.

Mr. HICE. More than a 10-second question, but I appreciate your answer.

I yield back, Mr. Chairman.

Mr. LYNCH. The Chair now recognizes the gentleman from Tennessee, Mr. Cooper, for five minutes.

Mr. COOPER. Thank you, Mr. Chairman.

Director Krebs, apparently you warned us earlier this year that the 2020 election is, quote, "the big game" for foreign adversaries looking to undermine our democracy. I want to understand your analogy a little better. By "big game," did you mean an amusement or a plaything, or did you mean more like big game, like we are an animal to be hunted?

Mr. KREBS. Sir, I think for the adversary, and this is consistent with what Director Wray at the FBI has recently said, that is the target, that is the big target, the 2020 election.

Mr. COOPER. So we are like the lion that is being hunted.

Mr. KREBS. I have not thought about it in a game hunting sort of analogy, but this is the great competition.

Mr. COOPER. And unless it is a photo safari, the hunter seeks to not only hunt but kill the lion, right? That is the big game trophy that many hunters are pursuing.

Mr. KREBS. I am not a hunter myself, sir, but I think that is probably right.

Mr. COOPER. I am concerned because my state, Tennessee, has voting systems in most of our counties that have been judged some of the most vulnerable in the country. The Center for American Progress gave our state an F because so few of our voting machines have any sort of paper trail capability for voter verification or adequate audit procedures. So that means roughly about 15 percent of our counties apparently do have good machines; 85 percent do not. And yet our state has had on hand for nearly 18 years some $27.5 million unspent that could be used to acquire better voting machines. Davidson County, at least, has recently decided to buy better voting machines, which will be in place for the next election.

Ms. McCormick, what would you advise a state like Tennessee to do with that $27.5 million that has been sitting there for all these years just accumulating interest, even though that money has been held while we were under attack from foreign adversaries?

Ms. MCCORMICK. Well, we work with Secretary of state Hargett and with your elections coordinator, Mark Goins, and I trust that they are on top of that issue. We do suggest best practices, and one of those best practices is VDPAT on a voting system or a paper ballot. But we also have to keep in mind, of course, the voters with disabilities. I think that they are aware of this problem, and I suspect that they are working to fix the issue.

Mr. COOPER. So they are on top of the situation even though we got an F from the Center for American Progress?

Ms. MCCORMICK. Well, I can't speak for the Secretary or for Mr. Goins, but I think that they are doing a fine job in Tennessee. We do interact with them on a frequent basis.

Mr. COOPER. Were you aware that in 2018 hackers, apparently from the Ukraine, shut down a county election commission website during an election?

Ms. MCCORMICK. I was not aware of that.

Mr. COOPER. Well, being on top of the situation can mean various things, but presumably it would mean that websites would remain open during an election and not be shut down by a foreign potential adversary. Apparently no election data was manipulated, but a site that has been hacked successfully could be vulnerable.

Mr. Krebs knew exactly how many counties in Florida had Albert sensors. Can you tell me how many counties in Tennessee have an Albert sensor?

Mr. KREBS. Sir, I would have to come back with you and brief specifically on the counties. But I will say that the state has an Albert sensor, particularly Secretary Hargett's operation.

Mr. COOPER. But as you mentioned, elections really run at the county level, and you were very proud of the fact that 66 out of 67 Florida counties had Albert sensors, and you commended Florida for doing such an excellent job. Can you commend Tennessee in a similar fashion?

Mr. KREBS. Tennessee is a great partner. Every state runs their elections a little bit differently. Some are top down, some are bottom up, some are hybrid. Every state is going to run things a little bit differently and have different requirements. But Tennessee is a strong partner.

Mr. COOPER. Well, I know we are great and strong, but we also want to be unhackable.

Mr. KREBS. Sir, I think that is certainly a noble destination, but unhackable is not a realistic objective. What we are looking for is——

Mr. COOPER. Well, less vulnerable to hacking——

Mr. KREBS. Absolutely.

Mr. COOPER [continuing]. at least at the Florida level, which was two or three years late in discovering that they had been hacked.

Mr. KREBS. Sir, again, on 2016 issues, everyone that we had an understanding there was an issue was notified of the issue, and the issue was addressed.

Mr. COOPER. But as Mr. Hice pointed out, we still don't know which Florida counties were vulnerable. So apparently the American people are not allowed to know.

I see that my time has expired.

Mr. LYNCH. The gentleman yields back.

The Chair recognizes the gentleman, the doctor from Tennessee, Dr. Green.

Mr. GREEN. Thank you, Mr. Chairman and Ranking Member Hice. Thank you for today's hearing, and also let me thank our witnesses for being here today.

I am equally concerned about this topic, but really almost for other reasons. First, the discussion of the threat. Clearly there are several threats to the security of our election process. One, of course, is the cyber threat, domestic and foreign hacking that might alter vote counts. Another, of course, is local, focused on the polls themselves where intentional or unintentional mistakes can result in the wrong results, or worse, actual voter intimidation as seen in the 2017 special election in Philadelphia, where an election official pled guilty to voter intimidation against anyone voting for a non-Democrat. Philadelphia has seen many of those cases.

Other such examples of manipulation should also be considered, such as ballot harvesting. In Tennessee, we don't even allow candidates and their campaigns within a certain distance of the polling places so that individuals can be free of the pressure right as they cast their ballot.

But in California, the candidates can just go to the person's home with their ballot, pressure them, get their vote, and turn it in for them. As the former Speaker of the House said, that defies logic.

I would submit to you that our founders got it right on how best to do government, and that is the best government is the government that is closest to the people, and I think that is also the case in elections.

Let me just share a little bit about what my state is doing. While I deeply respect the gentleman, Mr. Cooper from Davidson County, I have to disagree with him. I think Tennessee and Secretary Hargett, and particularly the elections commissioner, Mark Goins, are doing a fantastic job.

As I mentioned above, we don't allow candidates in Tennessee to get anywhere near our polling sites. Further, all the poll workers are divided amongst the parties, effectively yielding an equal number of workers from each party at each polling station. So local intimidation, like they are seeing in Pennsylvania, is not happening in Tennessee.

As for cyber threats, our Secretary of State, Tre Hargett, and the head of our elections, Mark Goins, have done a spectacular job protecting the integrity of our elections. The state offers regular online cybersecurity hygiene training for election officials, including part-time election commissioners, and even volunteers. The state provides onsite security scans for our county election offices. Tennessee has conducted statewide cyber-related election tabletop exercises, war-gaming attacks and how to handle them.

Tennessee provides annual in-person cybersecurity hygiene training led by experts such as Paul Connolly, the Chief Information Officer from HCA, Healthcare Corporation of America. Our state election commission provides each county with hardware systems dedicated to interact with our statewide voter registration data base. Our personnel are trained on recommended best practices and guidelines for protecting election infrastructure. As we speak, the state is in the process of hiring more technical employees who assist counties with cyber-related issues.

Tennessee doesn't need, nor do we desire, the Federal Government's intrusion into our elections. It is clear the agenda of the leadership of the majority party is to do just that. They even, with H.R. 1, want to force California's election systems onto the states, basically making a Federal methodology and taking control from the states. It is their biggest initiative. It is H.R. 1, usually the designation reserved for the party's biggest push.

California-style elections on the rest of us, not an option. The goal is clearly to empower a certain group of people, a certain party. It is unacceptable.

Thank you, Mr. Chairman, for allowing me to share these thoughts and the thoughts of the people of Tennessee.

Mr. LYNCH. The gentleman yields back.

The Chair now recognizes the gentleman from California, Mr. Rouda, for five minutes.

Mr. ROUDA. Thank you, Mr. Chair.

To my esteemed colleague from Tennessee, I would like to point out that California does not harvest ballots, contrary to that false narrative being perpetuated. And I would also like to point out that

you conveniently forgot about the actual ballot harvesting that was taking place in North Carolina's 9th District, where we are having a special election to overturn the Republican operatives who unduly influenced the outcome of that election.

But I digress. We are here to talk about voting system vulnerabilities, and I appreciate the witnesses coming here today to help us better understand the challenges facing our country and our voters and our democratic foundations.

Chair McCormick, I would like to talk to you a little bit about the EAC guidelines. I know you are in the process right now of going through and updating those guidelines. When were those guidelines originally promulgated?

Ms. MCCORMICK. The systems that are now certified were certified under standards that were set in 2005.

Mr. ROUDA. And there has been no upgrade to those guidelines since then?

Ms. MCCORMICK. We actually upgraded those guidelines in 2015, which we call the VVSG 1.1. But we have seen no manufacturer bring a system into those updated requirements.

Mr. ROUDA. Yet the I-phone that has been out since the first rendition in 2007, I think we have had about 10 different renditions since. So when you look at those guidelines, what is your level of confidence in the guidelines providing the appropriate guidance to make sure that our election systems are safe and secure?

Ms. MCCORMICK. It is a complicated procedure because we still need to be sure that the manufacturers can design systems that will meet those requirements, and that the jurisdictions will have the funding to be able to buy those systems if they come onto the market. So we need to make sure that the systems are secure and accessible and reliable and usable, but also that they are designed in such a way to take advantage of the innovations that are in the market, but not so expensive that they are unreachable by most jurisdictions. Funding is always an issue when it comes to elections.

Mr. ROUDA. And do you have 100 percent confidence that these machines will secure our elections and there will be no fraud?

Ms. MCCORMICK. I don't believe there will be fraud on the voting systems. You know, we can't 100 percent guarantee that there can be no intrusions into the systems, but we are doing our absolute highest and best to test and certify machines that will be secure and will not be subject to fraud or manipulation of the votes cast on them.

Mr. ROUDA. Well, I am aware of the situation that took place in Las Vegas, where we invited in a bunch of hackers to try and get into voting machines who had a higher level of success than anybody in the industry was anticipating, and that should raise concerns for all of us.

Mr. Krebs, I would like to turn to you a little bit on this as well, because I think you had stated earlier in your testimony that you do not have 100 percent confidence that hacking could not take place in our electronic voting machines. Can you verify that I got that correctly?

Mr. KREBS. Yes, sir. One hundred percent security is not the objective. It is resilience of the system. So even if you do have a bad day, it is not a catastrophic day, that there is resilience built into

the system, that you can understand what happened across the process and point back to good.

Mr. ROUDA. As a guy who won a primary in Orange County, California by 125 votes, I am always a little bit more concerned about how sure we have to be in getting that vote correct. If you look at the information that has been provided by—let me make sure I get the institution correct—the Brennan Center for Justice, that 12 states still use paperless electronic voting machines that are at extreme risk, and there has been discussion that we need to have paper ballots to act as a back-up audit, or at least some sort of system within these electronic machines to have a back-up audit, what is your confidence level in that?

Mr. KREBS. So, we approach this problem set as IT security advisers. So we bring a cybersecurity and an IT security mindset to the issue. Auditability is a key tenet of cybersecurity, of IT security. If you don't know what is going on across the process, it is hard to guarantee an outcome and verify the process.

So one of our top priorities working with the EAC is encouraging and incentivizing auditability. It is getting these systems, these systems that don't have paper out and systems with paper in, and then implementing an audit process not just on the back end but throughout the process.

Mr. ROUDA. And one other quick question. If we are not completely successful in that outcome, are we looking to going back to analog, pen and paper?

Mr. KREBS. Pen and paper is already an option within the system. Every jurisdiction, in their sovereign responsibility of conducting elections in Article 1, Section 4, they can pick that if they would like, but there are other factors to put into the equation.

Mr. ROUDA. Thank you.

Mr. Chair, I yield back.

Mr. LYNCH. The gentleman yields.

The Chair now recognizes the gentle lady from North Carolina, Ms. Foxx, for five minutes.

Ms. FOXX. Thank you, Mr. Chairman.

I want to thank our witnesses for being here today.

Chairwoman McCormick, in your opinion, are state and local governments equipped to combat election interference?

Ms. MCCORMICK. state and local election officials are doing all they can right now, but they do need the assistance of the Federal partners. I don't think it is fair to put all of the onus on them when there are nation-states that are attempting to interfere with our elections, and I know that with our Federal partners we are trying to provide all the help we can and assistance with resources and information and actual physical support to the states and localities so that they can secure their systems.

Ms. FOXX. Thank you. I would like to followup. Congress established the EAC to develop guidance to meet the Help America Vote Act, HAVA, adopt voluntary voting system guidelines and serve as a national clearinghouse of information on election administration. In the last Congress, the Senate confirmed two new EAC commissioners, giving the EAC four commissioners for the first time in about 10 years, and a quorum after nine months without one.

Considering this, what are the top three priorities for your commission to accomplish in the next six months?

Ms. MCCORMICK. I would say to continue providing resources that we can to the states for election security, providing information on voter registration data bases and how to secure them, and also provide any information we can on best practices to the states and localities with regard to all of the other issues in election administration, of which there are many.

Ms. FOXX. So the EAC provides voluntary best practices to state and local governments to improve their systems. Could you highlight the top three practices states and counties find most helpful?

Ms. MCCORMICK. That would be very difficult for me to do because it is such a complicated and varied system throughout the country. We have a patchwork, so different states and localities rely on us for different needs. I can get back to you on that, if you would like.

Ms. FOXX. Sure. Well, then, aside from additional funding, which is what everybody always says they need, do you have any examples of two or three—do you have two or three examples from state and local officials that are the most concerning to them?

Ms. MCCORMICK. I think security is one of their top issues. I think there is also a concern with natural disasters. We have had a number of issues surrounding a number of events around elections that have caused a great deal of concern. And I also think that they are concerned about voter confidence, that our voters can be assured that their votes are going to count and count correctly.

Ms. FOXX. Thank you.

Mr. Chairman, I would just like to say, as a person who ran for the school board in 1974 and lost by about 200 votes, and then I ran again in 1976 and at the time we had an election for the Registrar of Deeds in our county, and we had in 1976 an 85 percent turnout that year, and there were a couple of precincts out in the far western part of our county that ran out of ballots; and, like Mr. Green, we have in North Carolina equal numbers of people from both parties there, and the two parties agreed they would make some ballots so that the people who came to vote wouldn't have any problem voting. So they made some ballots, and the gentleman, who was a good friend of mine, I liked him very much, who was running—a Democrat gentleman running against a Republican woman for Registrar of Deeds, the first time the seat had opened in over 50 years, and the Democrats had owned it for 55 years. Anyway, he lost by 13 votes.

But all the election officials agreed it was all very clear and we would have a hearing by the election board. So they ordered a new election for him at the time because he lost by 13 votes. There was a new election for him only. All the rest of the elections were certified. He lost by 1,300 votes.

I think, for the most part, our election officials locally, for the most part, are very honest people, do the best that they possibly can for the people, and I was frankly very proud of the people in my county for getting together that day, Democrats and Republicans, to make sure that everybody who showed up at the polls had a chance to vote even though they had run out of ballots.

Thank you very much.

Mr. LYNCH. I thank the gentle lady for sharing that with us.

I do want to note that I worry that state governments, because this is a foreign threat, may not be adequately equipped. So we don't encourage—we don't think of this as Federal interference with states conducting—it is Federal assistance and helping them, giving them grants so that they can run the election the way you have described, the way they see best. But I thank the gentle lady.

The Chair recognizes the gentleman from Vermont, Mr. Welch, for five minutes.

Mr. WELCH. Thank you. I thank the witnesses.

I have a question that I want to direct both to Mr. Krebs and Mr. Hickey, and it is about the public statement that you issued jointly in February 2019 concluding that there was "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 of political/campaign infrastructure used in the 2018 midterm election."

Before issuing this joint statement, how many voting machines used in November 2018 did DHS and DOJ forensically examine for evidence of hacking? And if the answer is none, don't you think such an unqualified statement is a bit of an overstatement?

Mr. HICKEY. Sir, as the statement lays out, we based what we called the 1B report or that conclusion, which is the bottom-line conclusion of the 1B report, on the report we were given from the ODNI, which looked at what efforts were made by foreign actors to interfere in a variety of ways, and then we looked at those instances and looked to see whether there was evidence of a material impact on infrastructure. So we didn't set out to audit or to prove a negative. We looked at the evidence that there was. There was evidence of efforts to interfere, and we looked at and measured that effort and determined it was not materially successful when it comes to altering election infrastructure, campaign infrastructure.

Mr. WELCH. Mr. Krebs?

Mr. KREBS. I concur with that. I would say we looked for three sort of feeding elements of that assessment. One is, as Mr. Hickey mentioned, from the intelligence community. The second is from actually partnerships with state and local officials, if they detected or noticed any anomalous activity. Whether it was them or their vendors noticed anything, we would certainly go and investigate that as a threshold matter. And then third is our own ability to understand what is going on in the ecosystem through our Albert sensors. If we had detected anything, again threshold, then we would go do additional engagement.

Mr. WELCH. So your view is that even taking a random sample to do forensic analysis of the machines themselves was not important to provide a foundational basis for that very explicit opinion?

Mr. KREBS. Auditing, as I think Mr. Hickey laid out, auditing is not within the scope of the engagements that tied into that assessment. We certainly offer auditing, forensic auditing capabilities, to any jurisdiction that would request it. Certainly, if they had noticed anything anomalous, we would come in and offer that service.

Mr. WELCH. You issued that report to the White House. My understanding is that it is classified; is that correct?

Mr. KREBS. Ultimately the report, under the executive order, does go to the National Security Council. Yes, sir.

Mr. WELCH. And I know you didn't make the decision about that classification, but I would object to that. Can you think of any policy reason why what you found and what you reported shouldn't be made known to all of the American people so that they can judge for themselves, Mr. Hickey?

Mr. HICKEY. Yes, sir, I think I can. As I mentioned, our report piggybacks on a report by the intelligence community which was a report on efforts they saw to interfere; attempts, if you will. Presumably those attempts and our awareness of them are derived from sources and methods that are sensitive, and if we were to reveal what we knew about what foreign actors had tried, we would necessarily be revealing what we don't know that foreign actors have tried.

Mr. WELCH. Well, that is not always the case, because reports can be issued with scrubbing out the sources and methods, because the point you make about sources and methods is a valid point. Let's assume that your concern about sources and methods could be addressed. Why not release the rest of the information for the benefit of the public?

Mr. HICKEY. Sir, as you mentioned, I was not the classification authority. My intuition is that would be impossible because the report doesn't actually contain the source and method or methods itself. Most of the intelligence I read doesn't tell me how the intelligence was collected. But from reading it, an adversary would be able to discern, aha, they have visibility here, or they have a human source there, and what they don't know is this, that, and the other thing. So they would be able to identify the most effective ways to target us in the future, right? Because if it is not in the report, they would probably draw the inference, oh, the Americans didn't see that, so that is a good technique for the future.

Mr. WELCH. I thank the witnesses.

My time has expired, and I yield back.

Mr. LYNCH. I thank the gentleman for yielding.

The Chair now recognizes the gentle lady from Illinois, Ms. Kelly, for five minutes.

Ms. KELLY. Thank you, Mr. Chair.

In February 2019, the Department of Homeland Security's Inspector General released an audit on the efforts of DHS to secure our election infrastructure. While the IG report credited the Department for taking some steps to lessen the risk to U.S. election systems, the IG also found some troubling gaps.

For example, according to the report, and I quote, "DHS has not completed the plans and strategies critical to identifying emerging threats and mitigation activities and establishing metrics to measure progress in securing the election infrastructure." The Department had also not incorporated election infrastructure into several of its key security plans, including the DHS Cybersecurity Strategy and the National Infrastructure Protection Plan. The IG noted that senior leadership and staff turnover had, and I quote, "hindered DHS' ability to accomplish such planning."

Director Krebs, has DHS developed an election security strategy, and has the President been informed?

Mr. KREBS. Ma'am, I think that Inspector General report, if you look at the end of it and the recommendations they make, they actually agreed that we had made the progress and were just awaiting documentation.

The sector-specific plan, Chairwoman McCormick talked about the Government Coordinating Council and the Sector Coordinating Council, those two bodies, which bring together the stakeholders across government at all levels of government and the private sector, are part of the election infrastructure ecosystem. So they are part of our joint effort to develop the plan. That planning process—again, that sector-specific plan that nests underneath the National Infrastructure Protection Plan that you referenced—that is under development right now. It is built on lessons learned from the 2018 process. It is a consensus-based, collaborative document, and I look forward to getting that wrapped up and will certainly push it up to the National Security Council and Master Bolton, and I would hope the President would take a look at it. Yes, ma'am.

Ms. KELLY. So is DHS working to incorporate election infrastructure security into the other existing strategic plans?

Mr. KREBS. The DHS cyber strategy that you referenced is actually agnostic to any specific sector or any specific issue set. It empowers subsequent tailoring of further plans against, for instance, election infrastructure and that sector-specific plan. It recognizes the role of the National Infrastructure Protection Plan. It, too, is an umbrella document. It says there are 16 sectors with sub-sectors, and each of those sectors and sub-sectors has individual tailored plans with metrics, with plans of action, and mechanisms and methodologies for engaging the entire stakeholder set.

Ms. KELLY. Okay. And, Director Krebs, the President's Fiscal Year 2020 budget proposal would cut funding for the Cybersecurity Infrastructure Security Agency from its 2018 and 2019 Fiscal Year levels. This is especially troubling since 2020 is a Presidential election year, and we know Russia and other malign actors are likely to target our infrastructure and political discourse, as they did in 2016.

Did you or others in CISA ask for more funding from the President before he released his budget proposal?

Mr. KREBS. So, we certainly contributed to the development of that budget. It, as I see it for CISA, is a maintenance budget that sustains operations as they exist now. With more, of course, we could do more, just as Chairwoman McCormick mentioned. I will note that that is the first budget released under my authority as the Director of CISA. It reflects my priorities. It reflects the fact that it is the first time in a budget we have actually requested election-specific funding. Prior, the $59.4, $8 million over 2018 and 2019, were graciously provided by Congress, and we thank you for that. This 2020 budget actually says we want to continue this. We need to continue growing our capacity to help EAC, to help state and local election officials boost their cybersecurity.

Ms. KELLY. Because I know people, you want to take—we want to give you the world; you are probably going to take it. But are you satisfied? Is it enough to do what you need to do?

Mr. KREBS. You know, with more, I can do more. As I mentioned, $59.4 is the most I am aware of for any specific sector or sub-sector

within the Department of Homeland Security's budget history. Just recently we released what is known as the National Critical Functions Set, which breaks out the 16 sectors into 55 different functions that underpin the economy, public health and safety, national security. I think with a cost buildup approach across those 55 sectors, there are a lot of things we could do positively to improve the cybersecurity and physical security, frankly, of this Nation.

Ms. KELLY. And with the money that you are getting, is there anything you would have to cut or cut out or lessen?

Mr. KREBS. No, ma'am. I think in the 2020 budget, I think what you are seeing is the rationalization of some Tier 1 acquisition programs, the life-cycle cost adjustments, and also finding some efficiencies in other contracting programs. What I am aiming to do is to push more resources out into the field so, in part, I can minimize travel out of D.C. and have more locally based assets. I can have the best tools, techniques, and capabilities in the world, but if they are sitting in D.C. and I don't have people out in the field to help carry them out through the Secretaries of State, election directors, chief security officers, whatever they are, then I am not optimized.

Ms. KELLY. Okay, thank you.

CISA and DHS have key roles to play in securing our elections. Your Department needs to be ready, as you know, to face down these threats and to help the states secure their infrastructure. We will make sure you have the resources you need to do so. It is important to all of us.

Mr. KREBS. Thank you, ma'am.

Mr. LYNCH. The gentle lady yields back?

Ms. KELLY. Oh, sorry. Yes, I yield back.

Mr. LYNCH. That is Okay.

The Chairman recognizes the gentleman from Maryland, Mr. Sarbanes, for five minutes.

Mr. SARBANES. Thank you, Mr. Chairman. Thank you for the opportunity to participate today.

So, we all know what happened in the 2016 election. We know what happened in the midterms in terms of attacks. We did a pretty good job, from what I am hearing, of rebuffing those attacks. But now we are looking down the barrel of the 2020 elections. Our intelligence community is obviously warning us that we are going to be attacked again. In fact, FBI Director Wray made the claim that he believes Russia treated the 2018 election as "a dress rehearsal for the big show in 2020." So the red lights are blinking, the alarm bells are going off. We are under attack. It is clear to everybody.

Unfortunately, the attempts to elevate attention to this and prepare for it in advance of 2020 have been met with hostility by officials at the highest level of our government. In fact, Mick Mulvaney was reported to have said that election security "wasn't a great subject and should be kept below his"—meaning the President's—"level." And just last week the Senate Rules Chairman, Roy Blunt, admitted that Senate Majority Leader McConnell won't allow a vote on election security legislation "no matter the policy and no matter the approach."

When we passed the For the People Act in the House, House Democrats essentially introduced a comprehensive set of election security reforms that would protect the ballot box, that would sty-

mie disinformation campaigns, close loopholes that allow foreign governments to intrude into our democracy. Title 3 of H.R. 1 was just reintroduced by the Democrats as a stand-alone bill that would address all of these important issues and provide states and local governments with the resources that you have described are necessary to make sure we are ready for 2020.

So there are solutions that we have. We encourage and ask our friends across the aisle to join us in this effort. This is about American patriots, not Republicans or Democrats, fighting back against these attacks on our democracy. So I thank you all for being here.

I have a couple of questions, Commissioner Weintraub, for you. Before I ask them, I did just want to say for the record I have some significant concerns about the interpretive rule that you announced earlier regarding the building fund account, both as a matter of rulemaking authority within the FEC, but also as a matter of policy. I definitely agree that we have to do more to provide resources to our political parties to bolster their cyber defenses, but I don't agree that the approach of relying on big donors to do so, that that is the solution, and I am going to offer some legislation that might pose an alternative way forward and look forward to having a discussion with you about that.

You said that we should not trust the next panel if they tell us they got this. I hear you on that. I am a little worried that, if the building fund is opened to big-donor contributions, they might say with respect to that "I got this," if you get my drift. So that is the concern I have.

Let me ask you a couple of questions.

Ms. WEINTRAUB. Could I comment on that, please?

Mr. SARBANES. Well, let me get my questions in, and then if you want to come back.

The Special Counsel chose not to prosecute campaign officials for coordinating with the Russian government, and he said his office's understanding of Federal law concerning coordination was that you need an agreement, tacit or express. But there is a definition of "coordination" in campaign finance existing law, and McCain-Feingold expressly provided that the FEC "shall not require agreement or formal collaboration to establish coordination." Is that your understanding of existing campaign finance coordination law?

Ms. WEINTRAUB. It is.

Mr. SARBANES. Thank you very much.

Much has been made of the Special Counsel's inability to value the opposition research that was solicited by campaign officials, thereby informing the Special Counsel's decision to not prosecute officials for an illegal solicitation of a foreign government. In other words, they are saying we have no way to figure out what the value of that is. But cash contributions from foreign nationals are strictly prohibited under existing campaign finance law. It could be one penny; it is expressly and strictly prohibited.

So for purposes of the foreign national prohibition, does the monetary value of an in-kind contribution matter, or should Congress clarify that all in-kind contributions, much like cash contributions, be prohibited? Do you think that would be a good measure for us to undertake?

Ms. WEINTRAUB. I believe that the current law is broad enough to encompass in-kind contributions. However, I think that clarification would be helpful, because my view of the law is not always shared by my colleagues.

Mr. SARBANES. Right. Well, hopefully we can undertake that and make that clarification, and that will be another way of protecting our elections going forward.

I have run out of time. I am sorry, but we can continue the conversation offline.

I yield back.

Ms. WEINTRAUB. Fair enough.

Mr. LYNCH. The gentleman yields, and I thank you.

Ms. Weintraub, I would like to come back to that question. I see the light bulb over your head and it seemed like you had something you were eager to contribute, so I do want to give you that opportunity. So just hold that thought.

Ms. WEINTRAUB. Okay.

Mr. LYNCH. The Chair now recognizes the gentleman from Maryland, Mr. Cummings, for five minutes.

Mr. CUMMINGS. Thank you very much.

Mr. LYNCH. The Chairman of the full committee.

Mr. CUMMINGS. Thank you.

Director Krebs, your Department is at the tip of the spear when it comes to protecting our elections. One of my worries, however, is that DHS and the Cybersecurity and Infrastructure Security Agency do not have enough employees specifically focused on securing our election infrastructure. According to the DHS Inspector General report released in February 2019, while DHS had one or two advisers to cover its 16 critical infrastructure areas, the Department, and I quote, "does not have dedicated staff focused on election infrastructure." The Inspector General's Office interviewed stakeholders who, and I quote, "expressed concerns about adequate DHS staffing, which they reported hindered their ability to develop relationships" with the Department.

How would you respond to that concern? Because it is a very serious one.

Mr. KREBS. I think at a point in time it was absolutely true. In 2016, I think the only people really in the Federal Government that understood elections was Chairman McCormick and her team and Chairman Weintraub. We came into this thing brand new. Again, we are cybersecurity and physical security experts. We still are. They are the election experts. We are the security experts that come in and support.

So when you talk about the pointy tip of the spear, it is a big, big spear. There are a lot of us on this team. So we support state and local officials. We support the EAC. We support the DOJ and FBI. This is a team effort.

At this point we have invested, with Congress' appropriations, to support our election infrastructure team. I have 17 full-time personnel dedicated to this issue, but I also have the capability to reach into my entire organization and draw any resource needed.

In the run-up to the 2018 midterm elections, in the month prior to the election, I had over 550 individuals that were working at the national, local, state level on elections. That is pretty good. I can

do better, I can do better. We can continue to work with the EAC. We can continue to work with state and locals. We can continue to invest in our people, and our capabilities get more scalable, and that is my plan for 2020. We will have more full-time dedicated staff. I will have more field staff to engage and ensure that 2020 is the most secure election ever.

Mr. CUMMINGS. So how many people will be permanent? Are these basically temporary employees you are talking about coming in, talking sort of seasonal?

Mr. KREBS. So DHS, keeping in mind DHS was established as a bit of a surge organization, right? Whether it is a hurricane or some other national emergency, we are able to surge capabilities. So for 2018, we surged. We established task forces. We cobbled together as many people as we could that had relevant expertise. Over that time, we also institutionalized as a program. So we have established since an election infrastructure security program, an initiative, that is dedicated permanent staff. My hope is by 2020 we will be well over two dozen, pushing 30 personnel, dedicated full-time, but able to draw on my field staff.

My field staff in the last two years, the demand signal for election infrastructure support services has surged to the point where it is basically a half-time job for my field team. On the other half, they are doing school safety, houses of worship, active shooter soft-target type work.

Mr. CUMMINGS. Have you or your deputies asked CISA employees to deploy to the U.S.-Mexico border?

Mr. KREBS. Yes, sir. As a matter of fact, the entire Department asked that the components, whether it is TSA, FEMA, anyone else, consider volunteering, or their personnel consider volunteering to go down and help some of the logistic support down at the border.

Mr. CUMMINGS. So how many of your employees at CISA have been sent to the border, and how many more are expected to be sent?

Mr. KREBS. Across the agency, 10 have deployed, and I think we have another 10 that are in an availability period where they may deploy down, keeping in mind that across the agency I have about 2,200 personnel. About 900 of them are cybersecurity focused. Another 800 are physical security focused. I have some communications specialists that are actual emergency communications specialists, and I have mission support personnel.

There will be risk-based decisions on people that deploy to the border. If it is an election issue, if it is a critical cyber operation, we will have conversations with supervisors and understand whether that is something we need to reconsider.

Mr. CUMMINGS. It sounds like they will be doing a number of different jobs. Is that it? What will their responsibilities be down there by the border?

Mr. KREBS. I would have to get back to you on the specifics. Acting Secretary McAleenan testified this morning in front of House Homeland and talked about this, but it is logistical jobs. In some cases it is attorneys, it is driving. The Federal Protective Service deployed some CDL drivers down. So there are a number of logistics and support functions.

Mr. CUMMINGS. If the Chairman would, just one last question.

Are CISA employees appropriately trained and qualified to provide security and support, the intake of migrants at our southern border?

Mr. KREBS. Sir, again, I suggest that we work with the Department legal team and the H.R. folks to figure out and explain what the actual functions are. My understanding, though, is that any person that goes to the border, whether it is from TSA, FEMA, CISA, anywhere, is going to have the appropriate training to do the function asked on the border.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

Mr. LYNCH. The gentleman yields back.

The gentleman yields momentarily to Mr. Hice, the Ranking Member.

Mr. HICE. Thank you, Mr. Chairman.

Just a clarifying question, Mr. Krebs. Are you saying that more resources are needed at the border? Because you are sending people down there.

Mr. KREBS. Yes, sir. I think that is consistent with the prior Secretary and the current Secretary's request.

Mr. HICE. Thank you for that clarification.

Mr. LYNCH. The Chair recognizes the gentle lady from Florida, Ms. Wasserman Schultz, for five minutes.

Ms. WASSERMAN SCHULTZ. Thank you, Mr. Chairman.

In 2018, the White House eliminated the cybersecurity coordinator position on the National Security Council.

Mr. Hickey, the National Security Council is responsible for facilitating the implementation of Administration policy and coordinating national security-related activities across the interagency. Is that correct?

Mr. HICKEY. That is my understanding, ma'am.

Ms. WASSERMAN SCHULTZ. So would it be fair to describe the National Security Council as a rudder that steers the U.S. interagency?

Mr. HICKEY. I don't know if they would like that analogy, but they certainly play a critical coordinating role. They have convening authority, and we meet with them frequently for that reason.

Ms. WASSERMAN SCHULTZ. Given the attitude of this Administration, I agree, they probably wouldn't like that description, but practically applied that is what they do; correct?

Mr. HICKEY. They play a critical coordinating function across the interagency, yes.

Ms. WASSERMAN SCHULTZ. Thank you.

Director Krebs, how has the absence of a cybersecurity coordinator at the National Security Council affected the Department's ability to coordinate its election security activity strategically and effectively across the interagency?

Mr. KREBS. There is a PCC process established under NSPM–4 with specific election security coordination. So we do work closely with the NSC, but it is also important to consider the fact that under the operational authorities that I have, that the DOJ, the FBI, the DIC, that DOD has, we are coordinating on a daily basis on operations, and then those inform the actual field activities. So

I would not mistake the lack of a coordinator for lack of coordination. It happens because it is our job.

Ms. WASSERMAN SCHULTZ. Mr. Krebs, the last time we spoke was on May 1st, when you testified before the Appropriations Subcommittee on Homeland Security, and at that hearing you raised serious concerns about Russian operatives attempting to influence our 2020 elections. I asked you then if the President had received a briefing from you or anyone in your Department on potential Russian interference in our elections in 2020, and you said he had not received a briefing.

Administration officials have offered plenty of sound bites suggesting the President is taking this issue seriously, so today I would like to ask you again. It is May 22, three weeks later. Has the President received a briefing from you or anyone in your Department about threats of foreign influence in the 2020 election?

Mr. KREBS. Ma'am, I am going to take your word for it that I said it that way.

Ms. WASSERMAN SCHULTZ. You did.

Mr. KREBS. Okay. I am not privy to the President's daily brief. He sees a range of intelligence——

Ms. WASSERMAN SCHULTZ. I am asking if he has had a briefing by you or anyone in your Department about threats—I mean, you are responsible for election security—about threats——

Mr. KREBS. The DNI, ma'am, is responsible for working with the President on intelligence matters. I am responsible for helping state and locals protect their systems.

Ms. WASSERMAN SCHULTZ. When I asked you at that meeting, you said to your knowledge, you said the President did not have a briefing on the threats potentially facing us in the 2020 election. Is that still true, to your knowledge?

Mr. KREBS. Certainly for me. Yes, ma'am, certainly for me.

Ms. WASSERMAN SCHULTZ. Okay. Director Krebs, during a House Homeland Security Subcommittee hearing on April 30th, you described President Trump as, quote, "the head coach for the Administration's cybersecurity strategy." I played team sports, so my question is if your head coach doubts the threat of foreign interference, how does your team prepare your defense, our defense, against our adversaries?

Mr. KREBS. Ma'am, as I discussed in that hearing, as I have discussed with you in the Appropriations hearing, the President supports the conclusions of the intelligence community assessment of January 2017. He said that on the record several times. So I have the guidance, I have the steerage I need from the coach. We are executing. We are working closely with the Department of Justice. We are working closely with the FBI. We work closely with the intelligence community and the Department of Defense. I have the guidance, I have the direction, I have the strategy I need to be effective to support Chairwoman McCormick and her constituents in the state and local election community.

Ms. WASSERMAN SCHULTZ. Okay. Well, President Trump has repeatedly publicly expressed doubt about Russian foreign interference in our elections. So how can we expect you and your colleagues here to tackle these threats if you don't have full buy-in from the White House, all the way to the top?

Mr. KREBS. Ma'am, again, he supports the intelligence community assessment in 2017. I take him at his word. I have what I need to go——

Ms. WASSERMAN SCHULTZ. Reclaiming my time, I take him at his word, because his words and deeds have demonstrated that he doesn't think that there was Russian interference. He has said that out loud. And his actions, particularly as it relates to not taking it seriously enough to even bother to have an election security briefing in advance of the 2020 elections, is mind-blowing.

Mr. KREBS. Ma'am, again, I am not privy to every briefing, every meeting he gets.

Ms. WASSERMAN SCHULTZ. I know, but I am just going by your answer to my question when I asked you, and I want to thank my colleagues who raised rightful concerns today about the lack of transparency regarding the hacking of two counties in particular in Florida.

We received a briefing from the FBI, along with the rest of our Florida delegation members, and while I can't share the two counties that were hacked, I believe that investigators should not be withholding that information from the real victims here, the voters in those counties. The lack of transparency from top to bottom in this Administration is stunning, and it diminishes voters' confidence in our election system, makes voting less likely, which unfortunately I think demonstrably has been shown is this Administration's true interest.

Thank you. I yield back.

Mr. LYNCH. The gentle lady yields back.

In concluding the business of this panel, Ms. Weintraub, I want to just address a question to you, and I know you had touched on this earlier in your opening remarks.

During the 2016 election, the Russian-based Internet Research Agency conducted its disinformation campaign not only by posting through fake accounts but also by purchasing ads on various social media platforms. I believe in some cases they paid in rubles, which should have been a tip.

Commissioner Weintraub, later today we will hear from Twitter, Facebook, and Google, your friends over there. I know you were throwing a little bit of shade on them earlier about their efforts to increase political ad disclosures on their sites. But given your role, your specific role with the Federal Election Commission, I would like to hear your insights on this issue.

Ms. WEINTRAUB. Well, first of all, let me say that I do think that the platforms are trying. They have taken steps and they are able to move quickly in a way that I sometimes can't. I have been trying to adopt new regulations on this, and it has just been bogged down at the FEC in terms of not getting an agreement from my colleagues on exactly what they are willing to agree to. So that is a point of frustration for me.

But I think that the point that I am trying to make about the platforms is that I really don't think this is something we should leave entirely in the hands of the private sector, because what they decide to do today they could take back tomorrow and decide to do something less. So I think the government has a role here to set

standards and to make sure that the platforms are complying with them, because it is an awful lot of power that they have.

Mr. LYNCH. Okay. Thank you very much.

I think this panel has suffered enough, and I want to thank you for your attendance. If there are any further questions by the members, obviously they can submit them in writing and we will forward them to you, if you would be so kind as to answer them in due course as rapidly as possible.

So this panel is recessed, and we would ask the next panel to come forward, and we will continue with the hearing. Thank you.

[Pause.]

Mr. LYNCH. We now welcome our final witnesses on the second panel and thank them for their testimony and their patience.

First of all, I would like to introduce the Honorable Bill Galvin, Secretary of the Commonwealth of Massachusetts, a dear friend and someone who I personally consider to be one of the foremost experts on our election systems, and I think he has done a remarkable job on behalf of our state where we have both a very secure digital system as well as a paper back-up system, which I think is commendable.

Richard Salgado, the Director of Law Enforcement and Information Security with Google.

Nathaniel Gleicher, Head of Cybersecurity Policy with Facebook.

And Kevin Kane, Public Policy Manager with Twitter.

If the witnesses would be so kind as to rise and raise your right hand, I will begin by swearing you in.

[Witnesses sworn.]

Mr. LYNCH. Let the record show that the witnesses have all answered in the affirmative.

Thank you, and please be seated.

The microphones are sensitive, so please speak directly into them.

Without objection, your written statements will be made a part of the record.

And with that, Secretary Galvin, you are now recognized to give an oral presentation of your testimony.

STATEMENT OF BILL GALVIN, SECRETARY OF THE COMMONWEALTH, MASSACHUSETTS

Mr. GALVIN. Thank you, Chairman Lynch and Ranking Member Hice, and distinguished committee members of the Subcommittee on National Security, for inviting me to testify today on the safety and security of the Nation's election infrastructure and the ongoing misinformation attempts to influence public opinion and trust in our election system.

As you noted, my name is Bill Galvin, and I have been the Secretary of the Commonwealth of Massachusetts since 1995. During my tenure as Secretary, I have worked hard to ensure elections in Massachusetts are fair, honest, and accurate. I am proud of that effort. My office has successfully implemented a statewide data base after passage of the National Voter Registration Act and continues to make improvements to implement state and Federal laws, including the Help America Vote Act.

In recent years, however, new challenges have emerged. I don't need to tell this committee what they are. I think you have discussed it very thoroughly here. I am here today to share with you the best practices we are using in Massachusetts and explain the challenges we face and what must be done moving forward.

Before addressing these topics, I think it is important to note the differences in election administration throughout the country and how this leads to unique challenges. Unlike the majority of the country in which election administration is county-based, in Massachusetts and the rest of New England, as well as in Michigan and Wisconsin, elections are conducted on a municipal level with local election officials in each of the cities and towns. Local election officials in Massachusetts, many of whom have responsibilities beyond elections such as vital records, and some of whom are part-time, have varying skills and expertise in security and overall information technology knowledge, as well as varying access to the resources likely available to county officials, such as onsite technical help.

Our best practices are pretty basic. Voting equipment in Massachusetts, all voters vote on paper ballots, and during my administration that has been something I have insisted on. Some ballots are hand counted, but most are tabulated through scanners. Tabulators must be federally certified and then state certified. Tabulators are not connected to the Internet, to each other, or to any external device, either by Wi-Fi or hard wire. Tabulators are required to undergo public logic and accuracy testing before every election. Clerks test the machines using the same ballot that will be used on election day. Tabulators are locked into the ballot box throughout the day. The keys to the ballot box and the tabulator are held by the police officer present in every polling location. In the event of a machine failure, voting continues and the ballots are hand-counted in public view at the end of the night. In the event of power failure, tabulators have a back-up that allows them to continue to operate.

In the event of an emergency or machine failure, the paper ballot can be hand-counted by poll workers. Voting can continue despite the power failure or natural disaster or other emergencies. Official results of the election are recorded by hand and certified. Official returns of the votes are entered into the statewide data base, and the official report must be printed, signed, and certified by the clerk and transmitted by mail.

Our statewide data base of voter registration is not on the Internet. My office maintains and supports the statewide data base voter registration system, VRIS. VRIS can only be accessed through an isolated network that connects each of the local election officials to my office. VRIS is not available via the Internet, as I have said. Users can only access the statewide data base using the work stations and equipment provided by my office.

The network is monitored. Albert sensors throughout the DHS are installed on the network. Each user has a unique username and a complex password. Users have separate logins for computers and for VRIS application on the computer. User transactions are logged with a date and time of the action taken.

The general cybersecurity is something that has always been a concern. Even prior to the spotlight on cybersecurity in 2016, we had worked to develop our data network and keep it secure. Prior to 2016, we contracted with independent vendors. Since the threat emerged in 2016, efforts have increased, including the addition of staff and tools to ensure the network and infrastructure. Using the new HAVA funds, we have created a robust cybersecurity team staffed by professionals. We use proper protocols and passwords to make sure it is done.

I want to focus in the seconds that I have left on what I think is the overarching issue that has to be dealt with, the urgency of action. This election is now less than 18 months away. If there is going to be any practical impact on what happens in 2020 given the threats that have been discussed here today, urgent action is needed, particularly at the level of the EAC. Even in a state like mine, where equipment is used for paper ballots, the need to process and certify new equipment is urgent. The bureaucracy has to be streamlined. Action must be taken now.

Given the amount of time left to acquire new equipment, to train people on it, and to have it in service on election day in 2020, there is no time. There is no time for bureaucracy. As somebody who has successfully run bureaucracies now for almost 25 years, I will tell you that the only way to get that kind of action is to demand time standards to make sure it is done.

Absent that effort, there will still certainly be problems with equipment and with process in 2020, the very problems that this committee has convened to hear about today. It is urgent that this committee urge the Congress and the Administration and the EAC and all the Federal bureaucracies that are here today to take action and to take it now to support the State officials involved.

Thank you very much for your attention.

Mr. LYNCH. Thank you, Secretary Galvin.

Mr. Gleicher, you are recognized for five minutes.

STATEMENT OF NATHANIEL GLEICHER, HEAD OF CYBERSECURITY POLICY, FACEBOOK

Mr. GLEICHER. Chairman Lynch, Ranking Member Hice, and members of the subcommittee, thank you for the opportunity to appear before you today. My name is Nathaniel Gleicher, and I am the Head of Cybersecurity Policy at Facebook. My work is focused on addressing the serious threats we face to the security and integrity of our networks and services. I have a background in both computer science and law. Before coming to Facebook, I prosecuted cybercrime at the U.S. Department of Justice and built and defended computer systems and networks.

Facebook cares deeply about defending the integrity of the democratic process. We don't want anyone using our tools to undermine elections or democracy. We have dedicated substantial resources to finding and removing malicious activity on our platforms. In fact, we have more than 30,000 people working on safety and security across the company, reviewing reported content in more than 50 languages, 24 hours a day. That is three times as many people as we had in 2017. And we have nearly 40 different teams focused particularly on election work across Facebook's family of apps.

We drive our election integrity efforts through a combination of automated systems and expert investigative teams. Our automated tools operate at scale, making any attempted bad behavior more difficult, while our expert investigators tackle the newest and fastest-moving threats. This combination ensures that we can continually evolve our responses as the threats change, identifying new trends early and staying ahead of them as they develop.

We aren't perfect, and this is an ongoing challenge, but we are improving every day.

Our election integrity efforts are focused on four major areas: blocking and removing fake accounts; finding and removing bad actors; limiting the spread of false news and misinformation; and increasing transparency for political advertising.

First, fake accounts are often behind harmful and misleading content, and we work hard to keep them off Facebook. In fact, we identify and remove millions of fake accounts from the platform every day, many shortly after they have been created.

Second, we focus on networks of deceptive behavior, which we call coordinated inauthentic behavior, or CIB. This is when networks of accounts, pages, or groups work together to mislead others about who they are or what they are doing. When we remove a network for engaging in CIB, it is because of the deceptive behavior that the group engages in—for example, using fake accounts to conceal their identity—not because of the content they post, the actors they represent, or the views they espouse.

We ban this kind of behavior so people trust the connections they make on Facebook. And while we have made real progress, it is an ongoing challenge because the actors engaged in this behavior are determined and often well-funded. We have to improve to stay ahead of them, including by building better technology and working more closely with law enforcement, security experts, and other companies.

Third, to combat false news, we follow a three-part framework. We remove content that violates our community standards. For content that doesn't directly violate our community standards but still undermines the authenticity of our platforms, like click bait or sensational material, we reduce its distribution so fewer people see it, and we give people more context about the information they see in News Feed.

Finally, when it comes to political advertising, transparency is critical. We work to ensure that people are able to understand easily why they are seeing ads, who paid for the ads, and what other ads that advertiser is running. We also require election-or issue-related ads on Facebook and Instagram to be labeled clearly, including a "paid for by" disclosure from the advertiser at the top of every ad.

In support of all of these efforts, we opened our first physical election operation center at our headquarters in Menlo Park in advance of the U.S. midterms last year. We have a dedicated team already focused on preparing for the 2020 election, and we will have an operation center set up to support that effort.

We are proud of our ongoing work to protect the integrity of our elections, but we know there is more to do. This is fundamentally a security problem. As we continue to improve our defenses, bad

actors evolve their tactics. This is also a whole-of-society challenge, which is why we focus on working so closely with our colleagues in industry, in government, and in civil society.

We will never be perfect, and we are up against determined adversaries, but we are committed to doing everything we can to strengthen our civic discourse and protect elections.

Once again, thank you very much for the opportunity to be here today, and I look forward to answering your questions.

Mr. LYNCH. Thank you, Mr. Gleicher.

Mr. Kane, you are recognized for five minutes.

STATEMENT OF KEVIN KANE, PUBLIC POLICY MANAGER, TWITTER

Mr. KANE. Chairman Lynch, Ranking Member Hice, and members of the subcommittee, I am grateful for the opportunity to appear before you today.

Twitter's purpose is to serve the public conversation, and the public conversation occurring on Twitter is never more important than during elections. I have provided more detail in my written testimony but would like to briefly outline some of the most important work we are doing to support the integrity of our elections by fighting platform manipulation and increasing transparency.

As the Internet evolves, so too do the challenges and opportunities society faces. Following the 2016 U.S. elections, Twitter's entire strategic posture changed. Collaborative partnerships with peer companies, Federal agencies, law enforcement, state governments, and civil society organizations were key to our preparation ahead of the 2018 U.S. midterms.

Since January 2017, we have launched dozens of product and policy improvements, expanded our enforcement and operations, and strengthened our team structure, all designed to foster the health of the service and protect the people who use Twitter. We continue to promote the health of the public conversation by countering all forms of platform manipulation. We define platform manipulation as using Twitter to disrupt the conversation by engaging in bulk, aggressive, or deceptive activity.

We have made significant progress. In fact, in 2018 we identified and challenged more than 425 million accounts suspected of engaging in platform manipulation, of which approximately 75 percent were ultimately suspended. We are increasingly using automated and proactive detection methods to find misuses of our platform before they impact anyone's experience. More than half of the accounts we suspend are removed within one week of registration, many within hours. We will continue to improve our ability to fight manipulative content before it affects the experience of people who use Twitter.

In addition to our efforts to safeguard the platform, we are committed to providing greater transparency around the conversation regarding elections. We believe transparency is a proven and powerful tool in the fight against misinformation and disinformation campaigns. We have taken a number of actions to disrupt foreign operations and limit domestic efforts at voter suppression, and have significantly increased transparency around these actions. We publicly released in January a retrospective review of the activity

that occurred on Twitter regarding the 2018 U.S. midterm elections. Last fall's midterms were the most tweeted about midterm elections in history. Twitter facilitated a robust global conversation that included more than 99 million tweets from the first primaries in March through election day. I have provided a full copy of our report, along with my submitted testimony, to be included in the record.

Our commitment to transparency extends to providing a unique archive of information operations to the public and researchers. We have provided data and information on more than 9,600 accounts, including accounts originating in Russia, Iran, and Venezuela, totaling over 25 million tweets. It is our fundamental belief that these accounts and their content should be available and searchable so members of the public, governments, researchers, and the broad community can investigate, learn, and build media literacy capabilities for the future.

Information operations are nothing new and have been a tool since before the dawn of social media. These operations continue to adapt and change as the geopolitical terrain evolves worldwide and as new technologies emerge. For our part, we are committed to understanding how bad-faith actors use our services.

We also have provided additional transparency with regard to paid advertisements on Twitter. Last year we launched our Ads Transparency Center where anyone, whether they have a Twitter account or not, can search for all ads running on the platform. You are able to find in our Ads Transparency Center a significant level of detail associated with each ad, including billing information, ad spend targeting, and impression data.

As I previously mentioned, partnerships are critical to this work, including collaboration with Federal, state, and local election officials. Since 2016, we continue to strengthen relationships with law enforcement agencies, including the Federal Bureau of Investigation's Foreign Influence Task Force and U.S. Department of Homeland Security. Indeed, on election day for the 2018 U.S. midterms, Twitter virtually participated in an operation center convened by the U.S. Department of Homeland Security.

In closing, our efforts enable Twitter to fight this threat while maintaining the integrity of people's experiences on Twitter and supporting the health of the conversation on our service. Our work on this issue is not done, nor will it ever be. I appreciate the opportunity to share our work with the members of this subcommittee.

Mr. Chairman, I would like to thank you again for calling this important hearing, and I look forward to your questions.

Mr. LYNCH. Thank you, Mr. Kane.

Mr. Salgado, you are now recognized for five minutes.

STATEMENT OF RICHARD SALGADO, DIRECTOR OF LAW ENFORCEMENT AND INFORMATION SECURITY, GOOGLE

Mr. SALGADO. Chairman Jordan, Chairman Lynch, Ranking Member Hice, and members of the committee, thank you for inviting me to testify today about Google's efforts to promote election integrity. I appreciate the opportunity to discuss our efforts in this space.

My name is Richard Salgado. As the Director of Law Enforcement and Information Security at Google, I work with thousands of people across teams at Google to protect the security of our networks and user data.

Google's mission is to organize the world's information and make it universally accessible and useful. Efforts to undermine the integrity of democratic elections are antithetical to that mission.

In my testimony today, I will focus on four areas where we are making progress to help ensure the integrity of elections. First, we are working to empower people with information they can trust when going to the polls. Second, we are helping defend campaigns, candidates, and others from network attacks. Third, we are combatting misinformation. And fourth, we are improving transparency of election advertisements.

I will start by addressing a few of the ways we are helping to empower people with information about their elections. We created our search engine in 1998 with a mission of providing greater access to information. To this end, Google aims to make civic information more easily accessible and useful to people globally.

In 2018, for example, we helped people in the U.S. access authoritative information about registering to vote, locations of polling places, and the mechanics of voting. We have partnered with organizations like the Voting Information Project and with the offices of 46 Secretaries of state to achieve this goal. On election day, we serviced election results for U.S. Congressional races directly in Search in over 30 languages.

We have also made voting information freely available through the Google Civic Information API. Over 400 sites have availed themselves of this API.

Google also offers a broad array of services and tools to help campaigns, candidates, and election officials reduce the likelihood of a successful security breach. We have multiple internal teams that work together to identify malicious actors, disable attacker accounts, secure victim accounts, and share threat information with other companies and law enforcement officials. In addition, Google's Threat Analysis Group, a dedicated team of security professionals, further detects, prevents, and mitigates government-backed threats, including through the use of warnings to users when we believe they may have been the targets of government-backed attacks.

In 2017, we unveiled the Advanced Protection Program, which provides the strongest account protection that Google offers. As part of that program, we have conducted extensive outreach to promote the use of security keys, which protects users from more sophisticated and targeted phishing campaigns.

Similarly, Google's safe browsing tool helps protect more than 4 billion devices from phishing. Safe browsing hunts and flags malicious extensions, helps block malicious ads, and shows warnings about websites it considers dangerous or insecure.

Separately, Google and Alphabet's Jigsaw Group have partnered on Protect Your Election, a suite of tools to help campaigns, candidates, and election-related websites protect themselves online. The initiative includes Project Shield, a free tool to mitigate the risk of distributed denial-of-service attacks.

We also recognize that it is critically important to combat misinformation in the context of democratic elections. This is especially important when users are seeking accurate, trusted information that will help them make critical decisions. We have a natural, long-term incentive to prevent anyone from interfering with the integrity of our products, and we have worked hard to curb misinformation.

Our efforts include designing better ranking algorithms and implementing tougher policies against misleading behavior, and deploying multiple teams to identify and take action against malicious actors.

At the same time, we have to be mindful that our platforms reflect a broad array of sources and information, and there are important free speech considerations. There is no silver bullet, but we will continue to work to get it right.

We have also been working hard to make election advertising more transparent. In 2017, we committed to making improvements to this important area, and we have delivered on our commitment. This includes a verification program for advertisers purchasing U.S. Federal election ads, in-ad disclosures of the name of the advertisers and, of course, a transparency report for election ads.

Looking forward, we are thinking hard on how to bring more transparency to election advertising online.

In conclusion, we appreciate that there is no panacea for the challenges that lie ahead, and we commend the committee for its efforts to ensure that we are collectively taking concrete steps to protect the integrity of our elections. Google is committed to building on our progress.

Thank you for the opportunity to address these issues, and I look forward to your questions.

Mr. LYNCH. Thank you.

There are currently seven votes scheduled on the floor. There is no time remaining prior to votes commencing. There are 260 members not voting yet, among us as well. So we will recess for those seven votes, and the committee will reconvene five minutes after the last votes on the floor. Thank you.

[Recess.]

Mr. LYNCH. Welcome back. We apologize for the delay with votes on the floor.

I now yield myself five minutes for questioning.

Secretary Galvin, the Omnibus Appropriations Act, enacted by Congress back in March 2018, included about $380 million for grants distributed under HAVA, the Help America Vote Act, to assist states in securing their voting systems against malicious cyberattacks and other vulnerabilities. HAVA marked the first Federal appropriation for this purpose in over 10 years.

In July of last year, the U.S. Election Assistance Commission announced that each of the 55 eligible states and territories had already requested 100 percent of the newly appropriated funds. According to the Election Assistance Commission, the Commonwealth of Massachusetts applied for and received nearly $8 million in grant funding. Is that correct?

Mr. GALVIN. Yes.

Mr. LYNCH. I think you are sort of a model situation where we have a paper back-up system. I vote there, so I am well aware of your system. Can you discuss some of the key election components where you applied that money, and maybe some gaps that continue to exist that could use some additional funding?

Mr. GALVIN. Well, first of all, Mr. Chairman, we had a pretty good system regarding our data base. Primarily it was on the data base side, what we used the appropriation for. As I mentioned during my regular testimony, we had vendors hired to make sure to protect our system.

With the new moneys that were made available, we upgraded, and as a result we were not subjected to attempted hacking in 2016, or so we were informed by Homeland Security. Nevertheless, as I frequently have pointed out, while the focus appropriately is on foreign action, it is also possible people domestically could do it.

Mr. LYNCH. Oh, sure.

Mr. GALVIN. As you are well aware, we have many institutions of higher learning in Massachusetts who have students who think they are geniuses, and probably are. The fact of the matter is, it is a challenge for them to think about breaking into things like our system.

So what I did after getting the new funds was to upgrade the quality of the security we had. We also have a specific person on staff now who only deals with cybersecurity issues. We continue to look forward to ways to implement our system.

The data base we created or we built is now approaching its 20th anniversary. We are going to have to replace all of it after the 2020 election. So we are looking to ways to make it more secure.

As I also mentioned in my affirmative testimony, because of the network by which we operate in Massachusetts and other New England states where we rely upon local communities and local election officials, some of whom I don't appoint and have no direct control over, we have to try to integrate them into our system. So much of the funds have been used to try to do that, to upgrade the quality of what they are doing at their local level to protect against any sort of intervention there.

With regard to equipment, we are looking at ways that in the future we can upgrade our equipment. One of the ways, for instance, where EAC action would be very helpful is electronic poll books. We are not allowing them to integrate with our system right now because we do have security concerns about them, but they could be helpful if there was a way to be assured of the quality of the security that they would be using, especially for things like early voting and other aspects of our election system.

Mr. LYNCH. Just to be clear, I know you testified that back in 2016, the analysis that was done, there were no breaches in Massachusetts.

Mr. GALVIN. That we were informed of. There had been attempts going back many years. We know something occurred, an attempt, but there have been no successful breaches as far as we know, and we——

Mr. LYNCH. What about 2018? What about the midterms?

Mr. GALVIN. Again, there were curious events that occurred but no breaches as far as we know.

Mr. LYNCH. Okay. I know this is an open forum, but to the extent possible, can you describe key actions that Massachusetts has taken to safeguard voting systems against that kind of foreign interference?

Mr. GALVIN. Again, as I mentioned, the key for us in terms of the equipment is we use a paper ballot system, so we also have the paper cards to fall back upon. So the only aspects of the system that could be electronically hackable would be the tabulators, which I mentioned again in my affirmative testimony. They are tested all the time. If there is a failure in the tabulator, we still have the cards to work with.

The data base for voter registration information is not on the Internet, so we have kept it secure that way. We continue to have concerns, like I mentioned the electronic poll book. Some communities have used electronic poll books internally for early voting and things like that, but we don't let them connect it to our system.

So there are concerns we have about all of these things that are going forward, and I don't think any of us can say we have a perfect system, nothing bad could ever happen to us. That is not true. We have to be vigilant.

One of my great concerns, I mentioned this earlier, about the certification process is all of us at the local level, state and local level that are dealing with election administration are going to have to replace equipment. We need the EAC to move on equipment as fast as possible. It is not happening, and I think you brought that out today in the testimony you received from them. That is the biggest problem all of us have, no matter what kind of system you have right now, anywhere in the United States.

Mr. LYNCH. I do have one data point, that when we did the analysis, 45 states have systems that are no longer manufactured, no longer currently manufactured. That tells you how—these are legacy systems that are completely outdated.

Mr. GALVIN. We have communities—you are familiar with the city of Lawrence, Massachusetts. They are a poor community. They want to replace their equipment. They need to replace it, and everything if paper ballot. But still, with the technologies that are available, the ones they would like to buy haven't been certified. We are concerned that if they were to make an investment in the ones that are currently available and certified, they may be replaced within the next few years, during the life of the equipment they purchased, and not have any money to replace them with. So it is a dilemma.

Specifically, I think we all see 2020 as having a very, very large turnout. We had a big turnout last year. We are going to have bigger turnouts in 2020. We all know that. And given the awareness the public has about voter security, which is a good thing for the most part, there is going to be anxiety. So we want to make sure we allay that anxiety by having the best equipment possible. Whatever state you are in, whatever kind of system you have that the local officials are trying to use, we want to give them the best equipment.

The problem right now is to make sure the bureaucracy functions to effectively give local officials options when it comes to equipment. That is not happening.

Mr. LYNCH. Right. Thank you.

I now yield five minutes to the Ranking Member.

Mr. HICE. Thank you, Mr. Chairman.

I knew coming into this, quite frankly, that we were going to hear the excellent work that these three companies are doing to try to safeguard their users from foreign interference. I get that.

My concern, though, is the active engagement from these companies into the speech of users as a publisher rather than a platform. Just last week, I believe it was, a Facebook memo leaked that catalogued so-called "hate agents," and of course it included some conservative individuals, Candace Owens. In fact, Mr. Speaker, I have a screenshot of that that I would ask unanimous consent be added to the record.

Mr. LYNCH. Without objection.

Mr. HICE. Thank you.

And I look at this with great concern. We have heard of it. We have had hearings about this type of thing.

Mr. Gleicher, let me ask you, it has been confirmed from Facebook that these "hate agent" lists exist, and you guys are supposedly a neutral platform. But doesn't the existence of these type of actions really create a type of election interference that you are trying—at least you say that you are trying to avoid?

Mr. GLEICHER. Congressman, thank you for the question. So the question that you are asking is an important one. Facebook is a platform for ideas across the spectrum. Whenever we are thinking about creating a new policy or changing the line in a policy, one of the things that we do is we look at what effect that might have, and in particular would it have any unintended consequences.

So in this context, we developed a list of people who are engaged in the public debate around white nationalism, white separatism, people who might be affected by this policy change, so that we could do the due diligence to understand what affect the change in this policy would have. This was an internal list so that we could do that type of analysis.

Ms. Owens was not affected by the policy, and——

Mr. HICE. She was initially. She got put back on, but she was.

Mr. GLEICHER. Congressman, these are actually two separate points. So, she was on the list, along with a number of other people, because we wanted to understand what affect the policy would have.

Mr. HICE. So, look, if you are engaged in curation of speech, you are de facto a publisher rather than a platform, and that is part of the issue here. I understand there are algorithms and all this kind of stuff, all these words you are catching and all this kind of stuff. But the code also includes de-boosting and shadow banning, and again there have been multiple examples of that—Steven Crowder, Daily Caller, and others. I mean, this goes on and on.

So doesn't even the algorithm itself indicate a bias that has been placed into the algorithms?

Mr. GLEICHER. Congressman, we are a platform for ideas. One of the things that is most important for us is to ensure that there is a space where people can speak safely and engage in public debate, robust public debate.

Mr. HICE. And there is a problem with that, which makes the whole platform issue in itself debatable, as opposed to being a publisher.

Mr. GLEICHER. I think one of the critical things in creating a space for public debate is to ensure that when statements cross the line into violence or threats or clearly are hate speech, we are able to take action in that space to ensure that people can engage in a discussion.

Mr. HICE. There is not that kind of conversation going on with Steven Crowder and Daily Caller. I mean, therein lies the problem. You can say what you want to say, but there are issues where conservatives are the ones oftentimes, most of the time, who are on the short end of this stick. One of your engineers, DeRuvo—I don't know how to pronounce his last name, but he actually made the statement, he said one strategy is to shadow ban so that you have ultimate control. The idea of shadow banning is that you ban someone and they don't know that they have been banned, because they keep posting but no one sees it, no one sees the content.

This is taking place, and it is inexcusable. We have got to get to the bottom of it, and it doesn't stop there. There was a report in May 2016 of stories of interest to conservative readers on Facebook who were routinely suppressed by human news curators. So there is both a problem with the human and the artificial. Bias is the problem that has got to be addressed.

Mr. GLEICHER. Congressman, we have a range of systems in place to address conscious or unconscious bias, and I think by combining—we have rigorous training programs and automated systems, and most critically we have an appeals process because we are not going to get every one of these right. We will make mistakes.

Mr. HICE. Well, it has got to get right as we are coming into another election cycle. We don't have time for appeal after appeal after appeal. These issues are problematic now, and I want to see—and my time has expired, but I want to see the solutions that you are coming up with in the political spectrum primarily directed against conservatives who do not have a voice. And this is not just toward Facebook but it is Twitter—we are seeing this kind of thing across the board. The transparency, we can talk about all these fancy things that we want to do, and I appreciate the effort that is being done, but the transparency and the outcome has still got to be resolved that this is indeed a platform and it is not a publisher where speech in itself is being censored.

And with that, Mr. Chairman, I will yield. Thank you.

Mr. LYNCH. The gentleman yields back.

The Chair now recognizes the gentle lady from Illinois, Ms. Kelly, for five minutes.

Ms. KELLY. Thank you, Mr. Chair.

The Special Counsel's report detailed an extensive Russian social media influence campaign during the 2016 Presidential election, primarily coordinated by the Internet Research Agency. As part of this operation, the IRA purchased political advertisements on social media in the name of U.S. individuals and organizations. The intent of these ad purchases was to, quote, "reach larger U.S. audiences."

Facebook has reported that the IRA purchased over 3,500 political ads on its platform, totaling an estimated $100,000, before the 2016 election. Google likewise discovered that thousands of dollars in advertisements on YouTube, Google Search, Gmail, and other company products were purchased by accounts associated with the Russian government during the 2016 election cycle. Political ads were also purchased from Russian Internet or physical addresses or using Russian currency.

Mr. Gleicher—is it Gleicher? What is it?

Mr. GLEICHER. Gleicher.

Ms. KELLY. Okay, I want to say it correctly. Can you briefly discuss the nature of these ads and give us an estimate on how many times they were viewed?

Mr. GLEICHER. Thank you, Congresswoman. One of the actually most important things that we have done in the wake of 2016 is a range of things to address the types of challenges you are talking about, particularly political advertising and ways that could be used by a foreign actor. I spoke in my opening statement a little bit about some of our transparency tools, but another piece that is important here is that we have imposed additional registration requirements and verification requirements, so that if someone wants to run political or issue ads in advance of an election, they have to verify that they are domestic actors, they have to provide an address, and they have to provide identifying information about themselves to tackle exactly the challenges you are talking about.

Ms. KELLY. So can you give me the nature of the ads and give us an estimate of how many times they were viewed from before? Do you know?

Mr. GLEICHER. So, for the ads that were published around the context of 2016 and 2017, we released those to Congress with the ads and with some information about how many impressions each received, and that information is public. I don't have the specific numbers on me right now, but all of that information has been made public.

Ms. KELLY. Okay. The purchase of political ads online has remained a tool of foreign election interference. In September 2018, the Department of Justice charged a Russian national with conspiring to interfere with the U.S. political system. As an alleged accountant for a Russian foreign influence operation known as Project Lakhta, the defendant spent over $60,000 on Facebook ads and over $6,000 for ads on Instagram prior to the 2018 midterm elections.

Can you again—I missed your opening statement. Can you briefly discuss the steps you have taken since 2016 to increase transparency and accountability in online ad purchases?

Mr. GLEICHER. Certainly, Congresswoman. So first, in the context of transparency, what we have done is we have created an ads library where any ad that is political in nature, that is specifically about a particular candidate or involves a political issue, will be visible in public for seven years. People will be able to see who ran the ad, how much was spent on it, the types of people who saw it, and in particular they will be able to see if individuals or groups ran multiple ads.

So, for example, one could see if someone was running one ad to one community saying their taxes would go up, and another ad to a different community saying taxes would go down. That type of transparency actually has already enabled a number of researchers to identify mismatches and concerning trends. One of our key goals has been to empower the public and researchers to be able to see some of these patterns.

That is one piece of the work, and then the other piece is that verification work that I described to you, and what is most encouraging about that is we have seen instances of foreign actors since those controls were in place trying to get verified and then failing.

Ms. KELLY. That is good news.

In her statement, Federal Election Commission Chairwoman Ellen Weintraub testified to how foreign adversaries can contribute to a 501(c) organization that can, in turn, contribute funds to a Super PAC without disclosing the foreign source of money. Furthermore, a foreign-owned LLC can contribute to a 501(c) or a Super PAC without those entities ever disclosing the true owners of the LLC.

What additional steps do you think are needed to limit the use of digital ads by hostile state actors to interfere in elections? And you can answer, Mr. Kane can answer, or Mr. Salgado, or all of you.

Mr. KANE. Ma'am, thank you very much for that question. It is a very important point. Similar to Facebook and Twitter, we have a very robust and rigorous process for those who seek to purchase political ads. The process takes about a week, and if an organization or an individual doesn't have an FEC I.D., it involves the U.S. Postal Service and getting forms notarized. We have built a lot of friction into the process to deter bad actors.

Once an ad is certified to run political ads, it is available and searchable. You do not have to have a Twitter account to see what political ads are running, who paid for them, and the impressions of their tweets and information like that. That information is all available, and it is going to stay up for an indefinite period of time.

Ms. KELLY. I am out of time, so I don't know if you want Mr. Salgado to answer.

Mr. SALGADO. I am certainly happy to answer that, as well. We also have the same sort of verification process for election ads that requires the proof of identity and the various numbers that show that they are campaigns. We are very live time when an ad is actually displayed. We have the ability for the user to see who is behind the ad. So when it is displayed, it would either be displayed underneath the ad saying who actually is the purchaser of the ad, or they will be able to click through and easily find it.

We also have a transparency report about the ads so that even if you were never served an ad, you can actually go and look at spends by different purchasers of ads and get a pretty good deep dive into what sort of content is being displayed through the different campaigns.

Mr. LYNCH. The gentle lady yields.

The Chair now recognizes the full committee Ranking Member, the gentleman from Ohio, Mr. Jordan, for five minutes.

Mr. JORDAN. I thank the Chairman.

Mr. Kane, does Twitter shadow ban?

Mr. KANE. No, sir.

Mr. JORDAN. Last summer, were there accounts, were there Twitter accounts that were not being auto-suggested?

Mr. KANE. Yes, sir. There were approximately 600,000 accounts across the platform that were not auto-suggested. Once you click Search, the accounts that you were searching for came right up. But we identified that bug and fixed it within about 24 hours, and then publicly explained exactly what happened with regard to that issue.

Mr. JORDAN. Six-hundred thousand?

Mr. KANE. I apologize; 600,000. Yes, sir.

Mr. JORDAN. How many total Twitter accounts are there?

Mr. KANE. Approximately—we have about 330 million monthly active users.

Mr. JORDAN. Three-hundred thirty million, but only 600,000 had this auto-suggest feature not work; is that right?

Mr. KANE. Yes, sir, that is my understanding.

Mr. JORDAN. How many of those 600,000 were Members of Congress?

Mr. KANE. I believe the number was approximately four.

Mr. JORDAN. Do you know who those four were?

Mr. KANE. I believe one was your account. I believe Congressman Meadows, Congressman Nunes, and I can't recall the fourth off the top of my——

Mr. JORDAN. Mr. Gaetz.

Mr. KANE. Yes, sir, that is correct.

Mr. JORDAN. So only 600,000 out of 330 million. There are 435 members of the House, and 100 members of the Senate, 535 accounts. But four of them had this happen to them, and they just happened to be four Republicans, four conservative Republicans. Was that just an accident?

Mr. KANE. Yes, sir.

Mr. JORDAN. Total accident.

Mr. KANE. Yes, sir, and that is exactly why we fixed the problem.

Mr. JORDAN. Okay. You can assure this committee that there is no shadow banning that ever takes place with Twitter accounts?

Mr. KANE. Yes, sir. Twitter does not shadow ban.

Mr. JORDAN. Okay. So, I think you said earlier in your opening testimony 99 million Tweets were sent last election cycle; is that right?

Mr. KANE. Yes, sir. Between March and November of last year, there was approximately 99 million tweets associated with the U.S. midterms.

Mr. JORDAN. So four Republican accounts had a problem with them that made it difficult for people to access those accounts during that timeframe; is that right?

Mr. KANE. Yes, sir. We provided to the committee—we provided information in terms of the follower graphs over a period of time, and we noticed no impact whatsoever in terms of the amount of followers that each of those accounts received over time.

Mr. JORDAN. They grew?

Mr. KANE. Yes, sir.

Mr. JORDAN. That is right, they did grow. They actually grew during the time that you were actually making it difficult for people to access those four accounts. What is interesting, once you fixed the problem, they grew a lot faster. So there may have been an impact.

Mr. KANE. Sir, it is difficult to determine. There were a number of Members of Congress who were talking about that issue, which could generate more interest and lead to more followers. It is difficult to determine motives.

Mr. JORDAN. Has it happened since?

Mr. KANE. Not that I am aware of, sir.

Mr. JORDAN. Were there any Democrats that had their accounts—the same thing happen to them?

Mr. KANE. Sir, with 600,000 accounts worldwide, that accounts for a number of views across the ideological spectrum. And so I feel very——

Mr. JORDAN. No, no. I meant—fair enough. Democrat officer holders.

Mr. KANE. I don't recall, but I would be happy to followup for the record. I know that there was a few individuals who, at the state level, were of the Democrat Party that were running. I don't have those specific names, but I would be more than happy to see what we can provide for the record.

Mr. JORDAN. Mr.—is it Gleicher? Mr. Gleicher?

Mr. GLEICHER. Yes, Congressman.

Mr. JORDAN. I think earlier you said that you would, when you have bad actors, they are removed, their comments or whatever are taken down. Who defines who the bad actors are?

Mr. GLEICHER. Thanks, Congressman. Specifically, there I was talking about actors that we see who are engaged in coordinated inauthentic behavior, which is the coordinated use of fake accounts and other assets to manipulate people, and in particular to deceive users about who they are or what their purpose is.

Mr. JORDAN. Okay.

Mr. Kane, same question. Bad actors on Twitter, who defines who is a bad actor and who is not, and what happens with those accounts, with those individuals?

Mr. KANE. Yes, sir. We have a number of policies to support the conversational health of Twitter. We have clearly defined policies on fake accounts. We have clearly defined policies on spam. So it is a broad range of issues as we continue to focus on improving the health of the conversation. It is not just one particular area.

Mr. JORDAN. Thank you.

Mr. Chairman, I yield back.

Mr. LYNCH. The gentleman yields back.

The Chair now recognizes the gentleman from California, Mr. DeSaulnier, for five minutes.

Mr. DESAULNIER. Thank you, Mr. Chairman. Thank you for this hearing.

Mr. Galvin, thank you for your years of service. Given your years and how diffuse our oversight is, and given what you have heard today from these three companies that have a net worth and financial resources greater than most states, how do we hold them accountable? This is all nice to hear, but, quite frankly, people don't

trust the three of you the way they did five or 10 years ago in your organizations. They don't trust Congress very well, either.

So in a diffuse election process, how do you as an election overseer, who has seen years of traditional miscommunication, how do we make sure that we have the right oversight nationally?

Mr. GALVIN. Well, it is very hard. Obviously, at the same time we want to protect people's freedom of speech, and it has been a problem that pre-dates the particular manifestation that this represents.

I think this hearing is a good start. As you know, a number of national spokespersons and candidates for president have suggested breaking up some of these entities. I am not sure that is necessarily the solution, although it is a reasonable suggestion to discuss.

I think I am very focused on the 2020 election because I think that is going to be defining in terms of policy going forward on elections. You are quite correct in saying that the whole situation has changed dramatically, certainly over my tenure. I think the question is what kind of scrutiny is going to be provided, and the scrutiny is not simply over how they use their platforms, it is going to be how people use them and what they do about it.

I suppose the best solution immediately is disclosure. I think the Congress going forward has a role to play in terms of monitoring not only their activity but, as I mentioned earlier, the activities of some of the bureaucracies that interact with the states, and the activities of the states.

While the states are sovereign states when it comes to election issues, nevertheless we want to make sure that states are performing correctly and adequately in terms of equipment and the maintenance of their data bases.

So I think in the short run—and I made a big point earlier, and I will recite it again—we have 18 months now left to this election, and the election is underway for all intents and purposes. I think regular scrutiny and updates, whether it is on equipment, preparation, certification, or conduct, is necessary. There has to be some mechanism by which all of these things are reviewed on a regular basis, and I think the Congress can contribute to that, I really do. Whichever point of view is represented, having that scrutiny out there for all of us I think is going to be helpful to making sure the whole process is transparent.

Mr. DESAULNIER. I appreciate that, Mr. Secretary.

To the three companies, as someone who moved from Boston to San Francisco in the 1970's, I have been to all your headquarters. I have been very proud of you as part of the culture of San Francisco, but my relationship has soured because of this and because of other things, and this is a real defining time for all three of you, and I think you are all aware of this, about trust.

In your innovation, we had an earlier hearing about facial recognition, and all three of us were there, and I hear you are inhibiting innovation if you are a policymaker and you question tech companies at all. And now you are here. I wish there was a way we could work with you so that we all were on the right page.

Having said that, and this is directed to Mr. Kane, MIT has done a study not long ago that looked at false rumors, negative rumors

on your platforms, all of social media, and how quickly that goes out. There is something about human nature that likes to—it is just like the car crash. There is certainly a lot of research and books that have been written about how you make money off of—I mean, in the newspaper business it used to be "if it bleeds, it leads." Your models are much more sophisticated.

So my question is there are human factors—the National Labs study human factors for the Secret Service, for public safety, and for NASA. We are learning more and more about how the mind works. You folks are spending a lot of money on that, to make more money.

How do we incorporate human factors as we anticipate, not just identify, somebody who is on your platform or using your infrastructure to affect democracy and elections? How do you sort of go a step forward as related to the MIT study? The quote I have here as part of that study, on the negative effects and rumor cascades: "This implies that misinformation containment policies should also emphasize behavioral intervention, like labeling, and incentives to dissuade the spread of information, and looking into human factors in neuroscience."

So do you have any response, any of you, to that? Mr. Kane to begin with.

Mr. KANE. Yes, sir. Thank you very much for that question. Partnerships are absolutely vital for the work that we do to better understand the current threat, which is always evolving, and to help better inform our policies and product changes. Just as recently as this week, Oxford released a study that found, with regard to the conversations around the elections in the EU, that less than four percent of tweets shared information from low-quality content. I refer to the Oxford study for their definition of low-quality news content. So we are clearly making significant progress as we continue to fight platform manipulation, as we continue to clean up the platform and develop new policies around fake accounts and other areas as well.

Mr. DESAULNIER. Mr. Kane, maybe I didn't communicate this well, but the MIT report is more about you looking at behavioral trends and human factors. You make money off of—all of you, as I understand it, make money off of oftentimes when people are upset. You may not be doing that deliberately. So in this instance, you want to identify people who are spreading false rumors.

So the MIT study, as I read it, is looking at that larger tendency, that people like negative news. So the question was what can you do about that, not specifically as to individual cases but more globally.

Mr. KANE. Yes, sir. We are looking at developing four key indicators to help measure conversational health. You can measure the temperature of your body to gauge how healthy you are, but we want to try to better measure the health of the public conversation.

There are really four criteria: one is shared attention; two being shared reality; three being variety of opinions; and four being receptivity. So we are constantly working with the research community to help better gauge how we can modify our systems to support a healthy conversation.

Mr. DESAULNIER. Okay. I will just conclude. Thank you, Mr. Chairman, for the indulgence.

For me, as somebody who respects innovation and respects what you have done from a Bay Area perspective, all of us would agree that if history looks back and looks at these companies as contributing to the lack of trust in American democracy, that is a hell of a legacy we will all live with.

Mr. LYNCH. The gentleman yields.

Just using a little bit of traditional news time, I just want to clarify shadow banning. You basically ban someone but you don't let them know that you are banning them; right?

Mr. KANE. That is my understanding of the definition, and that is a practice that Twitter does not do.

Mr. LYNCH. So you shadow banned four Members of Congress?

Mr. KANE. No, sir. What occurred was in the auto-complete feature in Twitter, when you go to type in the name of an account that you want to see on Twitter, you had to click Search to actually search for the content. Certain accounts were not automatically suggested. You could easily find the accounts you were looking for by clicking Search.

Mr. LYNCH. But you couldn't find these four folks.

Mr. KANE. No, sir. You could by clicking Search.

Mr. MEADOWS. Mr. Chairman——

Mr. LYNCH. Go ahead.

Mr. MEADOWS. Mr. Kane, listen, this is not our first rodeo together. I assume you were——

Mr. LYNCH. I am going to recognize you for five minutes.

Mr. MEADOWS. All right. Thank you.

So, Mr. Kane, you are sworn in, right?

Mr. KANE. Yes, sir, I am.

Mr. MEADOWS. So when you found the fact that we were not auto-suggesting, as you would say, were we treated any different than the other Members of Congress at that point?

Mr. KANE. Sir, when we found the feature, we worked to immediately correct it.

Mr. MEADOWS. So you found it on your own?

Mr. KANE. Sir, I can't recall the exact source——

Mr. MEADOWS. You prepared for this. You knew I was going to be here. So how did you find the problem, Mr. Kane?

Mr. KANE. Sir, my work is focused on the integrity of the United States elections, and that is my primary——

Mr. MEADOWS. But you anticipated that you would have to answer this question today; didn't you, Mr. Kane?

Mr. KANE. Oh, absolutely. Certainly. Yes, sir.

Mr. MEADOWS. Okay. So when you did your research and you looked at this, at what point were four Members of Congress treated different than the other 531 Members of Congress?

Mr. KANE. Sir, when this was brought to our attention, it——

Mr. MEADOWS. How was it brought to your attention?

Mr. KANE. I believe it was a media article that——

Mr. MEADOWS. So you didn't find it on your own, because that is what you just told Mr. Jordan a few minutes ago, that you found it on your own, because you found it the same way I did, which was reading about it in Vice News. Didn't you find it that way?

Mr. KANE. Sir, I believe so, and that was my——

Mr. MEADOWS. Okay, but you didn't tell Mr. Jordan that. You indicated that you found it and fixed it in 24 hours.

Mr. KANE. Sir, that was certainly not my intent to indicate that at all. When it was brought to our attention, it was promptly fixed——

Mr. MEADOWS. Okay, and how was it brought to your attention? You raised your right hand.

Mr. KANE. Yes, sir.

Mr. MEADOWS. How was it brought to your attention?

Mr. KANE. Yes, sir. If I recall correctly, it was media reports. I am certainly happy to go back——

Mr. MEADOWS. So how long did it go on before the media reported it?

Mr. KANE. Sir, I am going to have to go back to our team to make sure we provide——

Mr. MEADOWS. So it is your sworn testimony that you don't know the answer to that question today?

Mr. KANE. Sir, that is correct. I don't have that specific information available.

Mr. MEADOWS. That is not the question I asked. When you found the problem, did you analyze how long it had been going on with Members of Congress? Did your Twitter team figure out how long it had been going on?

Mr. KANE. Sir, I am going to have to check with our team to make sure we give you a complete answer on that.

Mr. MEADOWS. All right. So let me go on a little bit further, then. If indeed this is the case, how often do you change your algorithms?

Mr. KANE. Sir, we are constantly working to improve our systems to support the conversational health, particularly in response to——

Mr. MEADOWS. How do you define what conversational health is?

Mr. KANE. Sir, as I indicated in the previous——

Mr. MEADOWS. I got those four things.

Mr. KANE. Yes, sir.

Mr. MEADOWS. Who is the determinant of that?

Mr. KANE. Sir, this is why we are working with outside researchers, to help us with——

Mr. MEADOWS. Because Mr. Galvin suggested that maybe you ought to be broken up. Listen, what you are finding is the wild, wild west, and I am all for the wild, wild west and freedom. But the minute that you start putting your hand on the scale of freedom and justice to tilt it one way or another, quite frankly, we have to act as Members of Congress. It may be two very different motives; but, Mr. Kane, let me just say this, is you know that four conservative members were treated differently with Twitter. Do you not know that?

Mr. KANE. Sir, I am well aware that four conservative members of the U.S. Congress did not have their accounts auto-completed.

Mr. MEADOWS. And so when did you fix the problem? What was the day?

Mr. KANE. I don't recall the exact date. I believe it was last May or June. I don't recall the exact day.

Mr. MEADOWS. All right. Can you get back with us?

Mr. KANE. Yes, sir, I can.

Mr. MEADOWS. Because—and you can let us know how long that practice had been going on?

Mr. KANE. Yes, sir. We will certainly do whatever we can to provide any additional information above and beyond what we had released publicly——

Mr. MEADOWS. That is not the question I asked.

Mr. KANE. Yes, sir.

Mr. MEADOWS. I said obviously if you have all these wonderful analytics that are going to find Russians, you can figure out how long——

Mr. KANE. Yes, sir.

Mr. MEADOWS [continuing]. the auto-populate for four Members of Congress——

Mr. KANE. Yes, sir. You have my commitment to work with you and your staff to make sure we provide a complete answer.

Mr. MEADOWS. All right. So here is the other thing that I want to go back to, Mr. Kane, because the problem that I have with this is the Chairman is talking about shadow banning, and you say that you don't do it. We don't know what you do and what you don't do; because, quite frankly, it took Vice News, who is normally no friend of conservatives, to actually report on this, and that is when we found out about it, that is when you say you found out about it.

Are you aware of any current Twitter employees or previous Twitter employees who have shared information with the public on how to affect the Twitter followers and engagement of people that are on Twitter?

Mr. KANE. Sir, as I sit here today, I have no knowledge of that.

Mr. MEADOWS. All right. Have you investigated that internally?

Mr. KANE. Sir, I have not. I am happy to——

Mr. MEADOWS. Has your team investigated it? You are here testifying for Twitter.

Mr. KANE. Yes, sir.

Mr. MEADOWS. So I assume you are speaking for Twitter as a whole——

Mr. KANE. Yes, sir.

Mr. MEADOWS [continuing]. not for Mr. Kane.

Mr. KANE. Yes, sir, and not that I am aware of, but I am happy to followup——

Mr. MEADOWS. So you haven't looked at whether you have actually either a current or previous employee has tried to manipulate information by allowing people to understand your algorithms maybe a little bit more intimately than a Member of Congress?

Mr. KANE. Sir, I have no knowledge of that, and that is why I want to make sure I followup with you, to provide a complete answer.

Mr. MEADOWS. Mr. Gleicher, let me come to you. You said earlier about you have an automated algorithm that will stop certain types of speech, and then you have individuals, I think, when I came in. Is that correct?

Mr. GLEICHER. Congressman, at the beginning what I was talking about, we have an automated system to detect and remove fake accounts, accounts that——

Mr. MEADOWS. Yes, but I am talking about content.

Mr. GLEICHER. If we are engaged with content and we do have algorithms that help surface content, and for certain specific types of content—for example, terrorist content—algorithms will take care of that——

Mr. MEADOWS. I get that. So let me go back. We are talking about free speech, campaigns, all that kind of stuff. Why would, on any of your platforms, why would Marsha Blackburn's campaign thing that had to do with a life issue have been banned, or at least withdrawn? Was that on Facebook?

Mr. GLEICHER. Congressman, in that context, we have humans that review when we are taking a content action. It depends a little bit on whether it is advertising or organic. But one of the things that we have seen very clearly is we are not going to be perfect. We make mistakes.

Mr. MEADOWS. Okay. But here is the thing. When you are taking down political campaign ads, every minute matters. And for you to have someone back there assuming—so you are admitting you made a mistake with Ms. Blackburn.

Mr. GLEICHER. We make mistakes, Congressman.

Mr. MEADOWS. You answered a question I didn't ask. Did you make a mistake by taking down now Senator Blackburn's ad? Did Facebook make a mistake? Yes or no?

Mr. GLEICHER. We did not, Congressman.

Mr. MEADOWS. Oh, so it is——

Mr. GLEICHER. We didn't take it down, Congressman. My apologies. I am not fully aware of the details of this specific incident.

Mr. MEADOWS. So when did it—if you didn't take it down, who did? Are you saying that your automated system took it down? Turn around and talk to your counsel so you can give me an honest answer, I guess.

Mr. GLEICHER. Thank you, Congressman.

I am not aware of us taking down an ad by Marsha Blackburn, from Marsha Blackburn's office, sir.

Mr. MEADOWS. All right. Will you go back and research that?

Mr. GLEICHER. Surely.

Mr. MEADOWS. They pick up on stuff that comes from the left, we pick up on stuff from the right, banning of Candace Owens, other people. When you do that, let me just tell you, the days of freelancing on this and having somebody stick their finger up and figure out whether they are going to take them, they are over, I am here to tell you. And even if it takes extreme measures, you have now collided with a bipartisan issue for different reasons, and we will make sure that we do that.

So actually, I guess, Mr. Kane, you should have spoken up. It was Twitter that took it down, wasn't it?

Mr. KANE. Yes, sir, and we publicly apologized for that.

Mr. MEADOWS. All right. So you made a mistake.

Mr. KANE. We did.

Mr. MEADOWS. So who made the decision to take it down?

Mr. KANE. I don't have the specific name of the individual.

Mr. MEADOWS. So you have individuals making determinations on political ads?

Mr. KANE. Yes, sir, we do.

Mr. MEADOWS. Okay. So let me just tell you—I will say the same to you. The days are over with, and you had better come up with a plan to this Chairman on how you are going to fix it, how you are going to stop Russians, how you are going to make sure that we are fair with all of this, because I can tell you it is a real problem.

I appreciate the gentleman's generosity with the clock.

Mr. LYNCH. The gentleman yields back.

The Chair now recognizes the gentleman from Arizona, Mr. Gosar, for five minutes.

Mr. GOSAR. Thank you, Mr. Chairman.

We are going to stay on the same topic, because as a business you have some responsibilities. So let's go into this.

An algorithm is only as good as the people that design it. Is that true, Mr. Kane?

Mr. KANE. I would agree with that assessment. Yes, sir.

Mr. GOSAR. How about you, Mr. Salgado?

Mr. SALGADO. I think that is essentially true.

Mr. GOSAR. How about you, Mr. Gleicher?

Mr. GLEICHER. I would agree.

Mr. GOSAR. Okay. So let me ask you a question. I want each one of you to describe the typical person creating an algorithm.

Mr. Gleicher, describe age, where they are at, mindset, background, education.

Mr. GLEICHER. Congressman, we have a pretty diverse team. The teams that work on our algorithms are based in cities around the world. I know engineers that——

Mr. GOSAR. Okay, so let me ask you a question. Young? Under 30?

Mr. GLEICHER. Congressman, I have worked with engineers that are quite young. I have worked with engineers that are older——

Mr. GOSAR. I am asking for a typical individual with algorithms. I am very aware of algorithms. I have a science background. I have a big math background, so I am very aware of this. So give me a typical portfolio of that person. Describe that person for me.

Mr. GLEICHER. I don't have a specific description for the sort of median individual who works on these, Congressman, but I would say I personally have worked with a number of our engineers, a wide range of our engineers, on some of the algorithmic work, and I see engineers that are older, younger, from a range of different backgrounds. Diversity is——

Mr. GOSAR. For the majority of them, they are younger.

Mr. GLEICHER. I can't speak to that, sir.

Mr. GOSAR. How about you, Mr. Kane?

Mr. KANE. Very similar to Facebook. We have a very diverse work force. We have engineers around the world. I don't have any specific data with regard to average age. I am more than happy to look into that and followup——

Mr. GOSAR. And education, I am looking for education too.

Mr. Salgado, how about you?

Mr. SALGADO. I am not aware of the demographics of the engineers who work on the algorithm.

Mr. GOSAR. Well, the reason I ask you that is that when you have something of this magnitude that is this influential, you want

to know that work force. You want to know the cross-sectional application.

So my question comes back to doesn't it bother you that this is a key component that you ought to be looking at, their political bias? Wouldn't you agree, Mr. Gleicher?

Mr. GLEICHER. Sorry. Could you restate the question?

Mr. GOSAR. Yes. This is that position that you ought to know that this person is unbiased. True?

Mr. GLEICHER. Congressman, I have found that everyone has some form of bias or unconscious bias.

Mr. GOSAR. Oh, there you go. Now, I am glad that you brought that up. Now that you know that everybody has an inherent bias, what is your correction factor? You were talking to Mr. Meadows in that regard. You couldn't give us how long it was because you didn't do the proper followup.

So let me ask you again. What does that background—what do you do to assert that there is no bias with those algorithm people?

Mr. GLEICHER. Thank you, Congressman. What I would say is the first step is we recognize that everyone walking into a system like this and building systems is going to have some bias. We try to build systems to manage that, exactly as you are saying.

Mr. GOSAR. What is your review process?

Mr. GLEICHER. A couple of things that we do. First, we have—we make all the guidelines that the algorithms are implementing public so people can see what the rules are and can understand when we take action and when we don't.

Second, we have an appeals process so that if we make mistakes, then they can be reviewed and we can take action to resolve them quickly.

And I would say the third, which is particularly important, is we have a wide range of partnerships, people that we work with and consult with on the consequences of algorithmic developments or other steps that we are taking, to make sure that we are understanding the consequences of what these steps might be.

Mr. GOSAR. Mr. Kane, do you want to address that?

Mr. KANE. Sir, very similar to our colleagues at Facebook. We are all human, but Twitter's purpose is to serve the public conversation, not just any particular segment of the conversation but the broader conversation.

Mr. GOSAR. I get it, we are all human. But once again, when the impetus is that this is a key position that has dramatic influence as to how and who is implicated by that, wouldn't you agree with me that this is a core part that you would really want to focus on?

So, for example, if I am a surgeon, to err is human, so I want to minimize my chances of error over and over and over again. So I surround myself with good people. I make sure that they are up to par on protocols. You should be doing the same thing. That is what I am getting at, and it seems like there is a failure here. So please keep describing what you are talking about.

Mr. KANE. Yes, sir. Our teams are consistently working to improve our product and make sure that it is, in fact, serving the public conversation. There are a number of actions that we take to constantly work this. I can say for every policy or product decision, going into the room I do not know who is a Democrat, who is a Re-

publican, who is an Independent. Those views don't matter when we are building and designing our systems.

We are here to support the public conversation. That is what we seek to do every day, and I am very proud of the work my colleagues do.

Mr. GOSAR. Well, once again, we saw a problem here. To me, having been alerted, if you had followed good business protocols here, you would have discovered this before being advised that it was happening. That is my process here.

Mr. Salgado, how about you?

Mr. SALGADO. It is similar for Google. There is no place for political bias in the algorithms, and we make sure that that is the case. So in addition to the 200-plus factors that go into our Search algorithm, for example, we also have raters who actually check actual Search results against guidelines of what we expect—the quality, the relevance, the authoritative Search ranking. Where we see a problem, we are able to adjust the algorithm. So it is a combination of good engineering with very discrete and detailed, nuanced Search algorithm components with human review and results, and as a result of this we make changes to the algorithm thousands of times in a year. So it is very carefully calibrated and changes with the times and with trends, and with the culture.

Mr. GOSAR. Would the Chairman indulge me for one last question?

So, for the last couple of Congresses—this is coming back to you, Mr. Galvin—I pushed legislation that would prohibit foreign nationals from cheating our system and would amend the Federal Election Act of 1971 to require the disclosure of the credit verification or the CVD and billing address for all online contributions. For those that still use cash, the CVD is that 3-digit code on the back of the credit card. As technology advances, we must continue to stay ahead of the curve, thwarting those who wish to inappropriately influence our political process.

Do you think this is a good recommendation?

Mr. GALVIN. I already said I think transparency is the goal here, whether it is the issues you have been speaking to with the social media or the election operations itself. Certainly when it comes to campaign contributions, that is clearly the case. The Chair of the FEC talked about dark money earlier before you were here in her testimony and her answers to questions.

So I think whatever perspective you are coming from, whatever part of the overall issue of conducting the election, both the campaign and the election itself, I think we need to have as much transparency as possible, and I think the Congress has a key role to play in providing that, because there is no other entity that is going to have a greater ability to look into and find out what is going on. No other entity could get all of the mix of players that you have had here today, the regulators, the government officials, the private officials together in a public forum. That has to continue. This can't be a one-time-only show.

Mr. GOSAR. Thank you.

Mr. Chairman, I really would like to see the answers as to that documentation on how, who, and what the overview is of all those who create the algorithms, please. Thank you.

Mr. LYNCH. If I understand the request from the gentleman from Arizona, you want them to substantiate in each of those instances where you said they need to go back. Any of the three of you, we expect answers in that regard.

Mr. KANE. Yes, sir.

Mr. LYNCH. Okay. So let me ask, we have had an opportunity to interview in various committees the Chief Operating Officer, Sheryl Sandberg with Facebook, and she said with respect to the Russian interference back in 2016 she admitted we were too slow to act on this, we should have seen it, we were slow to act on it. And then post-election reviews conducted by Twitter and Google, they had similar assessments. They reported that Russian activity was more widespread than previously known.

The actions of meaningful information-sharing between your companies and the intelligence community was problematic in that instance. In April 2019, former Facebook Chief Security Officer Alex Stamos also told a reporter, quote, "One of the biggest problems was a lack of cooperation between the public and the private sectors in 2016. It was nobody's job."

So, Secretary Galvin, do you ever hear from these folks? I mean, I know you got an assessment after 2016 that you weren't hacked successfully, and again in 2018 that was the assessment. But as far as regular communications in the run-up to elections, any——

Mr. GALVIN. No, my office has not.

Mr. LYNCH. Okay. How are things going in terms of information-sharing now, now that we have had these experiences in 2016 and 2018, with the intelligence community, and especially the FBI?

Mr. GLEICHER. Congressman, from our perspective I would just say that one of the really encouraging developments as we led into 2018 was the increased collaboration among industry with government and, quite frankly, with cybersecurity experts in civil society. In the 48 hours before the election, we in particular received a tip from law enforcement about a group of accounts that they believed were linked to Russian actors that we should look into. We took that information, we were able to run a six-hour investigation into it and remove it from the platform, which meant that the next day, literally on the eve of the vote, when Russian actors tried to trumpet those accounts, they had already been removed and the message had already been sent that government and the company were working together.

We also had some important instances where we worked closely with our colleagues here, including a recent take-down involving networks based in Iran where we actually worked with Twitter and both of us were able, because of the collaboration, to identify larger scopes of those networks and do a more aggressive take-down.

Mr. LYNCH. Mr. Kane?

Mr. KANE. I was just going to echo those sentiments. The relationship is very strong right now. We absolutely recognize the valuable partnerships that we have with the intelligence and law enforcement communities. It is strong now. We are looking at how can we improve those relationships moving forward in advance of 2020.

Mr. LYNCH. Mr. Salgado?

Mr. SALGADO. I concur with the statements of my colleagues here. We have very well-established routine information-sharing arrangements, security-to-security among the companies and with law enforcement, much more solid ground than we were on in 2016.

Mr. LYNCH. Okay. Let me go back to the instance where Mr. Meadows and Mr. Jordan, Mr. Gaetz and—who else?—Mr. Nunes were treated differently than others, their accounts. How did that happen? Explain it to me. Was this an algorithm that sort of swept them up, or were there individuals that actually identified their accounts and then altered them in some fashion?

Mr. KANE. Sir, we explained all this information publicly. But to summarize, what had occurred was for a number of the followers of these accounts that had been perhaps in violation of some rules in the past, that is what impacted that auto-search function. As soon as we realized the problem, again, we immediately fixed it within 24 hours. I was on the phone with the head of our product. Our CEO was certainly made aware, and we prioritized shipping a fix and explaining everything publicly very quickly, and that is exactly what we did.

Mr. LYNCH. Okay. But it was Vice News that picked it up; is that correct?

Mr. KANE. It is my understanding. Yes, sir.

Mr. LYNCH. That worries me. That worries me that—I mean, certainly, I probably didn't agree with anything that those members were——

Mr. MEADOWS. Oh, certainly not.

[Laughter.]

Mr. LYNCH. But still, it is free speech. Right now we have 257 million Americans with smart phones, and everyone is mobile right now. So the scale of what can happen if you make a mistake, as you conceded, is enormous. So that cannot happen, that cannot happen.

Mr. KANE. Yes, sir, I completely agree.

Mr. LYNCH. Yes, especially in the campaign context. That hurts our credibility as well. There are enough conspiracy theorists out there to damage the integrity just domestically, never mind foreign interference.

Let's see, I have a minute-and-a-half left.

So, changing algorithms or platforms can reduce visibility of some disinformation. But in the end, it is up to the user to believe or not believe a particular piece of content, and that was a report that we got from the Rand Corporation regarding the disinformation chain of Russian influence.

I know in Finland they are getting bombarded in their election from Russia because of the proximity there, and they are engaged in sort of an education program, starting in their grade schools, to basically, I guess, build resilience among their population, their people, their kids, so that they are much more judicious and selective and scrutinizing in terms of the social media information that they are confronted with.

Is there any—it seems to me very difficult to do something like that, but what are your thoughts on that?

Mr. KANE. Sir, media literacy is a vital component to fighting misinformation and disinformation online. Twitter partners with a number of media literacy groups worldwide. We believe it is absolutely essential, and we are absolutely committed to promoting media literacy, and anything that we can do to work with this committee to expand media literacy programs, we are certainly happy to do so.

Mr. LYNCH. I didn't know if it was something you were—this is your world, and I would look to you to come up with the ideas, not Congress. This is your world. You created some of this problem, so it would be good if we got some direction from you in terms of what would work best.

Mr. KANE. Yes, sir, and you have my commitment to do that.

Mr. LYNCH. Okay. I am going to yield to the gentleman.

Mr. MEADOWS. I thank the Chairman.

Just one followup question for the three of you.

CDA 230; do you think that is a good law?

Mr. GLEICHER. Congressman, from my perspective, CDA 230 gives us the space to be able to take action against hate speech and situations where content or activity on the platform might threaten the safety of users, and it also gives our users the space to debate and engage in the public discussion the way they would like. I think it is an important component of enabling the type of robust public discourse that we would like to see on our platforms.

Mr. MEADOWS. Mr. Kane, the same question.

Mr. KANE. I have the same identical answer as my colleague from Facebook. I completely agree with how he phrased it.

Mr. MEADOWS. Mr. Salgado?

Mr. SALGADO. Absolutely, it is essential to promote free speech.

Mr. MEADOWS. All right. I thank the gentleman for his courtesy. I yield back.

Mr. LYNCH. My pleasure.

I would like to thank our witnesses.

I see the gentleman from Tennessee, Mr. Cooper, has arrived, and I would yield—do you need a minute to gather your thoughts? Okay, you are good to go.

Mr. COOPER. Thank you, Mr. Chairman. I apologize for being late.

I am from a small state. There was a Twitter account that had 150,000 followers. It was listed early in the Mueller report. The account was called Tennessee—GOP. It was a Russian bot.

What are we to think of things like that? Have you no algorithms to expose that? It was eventually cleared out, but in August 2017, long after the damage had been done, and long after lots of prominent people had retweeted what was on that robot site. It wasn't just a bot, it was a Russian robot—IRA, St. Petersburg. We have our own little Petersburg in Tennessee, but it is a small country village. It is not a major Russian city.

So you said in your testimony that you get rid of deceptive stuff, and it all sounded good, but can you commit to getting rid of all the bots, all the deep fakes?

Mr. KANE. Yes, sir. With regard to malicious automation, as I mentioned, Twitter identified and challenged 425 million accounts in 2018 suspected of engaging in malicious automation. I note for

the first half of 2018, we identified and challenged approximately 232 million accounts. For the second half, that number went down to 194 million.

We also, in the first half of 2018, we had 3.6 million reports of suspected spam. That number went down to 3.1 million. So we had half-a-million fewer reports.

So what we are seeing is that we are doing a much better job at disrupting these networks. We are doing a much better job at disrupting them early during the sign-up process, and we continue to improve our machine learning to focus on the conversation on the platform and cleanup malicious automation.

Mr. COOPER. But you understand the different standard at work here. The billionaire founders of these companies, who should be rewarded for their amazing creativity, they don't keep their money in a bank that uses its best efforts to protect their wealth. They put their money in a bank that doesn't lose any of it, ever. Different standard, because they would be upset if just a few thousand dollars were missing. So there is a completely different standard here.

I know this is a new technology, and we have to adjust. But just think of your founders and how careful they are, and why can't we have a safer, better standard? Because this isn't a Democratic site that was hugely embarrassing. This was a Republican site. It doesn't matter which party it is. Bots should not influence elections, especially Russian bots.

Mr. KANE. I absolutely agree with you, and that is why we are also expanding our partnerships with both the RNC and the DNC and with Director Krebs' organization.

Mr. COOPER. In the business world there is bank security. There are things like guarantees, warranties, money-back refunds. We are not hearing any of that sort of certainty that most regular people are used to.

I would be happy to yield to the gentleman from North Carolina.

Mr. MEADOWS. Well, I think the gentleman makes a perfect point. We are talking about best efforts. Actually, you are bigger than most of the big banks.

Mr. COOPER. Completely.

Mr. MEADOWS. So there has to be some kind of punitive measure.

I yield back.

Mr. COOPER. A final thing. Is there a button I don't know about on Google where I can go back and get the default setting, like the original Search before it has been corrupted by all my prior searches? I know you can eliminate some history, but on the laptop there is a default button where you can go back to the factory settings. I would love brand-new, fresh, virginal Google.

I needed a black toilet for my house because it was built in the 1950's and they had a black toilet in there. For years afterwards, all I have been seeing are black toilet advertisements.

[Laughter.]

Mr. COOPER. This is wrong. We went ahead and got a white toilet. Why are we plagued with this? Why isn't there a default button?

Mr. MEADOWS. It was wrong from the beginning.

[Laughter.]

Mr. COOPER. I agree, but my wife picked the house. It wasn't me.
[Laughter.]

Mr. COOPER. People are so deeply offended by this, and it may seem trivial but just a simple button to say the original Google, that is the one I bought.

Mr. SALGADO. I will take that back as a feature request. As perhaps some IT Desk help here, I would suggest you clear your cookies on your laptop and you may no longer be served those ads. I am not sure that has anything to do with Google, but I am happy to take that suggestion back. Thank you.

Mr. LYNCH. Okay. In closing, I just want to say that if you listen to FBI Director Wray, he has said that looking at the data from 2018, the midterms, that he felt that the Russians and others were using that as sort of a prep or—I forget the term he used, but as a practice session for the big show in 2020 and that we should expect a major onslaught in the run-up to 2020.

If we go back to the banking analogy, if we were banks, I would ask them to do stress tests on their systems, and that is what I would like you to do. Is there a way that we can stress test what we might expect the activity might be in the run-up to the election in 2020 so that we have a certain comfort level with whether or not we are going to be able to defend the integrity of our electoral system?

My fear is that we will have a really close election and that the losing party will point to breaches or inconsistencies or hacks to disavow the results. We have seen that happen in other countries. Afghanistan is a good example. But there were millions of ballots that were falsified. But still, to this day, the dispute over that election undermines the credibility in some provinces of the sitting Prime Minister. I don't want us to be one of those countries in January 2021.

I want to thank you all. I know Secretary Galvin has a 7:30 flight, so whatever assistance I can give to get you to the airport on time. We appreciate all of your testimony, so I want to thank our witnesses for their testimony today.

Without objection, all members will have five legislative days within which to submit additional written questions for the witnesses, through the Chair, which will be forwarded to the witnesses for response. I ask our witnesses to please respond promptly, as you are able.

This hearing is now adjourned. Thank you.

[Whereupon, at 6:29 p.m., the subcommittee was adjourned.]