CYBER–SECURING THE VOTE: ENSURING THE INTEGRITY OF THE U.S. ELECTION SYSTEM

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JULY 24, 2018

Serial No. 115–111

Printed for the use of the Committee on Oversight and Government Reform

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

U.S. GOVERNMENT PUBLISHING OFFICE

33–089 PDF WASHINGTON : 2018

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

Trey Gowdy, South Carolina, *Chairman*

John J. Duncan, Jr., Tennessee
Darrell E. Issa, California
Jim Jordan, Ohio
Mark Sanford, South Carolina
Justin Amash, Michigan
Paul A. Gosar, Arizona
Scott DesJarlais, Tennessee
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Meadows, North Carolina
Ron DeSantis, Florida
Dennis A. Ross, Florida
Mark Walker, North Carolina
Rod Blum, Iowa
Jody B. Hice, Georgia
Steve Russell, Oklahoma
Glenn Grothman, Wisconsin
Will Hurd, Texas
Gary J. Palmer, Alabama
James Comer, Kentucky
Paul Mitchell, Michigan
Greg Gianforte, Montana
Michael Cloud, Texas

Elijah E. Cummings, Maryland, *Ranking Minority Member*
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
Robin L. Kelly, Illinois
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey
Raja Krishnamoorthi, Illinois
Jamie Raskin, Maryland
Jimmy Gomez, Maryland
Peter Welch, Vermont
Matt Cartwright, Pennsylvania
Mark DeSaulnier, California
Stacey E. Plaskett, Virgin Islands
John P. Sarbanes, Maryland

SHERIA CLARKE, *Staff Director*
WILLIAM MCKENNA, *General Counsel*
TROY STOCK, *Subcommittee Staff Director*
KILEY BIDELMAN, *Clerk*
DAVID RAPALLO, *Minority Staff Director*

CONTENTS

	Page
Hearing held on July 24, 2018	1

WITNESSES

The Honorable Christopher Krebs, Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security	
Oral Statement	6
Written Statement	9
The Honorable Thomas Hicks, Commissioner, U.S. Election Assistance Commission	
Oral Statement	14
Written Statement	17
The Honorable Maggie Toulouse Oliver, Secretary of State, New Mexico	
Oral Statement	22
Written Statement	24
The Honorable Ricky Hatch, County Auditor, Weber County, Utah	
Oral Statement	29
Written Statement	31

APPENDIX

Motion to Issue Subpoena to Dan Coats, offered by Mr. Connolly	88
Mr. Meadows Motion to Table the Connolly Motion Vote Sheet	90
Letter for the Record from 21 State Attorneys General, submitted by Ranking Member Cummings	91
Four Letters for the Record, submitted by Mr. Clay	96
Two Letters for the Record, submitted by Ms. Lawrence	105
Report from Capital Research Center, submitted by Mr. Palmer	116
Questions for the Record for Mr. Krebs, submitted by Ranking Member Cummings	132

CYBER–SECURING THE VOTE: ENSURING THE INTEGRITY OF THE U.S. ELECTION SYSTEM

Tuesday, July 24, 2018

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The committee met, pursuant to call, at 10:01 a.m., in Room 2154, Rayburn House Office Building, Hon. Trey Gowdy [chairman of the committee] presiding.

Present: Representatives Gowdy, Jordan, Sanford, Amash, Gosar, Foxx, Massie, Meadows, DeSantis, Ross, Walker, Blum, Hice, Grothman, Hurd, Palmer, Comer, Mitchell, Gianforte, Cloud, Cummings, Maloney, Norton, Clay, Lynch, Connolly, Lawrence, Watson Coleman, Krishnamoorthi, Raskin, Gomez, Welch, DeSaulnier, Plaskett, and Sarbanes.

Chairman GOWDY. Good morning. The Committee on Oversight and Government Reform will come to order.

Without objection, the presiding member is authorized is declare a recess at any time.

I recognize myself for an opening statement, and then the gentleman from Maryland, and then I'll recognize each of today's witnesses.

The right to vote is fundamental in a functioning democracy. In fact, the ability to pick our own leaders defines democracy. It's the essence of self-governing. Everything we do in Congress from any legislative body, every bill passed, every hearing conducted, every witness summoned, every document accessed, all of it derives its power and legitimacy from an election. So the legitimacy of what we do is inextricably intertwined with the legitimacy of the underlying election.

The power to vote is likewise contingent on that vote being counted, no more or no less than anyone else's. And the legitimacy to govern, therefore, flows from the reliability of the underlying election process.

Further adding to the uniqueness of this idea called "America" is the duality that elections are principally governed by and conducted by State and local officials and sometimes volunteers, even though many elections have decidedly national implications. The stakes are national; the threats are sophisticated and international. The process is State- and local-driven. But the States can and do ask for assistance, particularly given the nature of the attacks we now seem so face.

Today's hearing is focused generally on election security, on accepting and advancing our individual and collective belief that the

legitimacy of our work and the work of others in elective office is in direct proportion to the reliability of our own elections.

Today's hearing is broader than what happened in 2016, but what happened in 2016 must be addressed because the malefactors will attack us again.

I personally am convinced beyond any evidentiary burden that Russia interfered with the 2016 election. I'm convinced Russia attempted to undermine the fundamentals of our democracy, impugn the reliability of the 2016 election, and sow the seeds of discord among Americans.

Our intelligence community, both past and present, concluded this, as did the House Intelligence Committee report, as I am quite certain will the Senate Intelligence Committee report, and, equally importantly, as did our fellow Americans who served on the two grand juries which returned true bills.

Just 10 days ago, the current Deputy Attorney General announced Russians engaged in cyber operations to interfere in the 2016 Presidential election. They hacked into computer networks and installed malicious software that allowed them to spy on users, capture keystrokes, take screenshots, and exfiltrate and remove data from these computers. They also discussed the timing of the release in an attempt to enhance the impact on the election.

This was not just his opinion; it was the consensus of average, everyday Americans who were called into service on what we call a grand jury.

The Department of Justice said in both indictments, "There is no allegation that this inference changed the vote count or affected any election result," but that was likely not for a lack of trying. What better way to undermine confidence in every derivative function of government than to cast doubt on the election results as a whole?

Last week, many of us were in a SCIF, meeting with Inspector General Michael Horowitz. There were no cameras. It was just us and our colleagues from Judiciary. And my suspicion is all of us who were there left with a renewed understanding of what happened both in 2016 and even before that. We left even more fully cognizant that every election henceforth will be subject to attack, and, therefore, we must be prepared, not as partisans, but as fellow citizens.

Russia attacked many institutions in our country. Some were successfully attacked, like the DNC and the DCCC, but many others were targeted. And I'm sure my colleagues were struck, as I was last week again and am struck every time I have access to relevant information, by the reality that all of us are actually victims. Some were impacted more than others, but the target was America, which is why those aforementioned indictments allege the "United States of America versus." It's not a political party or a group or an individual; it's the "United States of America versus."

I am sure someone will correct me, as they are kind enough to do from time to time. I think it was none other than the Greek philosopher Solon who said—and I'll get this partially right—the place we want to live is a place where even those of us who are not victimized by crime, even those of us who are not injured, even those

of us who are not aggrieved feel the pain of the injustice just as if we were victims ourselves.

In 2016, it was one political party that was successfully accessed and materials disseminated. Those who seek to do us harm will be back at it again in 2018, perhaps with a different target. So we must take every precaution to safeguard our electoral process. And we're here today to explore ways to ensure no vote count is ever affected and discuss how to protect our entire election process from start to finish.

It is our responsibility to ensure no election is ever successfully interfered with. It is likewise our responsibility to ensure, when our fellow citizens place their ballot in the ballot box by whatever means, their vote is recorded accurately and counted correctly.

There will be efforts to affect us. There will be attacks. There will be efforts to sow the seeds of discord and discontent. And there will be efforts to call into question the legitimacy of our electoral process. But Americans are uniquely good at coming together in the aftermath of a tragedy or a loss or an attack, or at least we used to be. It's one of the most endearing and unifying qualities. The challenge is, can we come together even in an environment like the one we find ourselves in now and repel the attack before it happens?

Whether we win or lose, we need and want to have confidence every valid vote was counted and nothing interfered with the will of the American jury. Americans are free to quarrel about who should be elected. We will have a hard time sustaining this gift of self-governance that we have been given if we begin to quarrel about who actually was elected.

With that, I would recognize the gentleman from Maryland.

Mr. CUMMINGS. I want to first thank the chairman for this hearing.

And, as the chairman was talking, I could not help but feel chills, because one of the last things that my mother said, a 92-year-old woman who had fought for the vote and who had seen people lynched and harmed trying to get the vote, one of the last things she said on her dying bed is, "Don't let them take the vote away from us." Chilling.

And so this hearing means a lot to me personally, and I know it means a lot to every Member of this body. After all, we wouldn't be here if people did not have the right to vote. And so I dedicate these words to Ruth Elma Cummings.

I want to thank the chairman for calling this very important hearing. Candidly, however, it is not enough. It's not enough. It's not enough. Words are cheap.

This is the first time since Donald Trump was elected in 2016 that the Oversight Committee has held a full committee hearing on Russian interference in the election. It took us a year and a half to finally hold today's hearing.

This hearing comes less than 4 months—hello—4 months before the 2018 midterm elections. And most States have already held their primaries.

In addition, the chairman denied our request to invite the Office of the Director of National Intelligence to testify today. Congress

needs to understand how Russia attacked our States in order to help States defend against these attacks in the future.

And I'm so glad that the chairman acknowledged the fact that we are under constant attack. This ain't nothing new. And they are prepared to do it again and again and again. And they have probably learned some things from what they've done; they're going to do it even better and try to do it more effectively—that is, interfering with our elections—the next time.

Dan Coats, the Director of National Intelligence, recently warned that, and I quote—listen to what he said: "The warning lights are blinking red." He compared these warning signs to what we saw before 9/11.

Let me repeat that. President Trump's own Director of National Intelligence compared our situation now to the months leading up to the attacks of September 11th, 2001.

Yet Chairman Gowdy would not send an invitation to ask anyone from ODNI to testify. We understand that we may get a classified briefing at some later date, but a closed-door briefing is no substitute for a public hearing to inform the American people about what is going on. We have DHS here. We should have the intelligence community here as well.

We held a subcommittee hearing in November on election cybersecurity, but it was also inadequate. Mr. Krebs, who is here from DHS, also testified in November. At that hearing, we asked him for documents showing how Russia attacked our States, doing our duty as a check on the executive branch. At first, Mr. Krebs gave us only a single document. Later, he gave us 50 pages, much of which was already public.

Thank you very much.

We sent a letter asking Chairman Gowdy to subpoena the documents DHS is withholding, but he ignored it. We sent another letter asking him to let us vote on a subpoena, but he denied our motion.

Because this issue is so important, we joined with the ranking members of other key committees and sent a letter to Speaker Paul Ryan. We implored him to help us get from the Trump administration these documents about how Russia attacked our States. But all we got was silence. Silence. Radio silence.

It was not until Special Counsel Robert Mueller indicted 12 Russian military officials on July 13 that we finally learned something more about the specific attacks Russia had launched against our States. The Trump administration withheld this information from us.

We should not have been forced to read about it in a press release. DHS and other agencies should have provided that information months ago. Again, that is our job, to check the executive branch. We can't even get the information, both classified and unclassified.

So we have worked with States to help secure their election systems. It is clear that the House Republicans do not want information about Russia's attack on our States in the last election, which seems like a pretty basic first step, pretty basic, just getting the information, when you are trying to help these very States defend against Russian attacks in the next one.

But even worse, the House Republicans are taking active steps to hurt State efforts to protect their election systems. Just last week, House Republicans blocked all attempts to provide additional funding to secure State election systems. They argued that States do not need more money because they could cover these security upgrades on their own.

I have a letter here that we just received yesterday completely contradicting that Republican talking point. And I ask unanimous consent to make it a part of the official hearing record, Mr. Chairman.

Chairman GOWDY. Without objection.

Mr. CUMMINGS. This letter is from a bipartisan group of 21 State attorneys general, both Republican and Democrat. They expressed, and I quote, "grave concern over the threat to the integrity of the American election system," end of quote, and they asked for additional funding.

"We are concerned that many States lack the resources and tools they need to protect the polls. Additional funding for voting infrastructure will not only allow States to upgrade election systems but will also allow for a comprehensive security risk assessment."

Let me conclude with this. Some Republicans have recently begun to issue more critical statements about President Trump and Russia. Chairman Hurd wrote an op-ed in The New York Times asserting that our committee must conduct vigorous and public oversight. And this is his quote. Now, I didn't say this. Chairman Hurd said this.

"I believe that lawmakers must fulfill our oversight duty as well as keep the American people informed of the current danger. As a member of the House Oversight and Government Reform Committee, I strongly believe in the importance of Congress's oversight responsibilities and will work with my colleagues to ensure that the administration is taking the Russian threat seriously," end of quote.

I agree with every syllable Chairman Hurd wrote. I think he's telling the truth. But it would be much more powerful with action to back it up. We need all of our Republican colleagues to conduct oversight, not just use strong words.

Support our request to subpoena the Trump administration for documents it is withholding about the Russian attacks.

Support our request for the Director of National Intelligence to testify in public.

Vote in favor of additional funding for States that desperately need it.

We don't need talk; we need action. This should be a bipartisan issue. And, Mr. Chairman, you are absolutely right. This must be a bipartisan issue. This must be an issue where we put our party hats to the side. And we have less than 4 months to help our States before the next election.

And, with that, I yield back.

Chairman GOWDY. The gentleman yields back.

I'm pleased to introduce today's witnesses. I'll introduce you in group and then recognize you individually for your opening statements.

The Honorable Christopher Krebs, Under Secretary for National Protection and Programs at the U.S. Department of Homeland Security; the Honorable Thomas Hicks, Commissioner at the U.S. Election Assistance Commission; the Honorable Maggie Toulouse—I knew I'd get that wrong, so my apologies. It's my South Carolina upbringing. I think I'll just go with "Oliver" and not even try to pronounce it one more time—secretary of State from New Mexico; the Honorable Ricky Hatch, county auditor of Weber County, Utah.

Welcome. Pursuant to committee rules, I'm going to have to administer an oath, so I'd ask you to please stand and raise your right hand.

Do you solemnly swear or affirm the testimony you're about to give shall be the truth, the whole truth, and nothing but the truth, so help you God?

May the record reflect that all the witnesses answered in the affirmative.

You may sit down. There's a lighting system that will help you. You may rest assured that your opening statements are in the possession of every member and they will be read. So, to the extent you're able to summarize your remarks in 5 minutes, that would be great.

With that, Mr. Krebs, you are recognized.

WITNESS STATEMENTS

STATEMENT OF THE HON. CHRISTOPHER KREBS

Mr. KREBS. Thank you.

Chairman Gowdy, Ranking Member Cummings, and members of the committee, thank you for today's opportunity to testify regarding the Department of Homeland Security's ongoing efforts to assist State and local election officials, those who own and operate election systems, with improving the resilience of election security across America.

Today's hearing is timely, as primary elections are winding down and election officials have time to reflect and get ready for the November elections. In fact, less than 2 weeks ago, Secretary Nielsen and the DHS leadership team met with election officials as they gathered in Philadelphia for their summer conference.

Let me state plainly and clearly: The 2018 midterm elections remain a potential target for Russian cyber and influence operations.

As described in the 2017 intelligence community assessment, we know the Russians engaged in a multifaceted campaign to meddle in the last election, including some influence tactics that they have used for decades. Based on this prior demonstration of capability and intent, we are planning and preparing as if they'll try again this fall and beyond.

In terms of current activity, the intelligence community has observed continued malign influence operations into 2018. While these recent activities are designed to exacerbate sociopolitical divisions, there does not appear to be an effort at the same scope or scale directed at the midterms that was observed in 2016, nor have we seen Russian cyber operations directly targeting State and local election systems infrastructure.

Having said that, there is little doubt that some adversaries and nonstate actors view elections as a target for cyber and influence operations. Having been given a roadmap, we are certain some cyber actors are interested in identifying and potentially exploiting vulnerabilities in election systems, some driven by prior malicious actions and global dialogue about risks to election infrastructure.

Additionally, malicious cyber activity from various actors is regularly observed against U.S. infrastructure, including during the 2018 primary season, often common types of activity seen by many internet-connected systems.

Due to that threat landscape, we remain vigilant, and any attempt to undermine our democracy will be met with consequences. In the meantime, we will continue to work with our election partners to strengthen the resilience of our election systems.

As I've traveled across the country during primary season, it's clear to me that secretaries of State and other election officials are not sitting back. They take cybersecurity and security in general seriously.

Our mission at DHS is to help our stakeholders better understand and manage the risks they face through concerted efforts. In part by building relationships, establishing trust, and understanding what it is that our stakeholders need to manage their risk, we have made significant progress over the last year and a half.

With strong partnership with the Election Assistance Commission, we are working with State and local officials as well as those private-sector partners who support them. We have created government and private-sector councils, who collaboratively work to share information, promote best practices, and develop strategies to reduce risk to the Nation's election systems.

We have created the Election Infrastructure Information Sharing and Analysis Center, or EI–ISAC, with almost 1,000 members, including all 50 States. We are sponsoring security clearances for multiple election officials in each State. We have increased the availability and deployment of free technical assistance. And we have offered cybersecurity and physical security training and exercises. And, in fact, later this summer, we'll conduct a 3-day tabletop exercise with a number of election officials.

We'll continue to refine and update our suite of services as the requirements identified by our stakeholders mature. This will take time and a deliberate effort on both sides, as across the 50 States and 5 territories there are over 10,000 jurisdictions that are responsible for elections. The systems, processes, and procedures used vary greatly. What works for the voters of Florida likely does not work for the voters of California.

We are focused on engaging those many jurisdictions by each State and territory. This effort, known as our Last Mile Initiative, is focused on tailoring awareness of the threat, security mitigation best practices, and election security guidance checklist to the individual county or local level. We understand that the only way to deliver a resilient election system is to work collaboratively with those officials, including our partners at the EAC, as well as those on the front line running the process.

Before I conclude, I want to take a moment to thank Congress for legislative progress thus far in strengthening DHS's cybersecurity authorities. And we strongly support the passage of the Cybersecurity and Infrastructure Security Agency Act.

I look forward to further outlining our efforts to enhance the security of elections, our progress to date, and our strategy moving forward.

Thank you, and I look forward to your questions.

[Prepared statement of Mr. Krebs follows:]

Statement for the Record

The Honorable Christopher C. Krebs
Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security

FOR A HEARING ON

"Cyber-securing the Vote: Ensuring the Integrity of the U.S. Election System"

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

Tuesday, July 24, 2018

Washington, DC

Chairman Gowdy, Ranking Member Cummings, and members of the Committee, thank you for today's opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) ongoing efforts to assist with reducing and mitigating risks to our election infrastructure. DHS is eager to share with you the progress we have made to establish trust-based partnerships with our Nation's election officials who administer our democratic election processes.

Recognizing that the 2018 U.S. mid-term elections are a potential target for malicious cyber activity, DHS is committed to robust engagement with state and local election officials, as well as private sector entities, to assist them with defining their risk, and providing them with information and capabilities that enable them to better defend their infrastructure.

Given the foundational role that elections play in a free and democratic society, in January 2017 the Secretary of Homeland Security designated election infrastructure as a critical infrastructure subsector. Under our system of laws, federal elections are administered by state and local election officials in thousands of jurisdictions across the country. These officials manage election infrastructure and ensure its security and resilience on a day-to-day basis.

As such, DHS and our federal partners have formalized the prioritization of ***voluntary*** cybersecurity assistance for election infrastructure similar to that which is provided to a range of other critical infrastructure entities, such as financial institutions and electric utilities.

Since 2016, DHS's National Protection and Programs Directorate (NPPD) has convened Federal Government and election officials regularly to share cybersecurity risk information and to determine an effective means of assistance. The Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) has worked to establish goals and objectives, including plans for EIS engagement and the establishment of a sector-specific plan (SSP). GCC representatives include DHS, the Election Assistance Commission (EAC), and 24 state and local election officials. Participation in the council is entirely voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

The Department and the EAC worked with election industry representatives to launch an industry-led Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed council with leadership designated by the sector membership. The SCC serves as industry's principal entity for coordinating with the government on critical infrastructure security activities and issues related to sector-specific strategies, and policies. This collaboration is conducted under DHS's authority to provide a forum in which government and private sector entities can jointly engage in a broad spectrum of activities to coordinate critical infrastructure security and resilience efforts which is used in each of the critical infrastructure sectors established under Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*. The process is a well-tested mechanism across critical infrastructure sectors for sharing threat information among the Federal Government and critical infrastructure partners, advancing risk management efforts, and prioritizing services available to sector partners in a trusted environment.

NPPD also engages directly with election officials—coordinating requests for assistance, risk mitigation, information sharing, and incident coordination, resources, and services. In order to ensure a coordinated approach from the federal government, NPPD has convened stakeholders

from across the Federal Government through an Election Task Force. The task force serves to provide actionable information and offer assistance to assist election officials with strengthening their election infrastructure by reducing and mitigating cyber risk, and increasing resilience of their processes.

Within the context of today's hearing, I will address the unclassified assessment of malicious cyber operations directed against U.S. election infrastructure and our efforts to help enhance the security of elections that are administered by jurisdictions around the country.

Enhancing Security for Future Elections

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

DHS is committed to ensuring a coordinated response from DHS and its federal partners to plan for, prepare for, and mitigate risk to election infrastructure. We understand that working with election infrastructure stakeholders is essential to ensuring a more secure election. DHS and our stakeholders are increasing awareness of potential vulnerabilities and providing capabilities to enhance the security of U.S. election infrastructure as well as that of our democratic allies.

Election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections. In partnering with these officials through both new and ongoing engagements, DHS is working to provide value-added—yet voluntary—services to support their efforts to secure elections.

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

The National Cybersecurity and Communications Integration Center (NCCIC) works with the MS-ISAC to provide threat and vulnerability information to state and local officials. For nearly a decade, DHS has funded the Multi-State Information Sharing and Analysis Center (MS-ISAC), which has since created the EI-ISAC, to enable its members to share cybersecurity information and collaborate with each other. The EI-ISAC's membership includes almost 1,000

SLTT election-specific entities. Through the MS-ISAC, it has representatives co-located with the NCCIC to enable regular collaboration and access to information and services for state chief information officers.

Providing Technical Assistance and Sharing Information. NPPD actively promotes a range of services including:

Cyber hygiene service for Internet-facing systems: Through this automated, remote scan, NPPD may provide a report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the Internet, such as online voter registration systems, election night reporting systems, and other Internet-connected election management systems.

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

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

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

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

Classified information sharing: To most effectively share information with all of our partners—not just those with security clearances—we work with the intelligence community to rapidly declassify relevant intelligence or provide tearlines. While DHS prioritizes declassifying information to the extent possible, we also provide classified information to cleared stakeholders, as appropriate. DHS has been working with state chief election officials and additional election staff in each state to provide them with security clearances. By working with ODNI and the Federal Bureau of Investigation (FBI), in February 2018 election officials from each state received one-day read-ins for a classified threat briefing while they were in Washington, DC. This briefing demonstrated our commitment to ensuring election officials have the information they need to understand the threats they face.

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

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

DHS has made tremendous strides and is committed to working collaboratively with those on the front lines of administering our elections to secure election infrastructure from risks. The establishment of government and sector coordinating councils will build the foundations for this enduring partnership not only in 2018, but for future elections as well. We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure. However, we recognize that there are significant technology needs across SLTT governments, and State and local election systems, in particular. It will take significant and continual investment to ensure that election systems across the nation are upgraded and secure, with vulnerable systems retired. These efforts require a whole of government approach. The President and this Administration are committed to addressing these risks.

In closing, there is a fundamental link between public trust in our election infrastructure and the confidence the American public places in basic democratic functions. Ensuring the security of our electoral process is a vital national interest and one of our highest priorities. Our voting infrastructure is diverse, subject to local control, and has many checks and balances. As the threat environment evolves, we will continue to work with federal agencies, state and local partners, and private sector entities to enhance our understanding of the threat; and to make essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

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

Chairman GOWDY. Mr. Hicks?

STATEMENT OF THE HON. THOMAS HICKS

Mr. HICKS. Good morning, Chairman Gowdy, Ranking Member Cummings, and members of the committee. I am pleased to testify before you today to discuss the U.S. Election Assistance Commission's work to support State and local election leaders in their efforts to conduct efficient, accessible, and secure elections.

When Congress passed the Help America Vote Act of 2002, it established the EAC as an independent, bipartisan commission charged with developing guidance to help meet HAVA's requirements: adopting voluntary voting system guidelines and certifying election systems, serving as the national clearinghouse of information on election administration, as well as dispensing and auditing HAVA funds.

I am pleased to report that our capable team continues to fulfill this mission day-in and day-out, and election officials across the country constantly affirm our work does indeed help America vote.

The EAC is the only Federal entity focused solely on the administration of elections. We serve as the central hub for other Federal agencies that spend only part of their time working on this important issue, including those who specialize in technology and cybersecurity. Our partners, ranging from DHS and the FBI to the U.S. Postal Service and DOD, rely on the EAC to provide deep knowledge about how elections work and a clear line of communication to those in the field who administer the vote.

Election security is not new to those election officials or the tens of thousands of election administrative staff members and election workers who support that work. That said, you can see from this diagram it is not our only responsibility. The work described for the election officials encompasses everything from the ADA compliance and voter registration to election mail management and human resources. This is why it's so vital that Congress and Federal agencies, especially the EAC, provide election administrators with resources and tools they need to help succeed.

The establishment of election systems as part of the Nation's critical infrastructure was one way that the Federal Government sought to improve the mechanisms it uses to accomplish this goal. Following Former Secretary Johnson's critical infrastructure announcement, the EAC worked actively to provide State and local election officials with a voice at the table during discussions about how the sector would function.

DHS has often stated that the sector's Government Coordinating Council, the GCC, was formed faster than any other similar critical infrastructure sector council to date. And the EAC takes pride in its role we played to make that happen. It is proof of how State, local, and Federal governments can effectively worked together for a common goal of protecting our Nation's infrastructure.

I serve on the GCC's Executive Committee, which has worked diligently to ensure the "critical infrastructure" designation has tangible, meaningful impact across the Nation. But we all know that many of the solutions to security challenges take resources, and we're pleased that members of this committee and your congressional colleagues recognized this reality when supporting the

Consolidated Appropriations Act of 2018. That legislation contained $380 million in security funds for States and territories to improve the administration of Federal elections.

Just 4 months after the appropriation bill was signed into law, I'm proud to report that we have received disbursement requests for 100 percent of the funds. That demonstrates the EAC's responsiveness and the States' and territories' urgency in addressing ways to improve election systems.

Less than 2 weeks after President Trump signed the appropriation bill into law, the EAC personally notified each eligible jurisdiction and issued notice of grant award letters to every State and territory. Just 1 week after that, the first State, Missouri, requested funds.

In the weeks that followed, the EAC conducted a webcast public forum to explain the funds and worked directly with the National Association of Secretaries of State and the National Association of State Election Directors to share information. The EAC also conducted webinars, published FAQs and other resources on our website, educated nongovernmental groups, including those focused on issues such as accessibility and security about the funds. Our expert grants team has also helped States navigate logistical hurdles.

To date, we know that the States plan to spend the vast majority of this money, nearly 75 percent, on cyber protection, new voting equipment, updates of registration systems, and audits. These are all investments that reflect congressional guidance and priorities.

For those of you who have specific questions about how your State are investing those funds or programs overall, the EAC would be happen to establish a time to provide additional details about those plans.

The EAC has a broad spectrum of ongoing work to complement our vital role as the administrator of HAVA funds, including the testing and certification of election systems; creation of new resources related to a broad spectrum of election administration activities; production of new research; convening of public events that bring together election administrators, security experts, academics, Federal Government officials, and many others to discuss the approach of election systems to better serve American voters.

The Commission continues to release new resources, conducting training participation in a series of events, including initiatives focused on election security. Our staff was intricately involved in the establishment of Harvard University Belfer Center's tabletop exercise that is conducted across the Nation. And our own staff has traveled to nearly a dozen States to conduct election officials as IT management trainings for State and local election officials. These trainings are ongoing, and we work with DHS to put these trainings online.

While election administrators at the State level, which is yet another layer of security to protect the vote, those who administer elections are grateful for Federal support and use these resources to ensure the election systems are secure and resilient. The EAC appreciates congressional support of our efforts and your commitment to provide resources to the States and territories that we serve.

I look forward to providing additional details about the Commission's work and answering any and all of your questions.

Thank you.

[Prepared statement of Mr. Hicks follows:]

House Committee on Oversight and Government Reform Hearing:
"Cyber-securing the Vote: Ensuring the Integrity of the U.S. Election System"
July 24, 2018
Commissioner Thomas Hicks, Chair,
United States Election Assistance Commission (EAC)

Good morning Chairman Gowdy, Ranking Member Cummings, and members of the committee. I am pleased to appear before you today to offer testimony on the pressing issue of election security. In this 2018 election year, providing election security tools and resources to state and local officials is one of the Election Assistance Commission's most important responsibilities.

Election security is not new to the EAC, and it is not new to the state and local officials who run elections. Much is riding on the shoulders of state and local election officials. These officials work endlessly and tirelessly to deliver upon the high expectations our country has of them. The EAC Commissioners and staff are privileged to have the opportunity to support these faithful and conscientious public servants, who are perpetually focused on ensuring that the nation has secure elections.

As emphasized during the June 20, 2018, Senate Rules Committee hearing on election security, the EAC focuses solely on elections and that is of great value to election administrators. We have attached a diagram at the end of this testimony that demonstrates the broad spectrum of duties that require election administrators' awareness and management. Since election officials operate in each of these important and distinct areas, the EAC also works to provide support for each of these responsibilities.

Beyond this work, the EAC provides voters with vital resources and assistance needed to register to vote and cast their ballots. We also cultivate and maintain a national clearinghouse of election administration information that provides our partners in Congress and across federal government, state and local leaders, private industry, advocacy organizations, academia, and others in the elections industry with the information, research, and best practices that informs their own election-related work.

The EAC also works alongside federal partners to leverage their subject matter specific expertise to augment the EAC's whole-of-elections perspective with specialized products. Among our wide variety of federal partners are the Department of Defense (DOD), the Department of Homeland Security (DHS), the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), the National Institute of Standards and Technology (NIST), and the United States Postal Service (USPS). We collaborate with these agencies on a wide range of issues and work with their teams to inform new EAC products and initiatives, share timely information with election stakeholders, and ensure state and local election leaders are aware of available federal resources beyond those offered by the EAC. We also advise federal agencies on how their products can best meet the needs of election stakeholders.

Election security is one of the most integral components of the EAC's work. To this end, the EAC has continued to work diligently over the last 12 months to help states secure elections. The EAC has expeditiously and responsibly distributed the newly appropriated Help America Vote Act (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 distributed important best practices in election administration as we all look ahead to the 2018 midterm election and beyond. My testimony will provide more detail about each of these activities.

Distributing Newly Appropriated HAVA Funds

In the Consolidated Appropriations Act of 2018, Congress appropriated $380 million in HAVA funds to the states and eligible territories for projects and programs to improve the administration of federal elections. In just over 3 months, the EAC has received disbursement requests for 100% of the funds from all 55 eligible states and eligible territories, and 100% of the funds are available for the eligible states and territories to draw down. This is a remarkable development, and on behalf of the states, I thank you for appropriating these vital resources.

The EAC's work to distribute these HAVA funds reflects our strong commitment to providing the unparalleled support for state and local election administrators. The EAC issued Notice of Grant Award letters to each state less than two weeks after the bill was signed into law by President Trump. Within three weeks of the signing, Missouri became the first state to request its funds. In the subsequent 10 weeks, the EAC conducted a webcast public forum to explain how the funding would proceed, worked directly with the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED) to share information, conducted multiple webinars to further discuss how the funds may be used, consulted with members of the disability community to hear their views on use of the funds, and had frequent contact with each state in an effort to move the funds quickly.

In addition, the EAC website provides access to a set of Frequently Asked Questions regarding the funds, and this information has been updated on a near-daily basis since the law was enacted. The attached map, also available on the EAC website (www.eac.gov), now shows the amount of funds appropriated to each state and indicates that all of the affected 55 states and territories have submitted disbursement requests. The EAC has fulfilled its promise to get the funds to the states as quickly as possible, and the EAC is proactively consulting each of the states and territories on the proper use of the funds.

While several administrative issues have arisen in the funds disbursement process, the EAC's grants department is endeavoring to help the states navigate such issues so they may receive the funds in advance of the coming elections. For example, one roadblock states encountered was the ongoing government-wide issue with System for Awards Management (SAM) accounts. The EAC's grants department is working alongside our federal partners at the Government Services Administration (GSA) to provide additional support to the states' SAM account holders to get the funds properly distributed.

The funds are being disbursed with agreement by the states to provide a short narrative describing plans for how the funds will be used. Details from these documents will be shared with the entire election community and on the EAC's website, which is a primary portal for information sharing. As states and territories fine tune their own plans for how to invest the new HAVA funds, it is essential that they have access to the wealth of ideas and innovative approaches contained in other states' activities. The EAC's staff continues to work closely with

the states and territories and to compile the information we receive so that the election community and others have access to particulars of how the states and territories are expending their funds, including efforts to further update and secure their election systems.

Critical Infrastructure Activities

The distribution of HAVA funds is only the latest example of the EAC's work related to election security. The EAC has served as a central partner with DHS in ensuring the success of this national security effort, including joint efforts that took place well before the 2017 Critical Infrastructure designation by former Secretary Jeh Johnson. The DHS has stated that the election sector's Government Coordinating Council (GCC) was formed faster than any other similar critical infrastructure sector council to date. The EAC took an early leadership role in working toward this accomplishment, and we recognize it as an exemplary proof-point of how local, state, and federal governments can effectively work together toward the shared goal of protecting our nation's election infrastructure.

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

During and after the 2016 election cycle, the EAC was a key player in federal efforts to share vital security information with the states and educate our federal partners about ways to best serve the needs of election administrators. For example, the EAC:

- Distributed urgent security alerts and threat indicators from the DHS and the Federal Bureau of Investigation (FBI) to states and territories to help protect election systems from specific cybersecurity threats.
- Met on multiple occasions with staff from the DHS, the FBI, and the White House to discuss specific and nonspecific threats, state and local election system security and protocols, and the dynamics of the election system and its 8,000 plus jurisdictions nationwide.
- Served as the federal government's primary communication channel to provide real-time cybersecurity information to election officials around the country. This information included current data on cyber threats, tactics for protecting election systems against these threats, and the availability and value of DHS resources for protecting cyber-assets.
- Participated in and convened conference calls with federal officials, Secretaries of State and other State Chief Election Officials, state and local election administration officials, federal law enforcement, and federal agency personnel to discuss the prospect of designating elections as part of the nation's critical infrastructure. These discussions focused on topics such as coordinating security flashes from the FBI, the implications of a critical infrastructure designation, education on the nation's election system, and the dynamics of successfully communicating information to every level of election officials responsible for running the nation's election system.

- Provided DHS with perspective, information, and data related to the election system, introductions to officials in the election community, and information that assisted the agency with shaping communications in a manner that would be useful to the states and local election officials.
- Published a white paper entitled "U.S. Election Systems as Critical Infrastructure" that provided a basic understanding of critical infrastructure for election officials.
- Contributed to multiple foundational DHS documents used to structure the Elections Systems Critical Infrastructure designation and sector.

The EAC Chair serves on the GCC Executive Committee, and all EAC Commissioners are chartered members of the committee. Like many other members of the GCC, the EAC is seeking security clearances through the DHS. We have been assured that the department will address those requests soon.

In 2018, the EAC has focused on steps our commission could take to further serve election officials operating in the new threat environment. The EAC gathered election officials, security officials, academics, and federal government partners for an Election 2018 kick-off summit at the National Press Club in January. This event raised awareness of the security preparations election officials had underway and the resources available to the states and localities to help with this critical work. In April, the EAC held a live-streamed public forum expressly comprised of election officials to facilitate the sharing of security best practices among election colleagues.

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

The EAC also produced a video and supporting meeting materials to help local election officials explain the many levels of election security at their jurisdiction. The video was designed to be viewed at civic group meetings and election worker trainings. It can also be customized by jurisdictions, and some states are tailoring the video to their voters and processes. In addition, the EAC Commissioners continuously meet with state and local election officials at regional conferences across the country. These visits allow the Commissioners to apprise officials of best practices, promote resources available from the EAC and our federal partners, and discuss current concerns and topics in election administration, such as contingency planning, accessibility, voter registration, and technology management.

Testing and Certification/Voluntary Voting System Guidelines

The Help America Vote Act charges the EAC with administering a federal program for setting a voluntary national standard for testing and certificating voting systems. This testing standard is the EAC's Voluntary Voting System Guidelines (VVSG), and vendors may choose to have EAC-accredited and monitored labs test their voting systems against these guidelines for certification. The guidelines contain requirements for security, as well as other important

components—such as accessibility, usability, and interoperability. In fact, while security is a guiding consideration of certification, so is accessibility for voters with disabilities and voters with limited English proficiency. These considerations are deliberated and developed in public working groups under the direction of the EAC's Technical Guidelines Development Committee, which is chaired by the Director and Undersecretary of Commerce for Standards and Technology, currently Dr. Walter G. Copan.

The TGDC's membership is made up of technical and scientific experts from fields such as security, accessibility, voting machine production, and voting machine use. After development and approval by the TGDC, the voluntary guidelines are submitted to the EAC's Executive Director, provided to the EAC's Standards Board and the Board of Advisors, published for public comment, and presented to the EAC's Commissioners for consideration and approval. The EAC recently convened its advisory boards to review and comment on the adoption of the newest version of the voluntary guidelines, VVSG 2.0. Both Boards recommended that the EAC adopt VVSG 2.0. The EAC, however, is currently without its minimum number of three commissioners needed for a quorum to vote on the VVSG.

While the EAC has been hard at work on the newest version of the VVSG, the commission has not stopped its ongoing work to rigorously review, test, and certify voting systems. These reviews are referred to as test campaigns. In these campaigns, EAC accredited laboratories test vendor-submitted voting systems against the standard contained in the VVSG. Once a system successfully completes a test campaign, the results of the campaign are transmitted to the EAC's Executive Director for certification of the voting system to the standard against which it was tested. If the EAC's Executive Director agrees that the voting system has conformed with the standard, it is certified as such and assigned a certification number.

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

Conclusion

The EAC's mission includes supporting election officials across the country with the administration of federal elections so that they can help "Help America Vote." We endeavor to provide as much support and assistance as possible to the state and local election officials we serve. The importance of election security and how the newly appropriated HAVA Funds will assist states are primary agency focuses and top priorities. We are honored to support the important work carried out by election administrators each and every day. We welcome your feedback, and we look forward to answering questions you may have.

Chairman GOWDY. Ms. Toulouse Oliver?

STATEMENT OF THE HON. MAGGIE TOULOUSE OLIVER

Ms. TOULOUSE OLIVER. Good morning. Thank you, Chairman Gowdy, Ranking Member Cummings, and members of the committee, for the chance to appear before you today and address some of the things happening at the national level and some work specific to New Mexico and also to the National Association of Secretaries of State.

My name is Maggie Toulouse Oliver. I'm the New Mexico secretary of State. Prior to serving as secretary of State, I was county clerk in Bernalillo County, which is the Albuquerque metropolitan area. I ran elections in the largest jurisdiction in the State of New Mexico for 10 years.

I'm also the treasurer of the National Association of Secretaries of State, known as NASS, and a founding and current member of the Election Infrastructure Subsector Government Coordinating Council, the EIS GCC.

NASS is a nonprofit professional organization founded in 1904. The organization provides secretaries of State, chief election officials, and other public officials from across the United States with opportunities to share public policy ideas and best practices. This collaboration is important because it gives election officials access to information beyond what is available in our own States, helping us find innovative solutions to common election administration issues.

During the recent NASS summer conference held in Philadelphia, Pennsylvania, over 80 of our sessions, workshops, and discussions revolved around elections cybersecurity. Election officials like myself are taking the possible threat of foreign actors meddling in our elections very seriously.

In addition, during the conference, Department of Homeland Security Secretary Kirstjen Nielsen delivered remarks to members of NASS and to the National Association of State Election Directors, during which Secretary Nielsen emphasized the fact that election security is national security. She also highlighted the positive progress and working relationships between DHS and the States to protect elections infrastructure.

While State and local officials have always been focused on election security, the focus of our national organizations and the Federal Government has increased significantly since 2016. It is clear that election security will be a top priority for State, local, and Federal officials as well as the general public moving forward.

What is also clear is that the Federal Government and State and local election officials must keep the lines of communication open when it comes to election security and must continuously work together to harden our Nation's election systems.

Now to a little bit about my State. New Mexico is a leader in best practices, I am proud to say. We utilize paper ballots in all elections and have robust pre- and post-election testing, accuracy, and auditing processes, just to name a few. In fact, New Mexico was one of the first States in the Nation to conduct post-election audits.

Additionally, the vote tabulation systems that we use are never connected to the internet and include other important security mechanisms that reduce the ability for a bad actor to change votes. These practices are important election security safeguards that are now being adopted by States all across the country.

In regard to specific State preparations for 2018 and beyond, I would like to thank you and your colleagues for appropriating the remaining Help America Vote, HAVA, funds to States in the recent omnibus bill. According to the U.S. Election Assistance Commission, as of July 16th, 2018, all of the funds have been requested by the States and eligible U.S. territories, of course as we just heard from Mr. Hicks.

In New Mexico, we recently requested our portion of over $3.6 million in HAVA dollars from the U.S. Election Assistance Commission. We plan to use these funds to ensure that New Mexico's election systems continue to be resilient and secure.

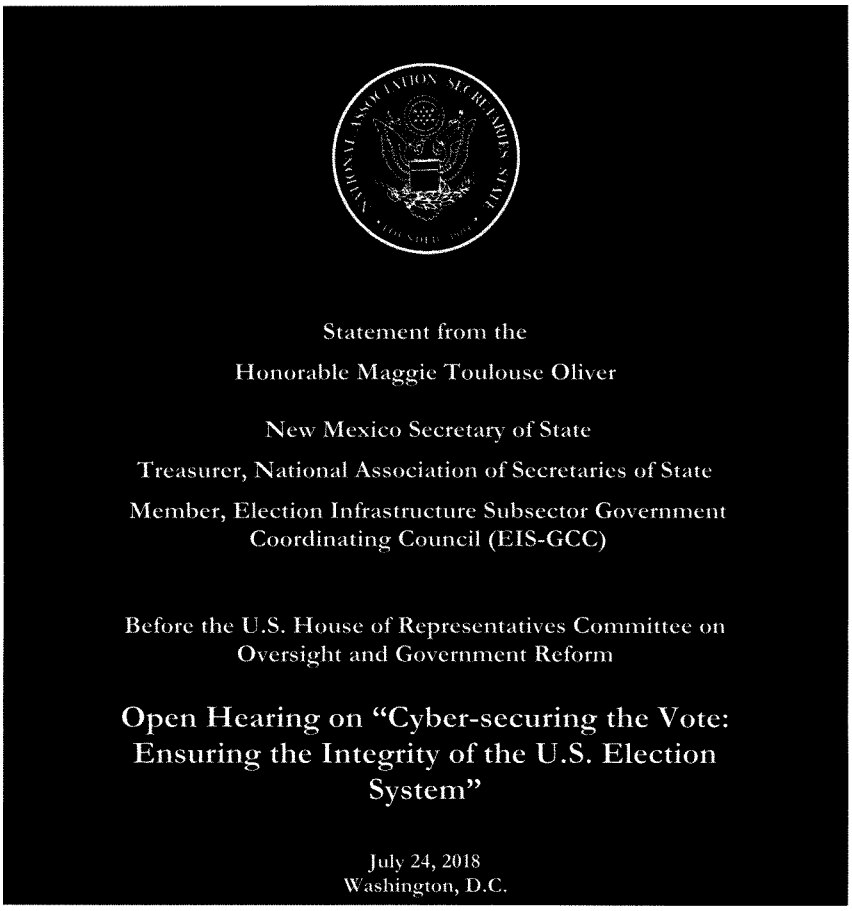
Some of the funds will be used to purchase more robust voting systems that provide for additional security features for our counties. We've also launched a brand-new election security program within our Bureau of Elections, with a portion of the HAVA funds earmarked to fund a full-time staff position to manage this program through 2023.

The program administrator will be responsible for implementing security best practices to safeguard New Mexico's sensitive election data and systems at the State and county level and to provide training and support to county clerks and their staff on cybersecurity issues. This is particularly important in New Mexico's smaller, more rural counties that may have limited technical support available to assist with security issues. We will also allocate some of the funds to assist counties with various system upgrades that they cannot afford on their own.

We are excited to have the opportunity to put this program into effect and appreciate the support of Congress and DHS in these efforts.

Thank you again, members of the committee and Mr. Chairman, for inviting me and my colleagues to testify before you and for giving me the opportunity to speak about this important matter on behalf of NASS and the State of New Mexico. I look forward to answering any questions you may have.

[prepared statement of Ms. Toulouse Oliver follows:]



Statement from the

Honorable Maggie Toulouse Oliver

New Mexico Secretary of State

Treasurer, National Association of Secretaries of State

Member, Election Infrastructure Subsector Government Coordinating Council (EIS-GCC)

Before the U.S. House of Representatives Committee on Oversight and Government Reform

Open Hearing on "Cyber-securing the Vote: Ensuring the Integrity of the U.S. Election System"

July 24, 2018
Washington, D.C.

National Association of Secretaries of State
444 North Capitol Street, NW – Suite 401
Washington, D.C. 20001
202-624-3525 Phone/202-624-3527 Fax
www.nass.org

My name is Maggie Toulouse Oliver, and I am the New Mexico Secretary of State. I am also the Treasurer of the nonpartisan National Association of Secretaries of State (NASS), and a founding member of the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC).

Thank you for the chance to appear before you today to address some of the things happening at the national level, some work specific to New Mexico and also with NASS.

The 2018 Primary elections across the country are well underway, with states administering elections in a secure, fair manner. Also, the General Election in November is less than 4 months away.

I. STATE AND FEDERAL PARTNERSHIP EFFORTS TO SECURE ELECTION INFRASTRUCTURE

During the NASS Summer Conference, held recently in Philadelphia, Pennsylvania, over 80 percent of our sessions, workshops and discussions revolved around elections cybersecurity. Election officials, like myself, are taking the possible threat of foreign actors meddling in our elections very seriously. In addition, during the conference Department of Homeland Security (DHS) Secretary Kirstjen Nielsen delivered remarks to members of NASS and the National Association of State Election Directors (NASED), during which Secretary Nielsen emphasized the fact that election security is national security. Also, Sec. Nielsen highlighted the positive progress and working relationships between DHS and the states to protect elections infrastructure. While state and local officials have always been focused on election security, the focus of our national organizations and the federal government has increased significantly since the summer of 2016. It is clear that election security will be a priority for state, local and federal officials as well as the general public moving forward.

State and local election officials and the federal government have worked diligently to create a productive relationship since former DHS Secretary Jeh Johnson announced the "critical infrastructure" designation for election systems in January 2017. As you may know, NASS and its members raised many questions and expressed serious concerns about the potential federal overreach into the administration of elections – a state and local government responsibility.

While we will remain vigilant about possible federal overreach, we have worked together to ensure that the "critical infrastructure" designation functions in a positive and effective way. Thus, we have chosen to actively focus on improving communication between the states and the federal government to achieve our shared goal of securing elections. In particular, we have utilized the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC), to open communications channels and guide future collaborative election security endeavors. At the EIS-GCC meeting on July 13, 2018, we approved a communications protocol document that my colleagues and I worked on for months. This document outlines the way that communications should flow between federal, state and local officials regarding threats, incidents, responses and recovery. It was some of our most important work to date and addresses the biggest challenge faced in 2016.

For instance, within the EIS-GCC's Subsector Specific Plan, which was also approved at our July 13th

meeting, there are many short and long-term goals and projects to support election officials, federal partners and stakeholders. These include deploying an online training environment for election officials, identifying resource gaps at the state level, and establishing a digital portal to increase communication between all levels. During our July 13th meeting, we also began important discussions with the Elections Infrastructure Sector Coordinating Council (EI-SCC). This is the Council representing the private sector and non-profit sector stakeholders that support election officials. I encourage members of this distinguished committee to call on the EI-SCC for more information on what is being done in the private sector to safeguard elections equipment and technology.

However, I would be remiss if I did not point out many of the organizations that have eagerly stepped up to help state and local governments with their election security efforts. NASS focuses a great deal on election security and our meetings are replete with shared practices from our colleagues around the country, along with presentations by security and auditing experts. We also hold forums twice a year for our office CIO/CISOs to come together to discuss challenges and solutions. The Belfer Center has developed a Tabletop Exercise that we can implement in our states to train both state and local election officials on addressing challenges leading up to and on Election Day. The Center for Internet Security has developed a handbook of election cybersecurity best practices and a checklist for states to monitor their progress. The Democracy Fund is supporting convenings of state and local officials to improve communication and governance between state agencies and between state and local governments. And private sector companies like Google and Cloudflare have stepped up to provide free resources to state and local governments to assist with preventing distributed denial-of-service (DDos) attacks and protecting our data and websites. The list truly goes on, but my time is limited.

II. STATE SPECIFIC EFFORTS TO SECURE 2018 AND 2020 ELECTIONS

In regards to specific state preparations for 2018 and beyond, I would like to thank you and your colleagues for appropriating the remaining Help America Vote Act (HAVA) funds to states in the recent omnibus bill. According to the U.S. Election Assistance Commission (EAC), as of July 16, 2018 all of the funds have been requested by the states and eligible U.S. territories. Election officials truly appreciate this money and it will go a long way in helping states strengthen and improve our elections systems. While our upgrades to equipment and cybersecurity improvements will be an ongoing challenge, and for many states the federal funding received will regrettably be insufficient to do all that they want and need, we are grateful for the boost these federal funds provide.

In New Mexico, we recently requested our portion of over $3.6 million in HAVA dollars from the U.S. Election Assistance Commission. We plan to use these funds to ensure that New Mexico's election systems continue to be resilient and secure. Some of the funds will be used to purchase more robust voting systems that provide for additional security features for our counties. We have also launched a brand-new Election Security Program within our Bureau of Elections with a portion of the HAVA funds earmarked to fund a full-time staff position to manage this program through 2023. The program administrator is responsible for implementing security best practices to safeguard New Mexico's sensitive election data and systems at the state and county level and to provide training, support and resources to county clerks and their staff on cybersecurity issues. This is particularly important in New Mexico's

smaller, more rural counties that may have limited technical support available to assist with security issues. We will also allocate some of the funds to assist counties with priority system upgrades that they cannot afford on their own.

In addition, some of the funds will be used to hire a Native American Election Liaison to assist with voter education and outreach in tribal communities which exist in one third of New Mexico's counties. Providing specialized outreach on voting procedures, voting rights, and voting technology all while addressing the unique language and cultural requirements of the voters living in these communities will work to make it easier for Native American voters to cast a ballot so we can finally close that gap in election participation.

New Mexico is a leader in election best practices. We utilize paper ballots in all elections and have robust pre- and post-election testing, accuracy and auditing processes just to name a few. These practices are important election security safeguards that are now being adopted by states all across the country. These enhancements are in addition to what we are already doing, including using a 100 percent paper ballot system that allows for votes to be recounted as needed to ensure the vote count is correct. We are also proud to be one of the first states to implement post-election risk limiting audits to ensure that the results of our elections are accurate. While my state has utilized these auditing processes since 2010, they are now being touted by election experts as essential to ensure voting systems are tallying accurately. Additionally, the vote tabulation systems that we use are never connected to the internet and include other important security mechanisms that reduce the ability for a bad actor to change votes.

A major component that is necessary to securing our elections is communication and collaboration across all levels of government. I am one of eight Secretaries of State serving on the EIS-GCC, which, as I said, has developed effective communication protocols between local, state and government officials on election security issues. I also served as the Co-Chair of the Elections Committee for the NASS, where the other committee members and I share best practices on protecting the integrity of every vote cast in our states.

I would be glad to elaborate during the question and answer portion of this hearing or anytime in the future.

III. THE FUTURE OF ELECTIONS AND VOTER CONFIDENCE

Much of the national attention over the past year and half has focused on election security issues – especially cybersecurity - which are of course, extremely important. If people are confident that the voting process is secure, they will be much more likely to participate. This is why we need members of this committee, DHS and our other federal partners to share with Americans that our elections are secure and indeed fair. The risks to our election system are real, and we have and will continue to address them appropriately. However, it is important to understand that those systems with the highest risk – online voter registration systems and election night reporting – are removed from the process of casting a ballot. If our protections to our voter registration system are breached, we can address that and the vote count is not impacted. If our protections election night reporting website are breached, we can address that

and the vote count is not impacted. Our voters' confidence may be impacted, and that is not insignificant, but they should be aware of the fact that the casting of a vote is separate from all these other parts of the system. While we all need to work together to combat misinformation – intentional and accidental - to maintain voter confidence, I also encourage those citizens watching today to get involved in the process by becoming a poll worker, reaching out to their state and local election officials with questions and ultimately voting in November.

In the meantime, please know that state election officials will continue to work to increase cybersecurity and run elections with the utmost integrity. The 2018 election will be a test on what we learned in 2016, but I feel that we are ready for 2018 and will continue to improve as time marches forward.

Thank you again Members of this Committee for inviting me and my peers to testify before this hearing and for giving me the opportunity to speak about this important matter on behalf of NASS and New Mexico.

I look forward to answering any questions you may have for me.

Chairman GOWDY. Thank you, Madam Secretary of State.
Mr. Hatch?

STATEMENT OF THE HON. RICKY HATCH

Mr. HATCH. Chairman Gowdy, Ranking Member Cummings, and members of the committee, thank you for the opportunity to testify this morning on how we can ensure the safety and security of our election system.

My name is Ricky Hatch, and I am the elected clerk auditor for Weber County, Utah. Today I'm here on behalf of the National Association of Counties, which represents all 3,069 county governments across the country.

In addition to running elections in my county, I serve as a NACo appointee to the Election Assistance Commission Board of Advisors, I am on the Government Coordinating Council for the Election Infrastructure Subsector, and I am the division director for election officials for the International Association of Government Officials.

As elections are the foundation of our democracy, election officials across the country embrace our duty to ensure that our elections are secure, fair, and trustworthy. All elections are local. And I'm here today to underscore the importance of including counties in Federal and State discussions to strengthen our national efforts to secure elections and also to offer suggestions to improve collaboration among all levels of government.

Counties play a key role in our Nation's election system and work with States to ensure the integrity of the process. In virtually every State, counties run the day-to-day operations of elections. There are almost 9,000 dedicated local election officials like me throughout the country who oversee the allocation of voting machines, manage polling locations, print and mail ballots, recruit and train poll workers, and ensure the integrity of the entire voting process. During the 2016 election, counties of all sizes managed over 100,000 polling locations and hired and trained over 800,000 poll workers.

But elections are not just a 1-day event for counties. From a cybersecurity standpoint alone, we work year-round to protect against direct hacking attempts that seek to improperly access voter rolls, remove election information from county websites, or alter voting data. We also work to protect voting machines, computers, and other equipment used to cast, record, tally, and certify votes. The integrity of the elections process is our main goal, and security is a key component of that goal.

Fortunately, coordination between the Federal Government and localities has improved dramatically in the past 18 months. These partnerships have been invaluable to help protect us from cybersecurity attacks. These include the establishment of the Government Coordinating Council by the Department of Homeland Security, which has been open and refreshingly responsive to our frank and frequent feedback during this process. They also include the $380 million in the 2018 omnibus. Many States, including my home State of Utah, are coordinating with their local governments on the best ways to use this funding. Throughout this whole proc-

ess, the EAC has been the glue in coordinating and promoting all of these new efforts.

While all of these are positive changes, we suggest three items to further improve our collective election security efforts.

First, we encourage Congress to support a dedicated, predictable Federal funding stream to help local governments protect elections. As you can imagine, resources often get stuck at the State level, which can be problematic for those of us on the ground. We upgrade aging equipment and shore up our defenses at great cost to county governments, which often do not have the luxury or ability to increase revenues to offset these costs. While the omnibus funding was helpful, we need more at the local level to combat these cyber threats.

Second, we recommend additional coordinated Federal and State outreach to local jurisdictions, especially those that are more remote and rural, as Ms. Oliver mentioned in her testimony. For a variety of reasons, such as limited staff, only a small percentage of local election officials are accessing the valuable free technical resources provided by our Federal partners. We urge our Federal and State partners to help us reach these jurisdictions.

And, finally, Congress and Federal agencies should undertake a robust federalism consultation process with States and local governments when considering any changes to election cybersecurity protocols. Local election officials have the most complete understanding of the elections process, and we want to share that understanding with lawmakers to help ensure that any Federal legislation or programs are fully effective on the ground.

Ultimately, the best way to safeguard our elections and shore up our cyber defenses is to communicate and work together. We stand ready to work with you, with Federal agencies, and with our States to strengthen our Nation's elections process and retain the public's confidence.

Chairman Gowdy and Ranking Member Cummings, thank you again for inviting me to testify today. And this concludes my testimony. I'm happy to take any questions.

[Prepared statement of Mr. Hatch follows:]

WRITTEN STATEMENT FOR THE RECORD

HON. RICKY HATCH
COUNTY CLERK/AUDITOR
WEBER COUNTY, UTAH

ON BEHALF OF THE NATIONAL ASSOCIATION OF COUNTIES

CYBER-SECURING THE VOTE: ENSURING THE INTEGRITY OF THE U.S. ELECTION SYSTEM

BEFORE THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

JULY 24, 2018
WASHINGTON, D.C.

Chairman Gowdy, Ranking Member Cummings and members of the committee, thank you for the opportunity to testify on "Cyber-Securing the Vote: Ensuring the Integrity of the U.S. Election System."

My name is Ricky Hatch and I currently serve as the elected Clerk Auditor for Weber County, Utah. Today, I am representing the National Association of Counties (NACo). In addition to my local responsibilities in Weber County, which include running elections, maintaining records and issuing marriage licenses, I am one of NACo's two appointees to the U.S. Election Assistance Commission (EAC) Board of Advisors. I also serve on the Government Coordinating Council (GCC) for the Election Infrastructure Subsector, which is jointly convened by the U.S. Department of Homeland Security (DHS), the EAC and the National Association of Secretaries of State (NASS). In addition to those roles, I am the Division Director for Election Officials for the International Association of Government Officials (iGO), an organization focusing on professional training and leadership development for county recorders, election officials, treasurers and clerks.

Elections are the basic foundation of our democracy, and ensuring they are secure, fair and trustworthy are the basic goals and responsibilities of every election official across the country. Because all elections are local, I am here today to reiterate the importance of including local governments, and especially counties, in federal and state discussions to strengthen our national efforts to secure elections.

About Weber County, Utah

While Weber County is considered "suburban" with our population of approximately 250,000 residents, we have a diverse mix of urban, suburban and rural components. Located north of Salt Lake City, we encompass 659 square miles around our county seat of Ogden, Utah. In the 2016 presidential elections, Weber County conducted the election partially by mail, and had ten different polling places with 60 poll workers. We saw a significant growth in our voting population with nearly 45,000 new and updated registrations for the election and an overall turnout of 67.3 percent.

About NACo

Founded in 1935, NACo is the only national organization that represents county governments in the United States and brings together county officials to advocate with a collective voice on national policy, exchange ideas, build new leadership skills, pursue transformational county solutions, enrich the public's understanding of county government and exercise exemplary leadership in public service.

About America's Counties

Counties are highly diverse, not only in my state of Utah, but across the nation, and vary immensely in natural resources, social and political systems, cultural, economic and structural circumstances, public health and environmental responsibilities. Counties range in area from 26 square miles (Arlington County, Virginia) to 87,860 square miles (North Slope Borough, Alaska). The population of counties varies from Loving County, Texas, with just under 100 residents, to Los Angeles County, California, which is home to close to ten million people. Of the nation's 3,069 counties, approximately 70 percent are

considered "rural," with populations of less than 50,000, and 50 percent of these counties have populations below 25,000. At the same time, there are more than 120 major urban counties, which collectively provide essential services – including administering elections – to more than 130 million people every day.

Many of the responsibilities of counties are mandated by both the states and federal government. While county responsibilities differ widely, most states give their counties significant authorities. These authorities include: administration of elections; construction and maintenance of roads, bridges and critical infrastructure; assessment of property taxes; record keeping; overseeing jails and court systems; and managing public hospitals and health systems. Counties are also responsible for child welfare, consumer protection, economic development, employment/workforce training, emergency management, land use planning, zoning and environmental protection.

Today, I hope to highlight the important role counties and other local jurisdictions play in administering and securing elections, examine ways we can further collaborate between different levels of government and share the following three suggestions for federal action:

1. **Enact a dedicated funding stream for local governments for election administration and security**
2. **Expand the federal government's efforts to provide technical assistance and best practices to local election officials**
3. **Engage in a robust federalism process with state and local stakeholders regarding any future legislative or regulatory changes**

Counties play a key role in our nation's election system and work in collaboration with states to ensure the security and integrity of the process.

The county role in elections complements the distinctly different role states generally play in the elections process. States are tasked with many administrative duties to ensure that elections run smoothly. The 2002 Help America Vote Act (HAVA) requires states to develop computerized, statewide voter registration lists, which counties use to administer elections at the local level. States continue to modernize voter registration through initiatives like online registration and automatic updates from motor vehicle departments. In addition to reducing the potential for voter fraud, the modernization of voter registration makes our elections more accessible to eligible citizens and reduces costs. As we have seen in recent elections, maintaining accurate lists is paramount to ensuring eligible and registered voters are not denied the opportunity to cast a ballot during an election.

In addition to voter registration databases, states may help administer elections by funneling or distributing information and resources from the federal government or working with local jurisdictions on voting equipment. In Maryland, for example, the State Board of Elections vets voting machines and helps deploy them, but mandates that counties pay for the equipment.

While states play an instrumental role in our nation's elections, counties and other local governments run elections on the ground. In almost every state, counties run the day-to-day operations of elections, and in every state, elections are broken down to local precincts for voting and administration. This means local governments are responsible for carrying out various key functions, from identifying polling places to printing ballots and protecting voting machines. The county official overseeing elections varies from state to state and may have one of several titles, including county clerk, county auditor or commissioner of elections. This official is responsible for overseeing the allocation of voting machines, managing polling locations, recruiting and training poll workers and ensuring the accessibility, integrity and efficiency of the voting process.

There are almost 9,000 dedicated local election officials throughout the country. During the 2016 election, counties supported over 100,000 polling locations and hired and trained over 800,000 poll workers. Counties of all sizes must undertake these tasks: according to data from the U.S. Election Assistance Commission (EAC), roughly 1,900 small counties reported having nearly 23,000 polling places in 2016 and over 130,000 poll workers. Counties with ten or fewer polling places had an average of 19 poll workers in 2016, while some of these small jurisdictions had as many as 100 volunteer poll workers. Meanwhile, only about seven percent of counties had 100 or more polling places, and these counties hired and trained over 400,000 poll workers.

County responsibilities for administering and securing elections begin well before Election Day and continue after votes are cast.

Before an election takes place

Prior to Election Day, county election officials have many responsibilities to ensure we are fully prepared for the election.

From a cybersecurity standpoint, we are most acutely concerned with "social engineering" hacking attempts, which include phishing and baiting attempts through email. Counties also protect against direct hacks to access voter rolls to alter data and attempts to remove election information from county websites. For example, according to Utah Lieutenant Governor Spencer Cox, the state of Utah faces about one billion "hacking attempts" every day. Most hacks are unsuccessful and crude attempts, akin to a burglar driving down a street looking for open windows or jiggling the locks, but it only takes one breach to cause significant problems.

Counties are also concerned with physical security measures prior to Election Day. We strategically place polling locations to ensure that they are accessible to voters and optimize the deployment of voting machines and poll workers, and to comply with federal and state requirements. Many counties enlist local law enforcement to conduct security sweeps of selected polling locations prior to Election Day. Counties also train poll workers to follow specific requirements regarding restrictions in and around polling locations.

Additionally, we vet, hire and train poll workers to ensure that they are well equipped to assist voters and protect against voter fraud or other security risks. Election officials also prepare for a wide range of "hard security" challenges at polling locations, including mitigating natural disasters and following protocols for an active shooter, fire, floods and other emergencies.

Election Day

On Election Day, election officials focus on ensuring the integrity of the voting systems themselves. These generally have four components: polling place management, voter verification and check-in systems (poll books and e-poll books), recording the vote using voting machines, ballot marking devices or paper ballots, and tabulating and reporting the results. Counties are meeting the unique security challenges presented by each of these components.

Through the Help America Vote Act of 2002 (HAVA), Congress sought to improve the election process by promoting the latest technology and moving away from traditional lever and punch-card machines. Today, approximately three out of every five counties use optical scan technology, which employs a scanner to read marked paper ballots and record the results. Two out of five counties use direct recording electronic (DRE) equipment that allows voters to make their selections via touch screen or other digital interface and records the results on a secure memory device.

Regardless of the type used, these voting machines are never connected to the internet or to each other. The transport and storage of voting machines, as well as ballots and vote tabulations, are directed by rigorous state and local security protocols. Voting machines are the voters' primary focus on Election Day, and though the type of machine each state or county uses varies, every state has specific policies governing voting machine setup. These controls include maintaining a verifiable chain of custody, pre-numbered tamper-evident seals, physical locks and documented reconciliations at the beginning, middle and end of Election Day.

After an election

Following Election Day, counties work with other municipalities and their state partners to certify the election results. This includes retaining vote counts and ballots, counting provisional ballots, verifying signatures and vote history, reconciling totals and preparing for a recount, if necessary. Additionally, many states and counties have implemented systems to "audit" the election results, including the security of the election. Each of these steps requires the retention and safeguarding of sensitive election information.

It takes time, resources, expertise and money to constantly combat these threats and ensure the public continues to place its faith in our electoral system. The cost of running elections is difficult to calculate and varies by county. According to the California Institute of Technology/ Massachusetts Institute of Technology Voting Technology Project, county election expenditures were an estimated $1 billion in 2000.

However, after HAVA was passed, substantial election reforms were implemented that included upgrading voting systems to ensure that voters could verify their selections before their ballot was cast. The need to continually upgrade voting machines to increase security and ensure accurate vote tabulations has increased the cost to run elections. The financial impact on counties varies depending on factors like how many voters vote by mail versus in person, how many machines are used in the county, the voting system vendor, state law requirements regarding the voting process, public expectations and many other factors. Costs, in addition to the actual equipment, can include transporting units to and from polling locations, the printing and mailing of paper ballots, poll worker pay, rent for polling locations, advertising, computers, other supplies and the annual maintenance of the machines.

Our main goal as county election officials is to ensure safe and efficient elections, and to maintain the public's trust in these elections. We know communication is one of the best ways to build trust within our communities, and counties are employing various strategies to meet this challenge. For example, Maricopa County, Arizona implemented a Community Relations Team (CRT) in 2017 to engage in proactive outreach activities to empower communities and help organizations register and educate voters. Similarly, Carroll County, Maryland developed an interactive website and an enhanced social media presence and offers regular opportunities to correspond with candidates and election judges.

President Dwight Eisenhower said, "Public confidence in the elective process is the foundation of public confidence in government." A voter's trust in the nation's elections process is driven by voter's experience with their local election office, whether they are registering to vote, receiving a ballot in the mail, using voting equipment at a polling place or checking out election results online. Local election officials are the face and voice of our nation's election infrastructure and drive the fundamental level of trust in each of our nation's elections. In fact, we are very detailed logistical planners, with backup plans for our backup plans. We're dedicated to the public trust and to doing things the right way, in full view of the public eye.

Locally-run elections have been a part of our country since its beginning. However, in the last two centuries, election administration has evolved as technology, opportunities and threats have all changed. While meeting these challenges and integrating new technologies, counties have continuously worked to preserve the integrity and security of America's elections, and we will continue to work to combat these new, sophisticated risks to election security.

A strong federal-state-local partnership is critical to securing our election systems.

Although the federal government, states, counties and other local jurisdictions have different roles in our election process, we must all work together to ensure the broader security of the election system. In any given election, we are only as secure as our weakest link: a failure in the chain at any point could cause major problems for the rest of the system. Since HAVA was implemented in 2002, intergovernmental coordination has gradually improved, especially in the last two years, but we need to keep improving.

A key part of this success was the formation of the U.S. Election Assistance Commissioner (EAC), which helps states and local governments in a variety of ways. Establishing the EAC was a landmark moment for collaboration on voting guidelines, auditing the use of election funds and establishing a national clearinghouse of information on election administration. Since 2002, the EAC has served as a reliable partner and information hub for counties as we compile information on best practices, vendor authentication and examples of how other counties and states are meeting challenges or needs.

Congress also boosted security efforts in the 2018 omnibus spending bill passed in March with the inclusion of $380 million in HAVA funds designated to improve election security. Many states are still determining how to prioritize the use of these extra funds. In Utah, we're using the funding to update and strengthen our statewide voter registration database software, buy more secure elections equipment and implement a more robust post-election audit process. We are also designating $300,000 of the funds to employ a new "cyber navigator" consulting program that will assist counties throughout the state with training on how to defend against and detect cyber-attacks, as well as how to recover if an attack occurs.

Additionally, the designation of election systems as critical infrastructure in 2017 under the U.S. Department of Homeland Security (DHS) catapulted the election community forward in its collaborative efforts. This led to the establishment of the Government Coordinating Council (GCC) in 2017, where the inclusion of local officials was well received. One third of GCC members are local government officials and they serve as an active and helpful addition to the conversation. In my experience, DHS has responded to feedback extremely well through the development of the GCC, pilot programs and during other discussions regarding election cybersecurity.

Furthermore, the focus on cyber-securing elections also led to the development of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) under the nonprofit Center for Internet Security (CIS), creating another central resource for election cybersecurity information that any local or state elections official can access. The EI-ISAC enables the quick dissemination of security alerts and best practices. Additionally, the completion of the CIS Handbook on Election Security earlier this year also gave many election offices a roadmap for both small and large steps we can take to further secure our systems.

This enhanced coordination is also occurring at the state level. Most states are proactively working with counties and other municipalities to determine the best use of the additional $380 million included in the FY 2018 omnibus package. Meanwhile, some states are pursuing other partnership opportunities. In Iowa, the Secretary of State's (SOS) office formed a Cybersecurity Working Group with representation from DHS, the Iowa Office of the Chief Information Officer (OCIO), the Iowa Air National Guard, county auditors (election officials) and county information technology directors. The Iowa SOS also held two cybersecurity workshops for county elections and IT staff in June, and counties have taken advantage of several resources that the Iowa OCIO has made available at no cost to counties, including Enterprise Vulnerability Management, Intrusion Detection, a Security Operations Center and other training courses.

Moreover, vendors and the private sector are also pitching in to augment our election cyber defenses. These partnerships are essential for counties of all sizes. Google's Project Shield and CloudFlare's Athenian Project both help safeguard election websites from distributed denial of service (DDOS) attacks, which would result in a severe loss of publicly available information about polling locations, times and access points. Google also helps with email services to deter some of the social engineering attacks I discussed earlier.

We are grateful that many of these conversations have included an increased opportunity for counties to be part of the intergovernmental process, but we still see opportunities for continued improvement.

We must do more to secure the 2018 elections and future election cycles.

Securing elections is not just a priority for 2018, nor is it necessary only for federal election cycles; it is a continuously changing landscape in constant need of attention, resources and interest. The more communication with county election officials, the better.

While some progress is being made, counties are taking it upon ourselves to shore up our defenses at great cost. As the voting machines purchased with HAVA funds age, counties are shouldering the burden of replacing these machines with new and updated technologies. For example, Tazewell County, Illinois – a mid-size county with a population of 150,000 – recently spent $700,000 on new voting machines, only a small portion of which will be reimbursed by state and federal resources. Counties are also doing this proactively, like Black Hawk County, Iowa, which purchased new voting machines in 2016 when the county was financially stable, rather than risking a future crisis.

Costs are not just confined to voting machines. Securing elections requires appropriate technological defenses and firewalls year-round. It also requires proper training for county staff and for volunteers and poll workers, hiring security before and during Election Day, safely transporting voting equipment and maintaining election information on the county website.

This growing number of demands comes at a time when counties – regardless of size – are experiencing significant fiscal constraints. In many cases, our capacity to fund compliance activities with state and federal mandates, or to update technology to meet growing security threats, is limited. In fact, 45 states curb counties' property tax authority and only 29 states authorize counties to collect sales taxes, albeit with restrictions. Given these constraints, ensuring that our elections are free and secure will take continued assistance from our federal and state governmental partners.

Therefore, to address existing election challenges and improve our collective security efforts, we respectfully offer the following suggestions:

1) **Counties support a dedicated, predictable federal funding stream to help local governments adequately secure elections, including upgrading and securing voting equipment.** Local governments fund most election investments, but much of our equipment is exceeding its useful

life. Compounding this problem are our efforts to keep up with technology changes and stay ahead of hackers.

While the omnibus and 2002 HAVA funding is a significant boost, often the resources get stuck at the state level. These dollars are needed at all levels, but they are especially vital at the county level with which voters interact the most. Furthermore, counties operate balanced budgets and approve future budgets up to two years before they are implemented, meaning uncertainty in the federal or state budgeting processes can leave counties unsure of if and when they will receive additional assistance.

The development of a reliable funding mechanism for local governments would allow all three levels of government to collaboratively target funding in areas of greatest need. These funds, when accompanied with training and expertise from our state and federal partners, will help local election officials properly implement cybersecurity tools and educate the public to ensure that public trust in the election process stays strong.

2) **Counties support continuing and expanding the federal government's efforts to provide technical assistance and best practices to local election officials.** In addition to funding, the federal government should continue to proactively work to distribute the available free resources to local elections officials. Only about nine percent of elections officials have joined the EI-ISAC to date, meaning the majority still lack access to proper information about the current risks they face and the appropriate resources that are available.

   Almost 80 percent of local election jurisdictions have fewer than 20,000 voters, and in many cases these small offices tend to be underfunded and are not staffed with cybersecurity experts. Therefore, a top priority for federal and state governments should be finding ways to involve these smaller jurisdictions and share already-available resources. As I mentioned earlier, a breach to even the smallest election office could have significant ramifications for the entire system.

   We urge the U.S Department of Homeland Security (DHS) to extend the availability of security clearances to local election officials, so that information can quickly flow between the entities most impacted by cyber threats.

   The federal government can also engage more directly with local election offices through trainings and sharing best practices. Each jurisdiction will have unique challenges. In some rural areas, a lack of broadband may prevent local election officials from engaging in enhanced technical training that is offered online. A "cyber navigator" program, like the one we are deploying in Utah, could help reach more remote offices. Urban areas also face challenges, where they must compete with the private sector in hiring and training cybersecurity staff as well as thousands of volunteer poll workers for every election.

3) **Finally, Congress and federal agencies should undertake a robust federalism consultation process with states and local governments when considering any other changes to election cybersecurity or administration protocols**. The development of the GCC, EI-ISAC and this hearing are clear examples of increased efforts from federal officials to include and communicate with local – and especially county – officials. We commend these efforts and encourage you to continue this trend.

In conclusion

Chairman Gowdy and Ranking Member Cummings, thank you again for inviting me to testify today. The most important way to guarantee we are working together to safeguard our elections is to ensure local officials – those running the elections on the ground – are included in the solutions. Inviting me to testify today is indicative of your commitment to including counties in these discussions, and I thank you both for your focus on this issue.

Our nation's counties stand ready to work with Congress, federal agencies and our states to ensure the 2018 election and any future elections are secure, fair and trustworthy.

Chairman GOWDY. Thank you very much.

Mr. CONNOLLY. Mr. Chairman?

Chairman GOWDY. For what purpose does the gentleman from Virginia seek recognition?

Mr. CONNOLLY. Mr. Chairman, I have a motion.

Chairman GOWDY. Reserving a point of order, the gentleman from Virginia is recognized for 5 minutes to state his motion.

Mr. CONNOLLY. I thank the chair.

Mr. Chairman, like so many of our colleagues on both sides of the aisle, I was very concerned by the President's statements last week in Helsinki about his 2-hour one-on-one meeting with Vladimir Putin.

President Trump capitulated to Mr. Putin on nearly every point of contention in the bilateral relationship with Russia. He publicly cast doubt on Russian interference in our election. He praised as an incredible offer an unprecedented proposal from Mr. Putin to hand over American officials, including the former U.S. Ambassador to Russia, for Russian interrogation. According to the Russians, President Trump even made agreements with Mr. Putin on Syria and Russian aggression in the Ukraine.

President Trump refused to allow his own senior staff to attend the meeting, and the President has so far declined to provide Congress or the public with any details about what occurred in that private meeting.

Our committee must act swiftly to determine what would cause President Trump to act in this way and to what extent President Trump is being manipulated by Mr. Putin. To do this, we must immediately hold a hearing with the Director of National Intelligence and others who can inform the committee and the public about the extent of the Russian threat to our country.

I'm joined in my concern by Subcommittee Chairman Mr. Hurd, who wrote an op-ed stating that he had seen Russian intelligence manipulate many people as a CIA undercover officer, but, he said, and I quote, "I never thought I would see the day when an American President would be one of them," unquote.

Mr. Hurd explained that our committee must work to, quote, "ensure that the administration is taking the Russian threat seriously," unquote, and "to fulfill our oversight duty and keep the American people informed of the current danger," he went on.

Even you, Mr. Chairman, said on "Fox News Sunday" that the evidence of Russia's attack on our country is overwhelming and that the President needs to say that and act like that. I couldn't agree more, Mr. Chairman.

In contrast, however, so far, the chair has declined our request to invite the Office of the Director of National Intelligence to testify during today's hearing on election security.

We appreciate your agreement to hold a classified briefing with ODNI, but we think the briefing, albeit helpful, needs to be accompanied by a public hearing. Closed-door briefings are simply not a substitute for public testimony from the top Federal intelligence official on how States were attacked by Russia in 2016 and the current threats to our election security.

Mr. Hurd again said, and I quote, "Lawmakers must fulfill our oversight duty as well as to keep the American people informed of

the current danger." Certainly, a public hearing would help accomplish that goal.

For all of these reasons, I hereby move to subpoena the Director of National Intelligence, Mr. Dan Coats, to testify in a public hearing before this committee and the public about the extent of the Russian threat involved.

I make this motion, Mr. Chairman, pursuant to House rule XI, clause 2(k)(6), and I believe the motion is in order. A written copy of my motion and the subpoena is at the clerk's desk. I ask that we dispose of this motion immediately.

Mr. CUMMINGS. I second the motion.

Would the gentleman yield?

Mr. CONNOLLY. Of course.

Mr. CUMMINGS. Mr. Chairman, I want to second the motion and associate myself with the eloquent words of Mr. Connolly.

As you know, I asked for you to invite a representative of the Office of the Director of National Intelligence to come testify here today next to DHS so that our committee members and the public could hear directly from the experts about the threat that Russia poses to our country and our electoral system.

Director Coats warned recently that, and I quote, "the warning lights are blinking red," end of quote. He compared these warning signs to what we saw before 9/11.

Our country is under attack, and we must understand that attack in order to protect ourselves. We must make sure that the public hears directly from Director Coats about the attack. We have to ring the alarm bell, and we need to ring it loud.

I know, Mr. Chairman, that you believe that Director Coats—because I have heard you say it. And just this past weekend, I heard a quote from you, and it says, quote, "The evidence is overwhelming. It can be proven beyond any evidentiary burden that Russia is not our friend and they tried to attack us in 2016." You said, going on, "The evidence is overwhelming, and the President needs to say that and act like it."

If I might just have unanimous consent for 1 more minute, Mr. Chairman.

But the simple fact is that the President is not saying that and he's not acting like that. And that makes it all more important that we here in Congress keep ringing that alarm bell and ringing it loud, that we make sure that the public understands that we hear clearly directly from the experts, that we make the evidence public, and that we put our money where our mouths are and fund the solutions.

Mr. Chairman, we should have Director Coats here testifying at this hearing today, but you did not invite him. And so I join my distinguished colleague, Mr. Connolly, in his motion to bring Director Coats before this committee on another day to testify about the threat that Russia poses to our national security and our electoral system.

And I want to thank the gentleman for yielding.

Chairman GOWDY. The gentleman from Maryland yields back to the gentleman from Virginia.

For what purpose does the gentleman from North Carolina seek recognition?

Mr. MEADOWS. Mr. Chairman, I move that we table the motion and, pending that, note the absence of a quorum.

Chairman GOWDY. The gentleman's correct. A quorum is not present.

The motion to table is made. And the motion to table and the underlying motion are held in abeyance until a sufficient quorum is present. Out of respect for our witnesses, I would suggest that we move on and proceed with the hearing until such time as that.

And, with that——

Mr. LYNCH. Mr. Chairman, may we be heard on the motion? I understand the abeyance and the lack of a quorum. But for the members that are here, I think it would help greatly if we were allowed to discuss the merits of the motion.

Chairman GOWDY. I do understand the gentleman's concern. Since the motion to table is made, I would ask my friend from Massachusetts, you're welcome to discuss it, but I want to vote on it later on, given the fact that the motion to table has been made and given the fact that we have our witnesses here. But I will be happy to give you a chance to speak on it at the appropriate time.

Mr. LYNCH. All right. Thank you. Thank you, Mr. Chairman.

Chairman GOWDY. With that, the gentleman from North Carolina is recognized for his 5 minutes of questioning, Mr. Walker.

Mr. WALKER. Thank you, Mr. Chairman, and thank our panel for being here today.

Just for record notice, Secretary of State, New Mexico, would you mind pronouncing that name one more time? I'm going to try here in just a second to get it right.

Ms. TOULOUSE OLIVER. Thank you, Mr. Chairman Member. It's Maggie Toulouse Oliver.

Mr. WALKER. Toulouse? Toulouse. All right. Okay. All right. When I come back around in a minute, we'll see if I can remember that, okay?

Mr. Hicks, I want to start with you, if that's possible. This past March, Congress appropriated $380 million in grants for State election security expenses that were intended to update voting equipment and improve cybersecurity practices overall.

Mr. Hicks, how much of these funds—or how many of these funds have been disbursed to States?

Mr. HICKS. All the money is going to be going to the States. So it's——

Mr. WALKER. Would you repeat that answer? Did you say all the money will be going to?

Mr. HICKS. Right. So about 335 million has been disbursed right now. But 100 percent of that money has been requested.

Mr. WALKER. And do you have a timeline as far as when the other $50 million or so would be?

Mr. HICKS. We should have that money out within the next couple of weeks.

Mr. WALKER. Okay. All right.

So, Secretary Toulouse Oliver and Mr. Hatch, how much did your State request, and how much have you received so far?

We'll start with the secretary of State.

Ms. TOULOUSE OLIVER. Mr. Chair—Mr. Walker, our State requested the full amount of $3.6 million to which we're entitled

based on population. We did request that full amount, and we have received that full amount.

Mr. WALKER. Okay.

Mr. Hatch?

Mr. HATCH. Utah requested the same full amount— or, not the same amount, but it came to about $4.1 million, $4.2 million.

Mr. WALKER. Okay. And have you received it as well?

Mr. HATCH. Yes. We received it last week.

Mr. WALKER. Okay. Good to hear.

Mr. Hicks, what election security priorities are the majority of States using these funds to pursue? Do you have any information?

Mr. HICKS. Yes, sir. Most of the States are looking to either do cybersecurity upgrades or purchase new voting equipment. About 75 percent of the money is going towards voter registration or cybersecurity or purchasing of new voting equipment.

Mr. WALKER. Okay.

Mr. Krebs, from your experience, what is the importance that the Federal Government plays in maintaining the integrity of elections? Can you zoom in a little bit and, taking maybe 30, 40 seconds at the most, give me an overview of what you see that role as?

Mr. KREBS. Yes. Thank you for the question.

So, as Secretary Nielsen has said several times, election security is national security. DHS plays a supporting role with the State and local officials, and it's important that we provide our cross-cutting cybersecurity expertise to help fill in some gaps at the State and local level, where they may not have in-depth cybersecurity expertise.

So where we can bring our broader learning throughout the critical infrastructure community, we can help at the local level.

Mr. WALKER. Let me follow up with that, if I could, please. What do you see, from your perspective, Congress's role in supporting States' and counties' electoral administration? Would you speak to that?

Mr. KREBS. Yes, sir. So it would continue to enable me to do my job in support of State and local, support the Election Assistance Commission, and provide, if necessary, additional support, including resources.

Mr. WALKER. Ms. Toulouse Oliver and Mr. Hatch, same question to you guys. What do you see Congress's role as, as far as assisting in this process?

Ms. TOULOUSE OLIVER. Mr. Chair Member Walker, I concur with Mr. Krebs: the continued provision of tools and resources for State and local jurisdictions to utilize, particularly as we get down the road with regard to our local entities.

For example, States utilize centralized statewide voter registration databases. So while I'm managing that and overseeing it from my office, it's being utilized by 33 counties across the State of New Mexico, some of which may not even have full-time IT staff. So it's really important that we are able to conduct risk assessments and provide the tools that have already been provided at the State level.

So we'll continue working with DHS, and we would love to have the assistance of Congress with regard to that.

Mr. WALKER. Okay.

Mr. Hatch, do you want to follow up with that?

Mr. HATCH. I agree with Secretary Oliver. The best way that the Federal Government can help is to provide assistance through resources, consulting, as well as dedicated and predictable funding so that we can identify, with our needs, how much we will be able to meet those needs financially.

Mr. WALKER. Yeah.

The first 2 years I was here, I served on Homeland Security. I was amazed at how many times, really on a daily basis, that there are attempts from the Russians and their cyber hacking. That's a nonstop. In fact, it was all the way back in 2012 when, I believe, a former Presidential candidate pointed out the concern as far as the geopolitical threat that Russia is.

Mr. Hicks, I have a question for you. What advise does the Election Assistance Commission, your area, provide the State and local officials when evaluating vendors for cybersecurity?

Mr. HICKS. Providing vendors? We operate under the Voluntary Voting System Guidelines. So that's a voluntary system. If a vendor wants to submit a system for certification, then we would give them guidance on that.

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

Chairman GOWDY. The gentlelady from New York is recognized.

Mrs. MALONEY. Thank you, Ranking Member, and thank you, Mr. Chairman, for calling this really vital, important hearing.

This past weekend, I went on a faith and politics pilgrimage—bipartisan, led Congressman Tom Reed—to upstate New York, the home of two of the vital human rights/social justice/civil rights movements in our country: the right to abolish slavery, the fight to abolish slavery, and the fight to grant women, half the population, the right to vote. And we went to the graves of Harriet Tubman, Frederick Douglass, Susan B. Anthony—all people that dedicated their lives to freedom and the right to vote for American citizens.

I cannot think of anything more important than this hearing. And I must say it is a national scandal that we have been asking for it ever since the election to find out what happened with the tampering, of trying to interfere and prevent people from having their vote.

The evidence is absolutely clear that the Russians tampered with our elections. Nothing is more important, and I hope, Mr. Chairman, this is the first of many hearings focusing on preserving the integrity of our votes and of our election system. I don't think anything is more important in our country.

And I'd like to start first by asking Mr. Krebs, have you read the indictment from Mr. Mueller, yes or no?

Mr. KREBS. Yes, ma'am. The most recent on the GRU officers? Yes, ma'am.

Mrs. MALONEY. In the indictment, the object of one of the Russian conspiracies was—and I'm quoting from the indictment—to hack into the computers of U.S. persons and entities involved in the 2016 Presidential election, steal documents from these computers, and stage releases of the stolen documents to interfere with the 2016 U.S. Presidential election.

Do you believe there is any reason to doubt this statement in this indictment, Mr. Krebs?

Mr. KREBS. No, ma'am.

Mrs. MALONEY. Okay.

Also, Mr. Krebs, the indictment goes on to say that in July 2016 the Russian spies, and I quote, hacked the website of a State board of elections and stole information related to approximately 500,000 U.S. voters, including names, addresses, partial Social Security numbers, dates of birth, and driver's license numbers.

Do you have any reason to doubt this information, Mr. Krebs?

Mr. KREBS. No, ma'am.

Mrs. MALONEY. And, also, the Russian spies, quote, hacked into the computers of U.S. vendors—not just voters, but the vendors—that supplied software used to verify voter registration information for the 2016 U.S. election.

Do you have any reason to doubt this information, Mr. Krebs?

Mr. KREBS. No, ma'am.

Mrs. MALONEY. And then, furthermore, the object of a second Russian conspiracy was, quote, again from the indictment, to hack into the protected computers of persons and entities charged with the administration of the 2016 U.S. election in order to access those computers and steal voter data and other information stored on those computers.

Do you have any reason to doubt this information?

Mr. KREBS. I do not.

Mrs. MALONEY. Okay.

I'd like to ask every member of the panel whether or not you doubt any of these informations.

Mr. Hicks, do you doubt this indictment in any way?

Mr. HICKS. No, ma'am.

Mrs. MALONEY. Ms. Oliver?

Ms. TOULOUSE OLIVER. No.

Mrs. MALONEY. And, Mr. Hatch, do you doubt this in any way, any of this information?

Mr. HATCH. No, ma'am.

Mrs. MALONEY. You know, now, many people have called this, including the President of the United States, a witch hunt just within the last few days.

Mr. Krebs, do you consider this a witch hunt, this data, this information?

Mr. KREBS. Ma'am, this is a duly authorized investigation, authorized and overseen by the Deputy Attorney General.

Mrs. MALONEY. And do you have any reason to doubt this information or to call it a witch hunt, Mr. Hicks?

Mr. HICKS. No, ma'am.

Mrs. MALONEY. Ms. Oliver?

Ms. TOULOUSE OLIVER. No, ma'am.

Mrs. MALONEY. And Mr. Hatch?

Mr. HATCH. No.

Mrs. MALONEY. Well, nobody, really. And I have no reason to doubt it either. And this President and administration and Congress need to take this threat seriously, and I would say this committee needs to take this threat seriously.

No fight was harder, nor more blood and suffering was shed in this country than the fight for liberty, independence, and the right to vote.

And I would like to give to the great State of New Mexico the last word, Ms. Oliver, on—I have just a few seconds left—your statement on this. How does your State feel about it? How do you feel about it?

Ms. TOULOUSE OLIVER. I'm deeply concerned, Mr. Chair Member Maloney, and that is why we are taking this so seriously and working so closely with our Federal partners.

Mrs. MALONEY. I thank you.

And I yield back.

Chairman GOWDY. The gentlelady yields back.

The gentleman from Michigan is recognized.

Mr. MITCHELL. Thank you, Mr. Chair.

We had a hearing—I'm concerned about some members of the committee talk about how there's been no hearings on this. With Mr. Hurd, we had a hearing on the 2016 election where we had a number of people from the elections folks come in and asked them very specifically, was there any evidence that the votes in the 2016 election were altered? We had multiple States there. Not one, not at Federal level reporting, not at the State level, indicated that votes were in any manner altered.

There is no quarrel that outside entities, including Russia, attempted to interfere with our election. Conflating the two gets in the way of doing the job we're trying to do here, which is to identify the resources we need to protect the integrity of that system. But I'm appalled at the ongoing conflating of those two, and suddenly the world has come to an end.

Let me ask you a question. Mr. Hicks, you're aware of the amounts of money put through to States to assist them with their elections. I've got Michigan's. Michigan requested—Michigan received $11.242 million to upgrade their systems. All of their voting machines will be replaced by the August primary, August 2018.

Have you received any further requests from Michigan for funding or support beyond that, sir?

Mr. HICKS. I am not aware of any funding—any other additional request from Michigan beyond the request from the——

Mr. MITCHELL. So Michigan has not raised a major crisis, that our election system in Michigan is suddenly about to come down around our ears at this point?

Mr. KREBS. I'm not aware.

Mr. MITCHELL. I've talked to secretary of State. Are you aware, sir, of the review of the State of Detroit's administration's 2016 general election?

Mr. KREBS. I am not.

Mr. MITCHELL. Let me give you some data on that. 392 precincts in the city of Detroit were out of balance. 26 percent of them, in terms of absentee ballot voting, could not be verified. One Detroit precinct was found to be missing over 250 ballots. They made six recommendations; all of them relate to training and staffing of the precincts. Not one, not a single recommendation related to either the voter registration file, electronic records, or the actual ballots, the actual voting. How are we going to support that given the fact

that despite the concerns of some of my colleagues have that the Russians are coming, the majority of the mistakes that are happening are human errors that just multiply, and they feel they've reconciled. The city of Detroit, if there was a recount in Michigan, by the way, the President won by like 12,000 votes, the city of Detroit could not a sustain an audit, they could not sustain a recount because of these problems. How do we support that?

Mr. KREBS. The EAC remains focused, laser-focused, on all aspects of elections, whether or not that's voter registration; whether or not that's equipment; whether or not that's poll worker training; whether or not that's election night reporting. There are about 8,000 jurisdictions across the country, and each jurisdiction has different aspects of it. And we try our best to help each and every one of those jurisdictions function well with the administration of elections through the Federal process.

Mr. MITCHELL. Do you have a current need for additional resources to support training personnel systems for voting, and what would that be?

Mr. KREBS. I don't have a specific number, but there's always need for additional resources. States are very tied to the fact that they have other things that they focus in on, whether or not that's roads, schools, police and so forth, elections is usually looked at as the last.

As Mr. Hatch talked about, there are additional ways that Congress can look at providing additional funding to the States.

Mr. MITCHELL. Okay. Ms. Oliver, let's switch because you're nodding your head. However we still want to maintain a system that, in fact, our elections are State and local, and not a Federal election system. I don't think you want to federalize it. Do you?

Ms. TOULOUSE OLIVER. No, sir. And speaking on behalf of NASS, the Secretaries of State naturally don't have a position on this issue. Speaking for myself personally, my experience in New Mexico, a State which has truly suffered ever since the economic decline, we can always use more funding. And I personally view conducting our Federal, State and local elections together on one ballot as a partnership. States have always had skin in the game on this issue. We've been doing all the election security work. We would love to have more resources in that regard, from my perspective.

Mr. MITCHELL. Has your group identified what those resources would be?

Ms. TOULOUSE OLIVER. Certainly we can provide you a list, but I agree with you, I think not only do we need to make sure we have the resources to protect in terms of cybersecurity, but we also—we have continuing and ongoing needs with regard to training.

Mr. MITCHELL. Sure.

Ms. TOULOUSE OLIVER. With regard to resourcing and other ways. So I'm happy to provide you any details you would like.

Mr. MITCHELL. I think any feedback you would have would be appreciated by the committee. We ask you to provide that. At this point in time, we haven't had any overwhelming requests. We certainly want to support that partnership.

I yield back. Thank you, Mr. Chairman.

Chairman GOWDY. The gentleman yields back. The gentlelady from the District of Columbia is recognized.

Ms. NORTON. Thank you very much, Mr. Chairman. It may not be enough, but it certainly is important to have this hearing.

And Mr. Krebs, before I ask a series of questions to clarify how the Russians got so proficient at what they do, can I ask you whether it is true, as I believe the President has implied, that the United States also engages in hacking or trying to get into the election systems of other countries.

Mr. KREBS. Ma'am, I have no information on that. My job is to help folks like Mr. Hatch and Secretary Toulouse to protect their system on a defensive Homeland Security, homeland defense operation.

Ms. NORTON. So you don't have any information that would indicate that the tit-for-tat kind of, as we do for example in spying, also goes on with respect to hacking into the election systems of other countries?

Mr. KREBS. Ma'am, I do not, in my—any official capacity, no, ma'am.

Mr. Krebs, you testified before the House Committee on Homeland Security, I'm interested because I want to know how the Russians got to be such experts at this. You used words I didn't understand, you said the Russians had, quote, "scanned" all 50 States.

Mr. KREBS. Yes, ma'am.

Ms. NORTON. I think you said 21, you were not able to see. What is scanning? What does it mean that they scanned all 50 States?

Mr. KREBS. Yes, ma'am, thank you for the question. So if I could back up a little bit. What we historically said dating back to last summer, was that we had based on network visibility, so it is sensors that were on state networks that were using DHS indicators of Russian activity, we were able to determine 21 States where scan—in some senses——

Ms. NORTON. You mean scanning, meaning what?

Mr. KREBS. So scanning can mean a number of things. I one sense, it could literally be a Russian officer getting on his computer in Moscow or elsewhere, and visiting a county or State system, just browsing, going through, whatever his research or search engine is of choice——

Ms. NORTON. Now, you saw 50—you say that they scanned 50, but you were able to see only 21. So why weren't you able to see—certainly we are going to have 50, but you have your own information on only 21?

Mr. KREBS. Yes, ma'am. So in my written, in my opening, I reference something called an Albert sensor. An Albert sensor is an intru—is a network intru—detection—it's an IDS, I'm sorry, intrusion detection system. What it does is does is it sits on a network and it looks for certain traffic IP addresses. So an actual internet-connected device somewhere else, trying to either come in or go out of that system.

Ms. NORTON. So you were able to see for 21 States, but not all 50.

Mr. KREBS. So we assume, because we only saw 21, and given the fact that we only saw 21, because that's where we had our Albert sensors deployed, we were able to see those 21. I did not have the visibility over the rest of the States.

Now, since February of this year, we have quadrupled our visibility. So when we come to 2018 in the midterms, ma'am, I suspect we'll have closer to all 50 States.

Ms. NORTON. So Albert sensors will be—used for all 50?

Mr. KREBS. Yes, ma'am. Thank Congress for that. That was in the fiscal year 2018 omnibus. We were provided additional funds to purchase——

Ms. NORTON. Was there anything that the Russians seemed to be more interested in, seem to be targeting more than other things? Were they just looking at the system to see what they could find? I mean, what—give us some information.

Mr. KREBS. I do believe that, to a certain extent, they were performing a reconnaissance. They were trying to figure out where they had landed, and what sort of functionality the systems had. And it's important to know that what they were able to see or scan, in one case, access a system of a voter registration database, that was all on the administration side. That was on the kind of information management side. It wasn't in the vote tallying or vote counting.

Ms. NORTON. So what do you think they ultimately want to do after scanning? What are they looking to do?

Mr. KREBS. It is hard to tell, based on their demonstrated capability. We do know that they attempted to interfere in the overarching election, that they intended to interfere in the election.

Ms. NORTON. And did so.

Thank you very much, Mr. Krebs.

Chairman GOWDY. The gentlelady from the District of Columbia yields back.

Before we recognize the gentleman from Georgia for his question, a quorum being present, the committee will resume consideration for the gentleman from North Carolina's motion to table. While the motion is not debatable, I did tell my friend from Massachusetts that he would have an opportunity to be heard. So I'm going to keep my word, and I'm going to ask unanimous consent, despite the fact that the motion is not debatable, that the gentleman from Massachusetts be recognized for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman. I do appreciate the courtesy that is being extended to me. I want to initially associate myself with much of the ranking member. He did correctly point out that it has been a long, long time, and I was at the hearing that Chairman Hurd had on the general issue of elections in this country, and that subsumed issues such as auditing and voter files and the other mechanics internally of our domestic elections. It did not precisely attempt to discern the level at which the Russians interfered with our—or attempted to interfere with our elections.

But I have to say that there is a wide gap between the opinions of many Members of Congress, both Democrat and Republican, regarding Russian interference, and opinions that I think are harmonized with our intelligence agencies that Russian interference did occur. And that's not what we hear coming out of the White House. And I greatly respect my friends on the other side of the aisle when they say they acknowledged it was—there was interference by the Russians. But they then talk for 10 seconds about that, and 4 minutes and 50 seconds about Detroit and how the vot-

ing files are inaccurate, and we need to train—train our election workers, that's not the point. If we had enough concern about Hillary's emails to do nine investigations in the House, and two in the Senate, and have hundreds of hearings on that issue, because we thought—a U.S. official mishandled their emails, hundreds of hearings, and we have two, when every single intelligence agency in this country tells us that the Russians hacked our election.

Two hearings, two hearings, that's it, after a year and a half. This used to be the Oversight Committee, this is the running away from oversight committee.

Since Trump took office, we do zero. I'm surprised we're having this hearing today. I'm shocked, because the Republican effort has been to rally around the President, even when he is wrong, even when he puts down publicly our intelligence agency, even when he disses us and sides with Putin.

Are you kidding me? Are you kidding me? This is where we are at now it? This is a disgrace, a disgrace. That was a national embarrassment in Helsinki. I was embarrassed that our President was siding against our intelligence agency and those people worked hard. You all work with them. You work with the NSA, you work with CIA. You know the good work that they do. And our President threw them under the bus in front of the world to side with Putin. You've got to be kidding me.

It's time to decide what you stand for. Do you stand for democracy, or are you stand with that gangster in Moscow? Do you stand for the right for your people to have a clean and honest election, or do you want to cozy up to the President, you don't want to make him look bad? I can understand when there's gray issues, but this is black and white, come on. I know there are colleagues on the other side of the aisle who feel the way that I do, and you're exasperated about this. But the time has come. On this issue, you can be a good Republican and still protect the electoral process in this country, you can do both. That's all I'm asking here. We can get at this, fix this problem, and you can still be a good and loyal Republican. It's not a question of either or. I know there are good men and women on your side. I know that. And you care deeply about this country.

I'm just saying on this issue, can we deal with the issue? Can we deal with it and fix it on both our behalves? Red States? Blue States? All Americans. That should be the goal here. We shouldn't let the President's quirks on this issue divide us, but to work on this problem as Americans. Thank you, I yield back.

Chairman GOWDY. The gentleman yields back. A quorum being present, the committee will resume consideration of the gentleman from North Carolina's motion to table. Those in favor will signify by say aye, aye.

All those in favor will signify by saying aye. Aye

Those opposed will signify by saying no.

While close, in the opinion of the chair, the ayes have it.

Motion from Virginia is laid upon the table.

Mr. CONNOLLY. Mr. Chairman, I would ask for a recorded vote.

Chairman GOWDY. The gentleman from Maryland and the gentleman from Virginia ask for a recorded vote. The clerk will call the roll.

The CLERK. Mr. Gowdy?
Chairman GOWDY. Yes.
The CLERK. Mr. Gowdy votes yes.
Mr. Duncan?
[No response.]
The CLERK. Mr. Issa?
[No response.]
The CLERK. Mr. Jordan?
Mr. JORDAN. Yes.
The CLERK. Mr. Jordan votes yes.
Mr. Sanford?
[No response.]
The CLERK. Mr. Amash?
[No response.]
The CLERK. Mr. Gosar?
Mr. GOSAR. Yes.
The CLERK. Mr. Gosar votes yes.
Mr. DesJarlais?
[No response.]
The CLERK. Ms. Foxx?
Ms. FOXX. Yes.
The CLERK. Ms. Foxx votes yes.
Mr. Massie?
Mr. MASSIE. Yes.
The CLERK. Mr. Massie votes yes.
Mr. Meadows?
Mr. MEADOWS. Yes.
The CLERK. Mr. Meadows votes yes.
Mr. DeSantis?
Mr. DESANTIS. Yes.
The CLERK. Mr. DeSantis votes yes.
Mr. Ross?
[No response.]
The CLERK. Mr. Walker?
Mr. WALKER. Yes.
The CLERK. Mr. Walker votes yes.
Mr. Blum?
Mr. BLUM. Aye.
The CLERK. Mr. Blum votes aye.
Mr. Hice?
Mr. HICE. Yes.
The CLERK. Mr. Hice votes yes.
Mr. Russell?
[No response.]
The CLERK. Mr. Grothman?
Mr. GROTHMAN. Yes.
The CLERK. Mr. Grothman votes yes.
Mr. Hurd?
Mr. HURD. Yes.
The CLERK. Mr. Hurd votes yes.
Mr. Palmer?
Mr. PALMER. Yes.
The CLERK. Mr. Palmer votes yes.
Mr. Comer?

Mr. COMER. Yes.
The CLERK. Mr. Comer votes yes.
Mr. Mitchell?
Mr. MITCHELL. Yes.
The CLERK. Mr. Mitchell votes yes.
Mr. Gianforte?
Mr. GIANFORTE. Yes.
The CLERK. Mr. Gianforte votes yes.
Mr. Cloud?
Mr. CLOUD. Yes.
The CLERK. Mr. Cloud votes yes.
Mr. Cummings?
Mr. CUMMINGS. No.
The CLERK. Mr. Cummings votes no.
Mrs. Maloney?
Mrs. MALONEY. No.
The CLERK. Mrs. Maloney votes no.
Ms. Norton?
Ms. NORTON. No.
The CLERK. Ms. Norton votes no.
Mr. Clay?
Mr. CLAY. No.
The CLERK. Mr. Clay votes no.
Mr. Lynch?
Mr. LYNCH. No.
The CLERK. Mr. Lynch votes no.
Mr. Cooper?
[No response.]
The CLERK. Mr. Connolly?
Mr. CONNOLLY. Nay.
The CLERK. Mr. Connolly votes no.
Ms. Kelly?
[No response.]
The CLERK. Mrs. Lawrence?
Mrs. LAWRENCE. No.
The CLERK. Mrs. Lawrence votes no.
Mrs. Watson Coleman?
Mrs. WATSON COLEMAN. No.
The CLERK. Mrs. Watson Coleman votes no.
Mr. Krishnamoorthi?
Mr. KRISHNAMOORTHI. No.
The CLERK. Mr. Krishnamoorthi votes no.
Mr. Raskin?
Mr. RASKIN. No.
The CLERK. Mr. Raskin votes no.
Mr. Gomez?
Mr. GOMEZ. No.
The CLERK. Mr. Gomez votes no.
Mr. Welch?
Mr. WELCH. No.
The CLERK. Mr. Welch votes no.
Mr. Cartwright?
[No response.]
The CLERK. Mr. DeSaulnier?

Mr. DESAULNIER. No.
The CLERK. Mr. DeSaulnier votes no.
Ms. Plaskett?
Ms. PLASKETT. No.
The CLERK. Ms. Plaskett votes no.
Mr. Sarbanes?
Mr. SARBANES. No.
The CLERK. Mr. Sarbanes votes no.
Chairman GOWDY. Have all members who wish to vote voted? The clerk will report the tally.
The CLERK. Mr. Chairman, on this vote there are 17 ayes and 15 noes.
Chairman GOWDY. The ayes have it, the motion is tabled.
The gentleman from Georgia is recognized for his 5 minutes of questions.
Mr. HICE. Thank you, Mr. Chairman. You know, I don't think anyone here denies the fact that Russia attempted to meddle in the elections. That it really is not the issue. They have done so in the past, they attempted in 2016. I don't have any reason to believe they won't attempt it again in 2018 what's coming up. I think what concerns me when we talk about the witch hunt, it involves over a year of an investigation by Mueller where not one bit of evidence has come forth that President Trump colluded with the Russians to try to influence the election. And, you know, when we're—Mr. Chairman, dealing with all this—this has been going on for a long time. Obama administration, this is way back as early as 2014 that they were meddling, and he did nothing about it.
So this is something that the issue of meddling is one thing, the issue of the President colluding is another, and that is indeed a witch hunt.
I want to go back to the topic here today, our whole election system involves States, not individual States. We've got over 8,000 jurisdictions, 110,000 different polling places throughout all 50 States, and for the most part, is a State issue, not the Federal Government. And I know in the omnibus that was passed in March, there was over merely $400 million that was granted for States to try to improve the security of the election infrastructure. One of the big concerns that comes along with those kinds of monies and funding is States and people know that as a general rule, wherever there is Federal funding, there is always strings attached to it, and as a result, States are leery of getting involved in accepting that kind of funds. I know in my home State of Georgia, that's certainly been an issue.
Mr. Krebs, I want to start with you. How has the Department of Homeland Security overcome these concerns of strings attached to some of the funding to try to help with election security?
Mr. KREBS. Thank you, sir. I can't speak specifically to any of the strings attached to the HAVA funding. And I defer to Mr. Hicks. But what we have done at DHS, working with the EAC, working with Secretary Toulouse Oliver, said, due to government coordinating counsel, we have worked to develop the set of guidance of investment guidance on things that State and local election officials can do to improve their cybersecurity. And that information is based on a range of factors, including some of the risk and vulner-

ability assessments that we've conducted over the last year or so on State networks and on election networks. And so what we've done across the 17 or so risk and vulnerability assessments, we've identified clear trends. There are a number of things that we are funding consistently across State networks, that frankly we are finding across any other IT system. And so, that's what bakes into the guidance and the recommendation, we are there to help from a technical perspective, help States implement that guidance.

Mr. HICE. Let me ask you this: I know that Georgia's secretary of State applied for a security clearance with DHS to try to access some of the shared classified threat information. Do you know whether or not that has been approved yet?

Mr. KREBS. So, sir, generally speaking, we don't discuss security clearance issues in public, due to the operation security nature that could make Secretary Kemp a target of foreign intelligence collection. I am happy to follow up off-line on that.

Mr. HICE. I would like to follow up on that, because, again, the integrity of State elections is at stake here.

Ms. Oliver, let me ask you, or Mr. Hatch, or whomever, regarding homeland security. How prepared are we, do you believe, going into this next election?

Ms. TOULOUSE OLIVER. Thank you for the question. I believe we always want to be more prepared. I feel fairly confident about where we are in New Mexico. I think Secretaries of State across the country and chief election officials are taking this issue very seriously. We are as prepared as we can be. And more important than prepared, we're also ready to be able to respond to any issues as they arise.

Mr. HATCH. I agree with Secretary Oliver. County election officials really have always had security, first and foremost, and not just cybersecurity, but physical security. So we were prepared. We were grateful for the additional funding and any additional resources provided by the DHS and EAC, as well as our States. It's a great partnership between the locals and the States. We enjoy sharing information and preparing together, and we feel confident. Of course, the attacks will come, and I wouldn't be surprised if there's a breach somewhere. It just happens with that many localities and that much attention. The key is to be prepared, and also to be resilient in the case of a breach.

Mr. HICE. Thank you very much. I yield back.

Chairman GOWDY. The gentleman yields back. The gentleman from Maryland is recognized.

Mr. CUMMINGS. Thank you very much, Mr. Chairman. I want to associate myself with the words of Mr. Lynch. In all my 21 years here in Congress, that has been one of the most moving statements I have heard in Congress. And I want to thank him for that statement.

Secretary Oliver, yesterday, a coalition of 21 State Attorneys General, both Republicans and Democrats, sent a letter to Congress that directly contradicts Republican claims that additional funding is not needed to help protect State election systems. The Attorneys General wrote, and I quote, "The undersigned Attorneys General's right to express our grave concern over the threat of the

integrity of the American election system," end of quote. I've heard your answers to other questions. But, have you seen that letter?

Ms. TOULOUSE OLIVER. Yes, sir, I have.

Mr. CUMMINGS. AGs also wrote "We are concerned that many States lack the resources and tools they need to protect the polls." I heard you say a little bit earlier that you all had gotten what you asked for based on a formula.Is that right?

Ms. TOULOUSE OLIVER. Yes, sir, that's correct.

Mr. CUMMINGS. Do you agree that the AGs that in many States, do not have the funding needed to protect their elections?

Ms. TOULOUSE OLIVER. So again, Mr. Ranking Member, I won't be speaking on behalf of NASS to answer this question, because we don't have a formal opinion as a group. But speaking on behalf of myself and my State, yes, I do strongly believe that ongoing funding is necessary, and that there's a consistent source of funding.

Election security is not a one-time issue, it's—you know, as has been mentioned multiple times today during this hearing, interference happened before 2016; it will continue to happen after 2016. I think 2016 really just brought a level of awareness to all of us about how serious the issue truly is.

And so, yes, I personally believe that elections are severely underfunded, particularly with regard to their significance. And so any additional help in terms of tools, resources and funding that the Federal Government can continue to provide is important. For example, this funding just provided through the omnibus bill wouldn't be enough to replace systems in a State that don't have paper ballot systems that are still using DRE machines, for example.

Mr. CUMMINGS. Well, you're going exactly where I was trying to get to. The AGs signed the letter that I just referred to and this is what they said, Ms. Oliver: "Additional funding for voting for infrastructure will not only allow States to upgrade election systems, but will also allow for a comprehensive security risk assessment. Unfortunately, past practice has shown that the existing Election Assistance Commission grants are simply insufficient to provide for the upgraded technology needed. More funding is essential to adequately equip States with the financial resource we need to safeguard our democracy and protect the data of voting members of our States," end of quote.

Secretary Oliver, do you agree with that statement?

Ms. TOULOUSE OLIVER. Again, speaking for myself personally.

Mr. CUMMINGS. You can speak for yourself.

Ms. TOULOUSE OLIVER. Yes, I agree.

Mr. CUMMINGS. And how would more funding help New Mexico conduct comprehensive risk assessment?

Ms. TOULOUSE OLIVER. For example, Mr. Ranking Member, right now, we have worked together with DHS to help conduct our State risk vul—vulnerability testing. What we don't have is a good sense of where each of our 33 counties in the State stand. I can tell you anecdotally, I think about four or five of our counties are in pretty good shape, but a giant question mark hangs over the rest.

So one of the things we want to do is do the same kind of vulnerability testing just to get a baseline to see where we are. If we continue to work with DHS in that process, which we would like to

do, it's probably going to take a while, because their resource are limited. If we were to try to contact with an outside entity that can do that privately, that's going to cost significantly more funds than we have available, even through this most recent grant. So these are the types of challenges that we are working within, Mr. Ranking Member.

Mr. CUMMINGS. The AG closed their letter with the following plea, and I quote, "the integrity of the Nation's voting infrastructure is that bipartisan issue and one that affects not only the national political landscape, but election, and State, county and municipal local levels.

It is our hope that you agree and will take swift action to protect our national legacy of fair and free elections," end of quote.

Mr. Krebs, last week Republicans refused, on the House floor, to approve another dime for States to protect their election systems. What is the Trump administration's official policy on this specific question? And do you support additional funding for State election systems or not?

Mr. KREBS. Sir, thank you for the question. In terms of additional funding, there certainly has been laid out both in the Attorney General letter, as well as Secretary Toulouse Oliver and Mr. Hatch have laid out. There is a requirement to update systems across the board, that is going to take money. Whether that comes from the State or the Federal Government, I don't have an official opinion on that. It is going to take money. We are going to have to identify where the risk is. And we're going to have to focus money on that risk.

As Secretary Toulouse Oliver said, there are still five States that have equipment that does not have a voter-verifiable paper trial. From a risk management perspective, that is where I would prefer that we focus resources and assets.

Mr. CUMMINGS. As I close, I hope my Republican colleagues will reverse the opposition and join us in helping these States. These 21 AGs are from States many of you represent: North Carolina, Michigan, California. Let me close by reading just one more quote from their letter. "It is imperative that we protect the integrity of our elections. We must ensure that the upcoming 2018 midterm elections are secure and untainted. Accordingly, we ask for your assistance, in shoring up our systems, so that we may protect elections from foreign attacks and interference."

Let me ask you this: Do you agree with that, Mr. Krebs?

Mr. KREBS. Sir, I'll tell you what, if you could repeat that.

Mr. CUMMINGS. Oh, no, no, I'm not going to repeat it. But basically what—what they are saying is, is that we want to make sure that our electoral system is protected and that people will know that their votes are going to be counted and that the process is untainted. And I would guess that is consistent with what you are in office for.

Mr. KREBS. Yes, sir. And that's why it's important that we are having this hearing right now, so the American people can hear about the efforts that DHS is leading, the Election System Commission is leading, that State secretaries are leading. This is a partnership that is working right now. We are improving security

practices across the electoral system in this Nation at great pace. There is a lot of work to do. This is a marathon, this is not a——

Mr. CUMMINGS. Well, speaking of a marathon, Mr. Hicks has said, you listed a number of things that you all look at. The one thing I notice that you did not mention is voter suppression. Do you all look at voter suppression, because that is a booger bear.

Mr. KREBS. That is not one of the functions of——

Mr. CUMMINGS. Okay. So that's why you didn't list it?

Mr. KREBS. Correct.

Mr. CUMMINGS. All right. Thank you.

Chairman GOWDY. The gentleman from Florida is recognized.

Mr. DESANTIS. Thank you, Mr. Chairman. I thank the witnesses.

Mr. Secretary, for the 2016 election, was there any cyber activity that influenced any of the vote totals in any jurisdiction, to your knowledge?

Mr. KREBS. So very specifically, drilling down to the cyber enabled hacking, we'll call it, of State election systems, we do not have information or evidence to suggest they had access to vote tallying systems. And that's why I made that distinction earlier; there is the administration piece, and then there is the vote tabulation and counting side.

Mr. DESANTIS. So—and the other stuff is obviously is still important. In fact, with the registration, like a registration database, if that were to be compromised, how would that have a negative effect? What would be the problem?

Mr. KREBS. On the specifics, we defer to Secretary Toulouse Oliver, but the way I see it, the way the Nation's laws are built up, there are checks and compensating controls in place, that, in fact, that State election, or that registration database, had been compromised to a point where information was deleted or changed such that a voter had showed up to vote, and their information was not there or otherwise not consistent and there was an abnormality at the poll. There are processes in place across the country, including provisional ballots that would allow that American voter to cast their vote and subsequently that vote would be counted correctly.

Now, I have to emphasize that the outcome here is not security, 100 percent security, it is resilience. So we can take a hit and we can keep functioning and that there is confidence in the system. Yes, that would create some challenges on election day if that had not been detected. I do think it probably be detected beforehand as we saw in 2016, where that compromise was detected. Nonetheless, there are checks, there are compensating controls in place for resilience in the system so that we can sustain those sorts of access and compromise.

Mr. DESANTIS. What's the breakdown roughly between States that use electronic poll books and States that use paper?

Mr. KREBS. So electronic poll books—and I defer to the voting experts on those numbers, if I can.

Mr. DESANTIS. Mr. Hicks?

Mr. HICKS. We would have to get back with you on that information, but there are a number of States that are going towards more electronic poll books as opposed to paper poll books, or registration things. As Mr. Krebs had talked about earlier, there is a resiliency in terms things that these States do. So if the voter registration list

is compromised, those are supposed to be backed up, and then also having some sort of paper form available, so that folks can make sure they are eligible to vote.

Also with provisional ballots, no voter should be able to leave the polls without a chance to cast their ballot under Federal law.

Mr. DESANTIS. In an age where the cyber stuff is always going to be a threat, is it just better for—of a confidence to just have paper ballots?

Mr. KREBS. As long as we continue on with security and accessibility. And right now, paper ballots are auditable. And as long as folks can still cast their ballots who are disabled, then I would say resoundingly yes.

Mr. DESANTIS. And what about election night reporting? What threats is there vulnerability at the local State, both levels, Mr. Secretary?

Mr. KREBS. So when you think about election night reporting, basically what you're talking about unofficial election results that are being reported to either the media, or in some cases, on a website. Keeping in mind, again, that is, on the administration side, it not the official data. And what we have seen recently were some either technical glitches in election night reporting, or perhaps, cyber actor efforts to disrupt election night reporting.

What's important here is, because it's on an NEIT system, it's much like your own congressional web page, it is a web page. There are vulnerabilities in any web page. So what we're trying to do is work with election officials, State and local election officials, to communicate clearly to the voting public that hey, this is unofficial data, if there's a problem we're still going to get you the official results or readout, it might take a little more time. But the integrity of the official election data is intact. There is no connection back between the web site, the reporting website and the official data.

Mr. DESANTIS. I yield back the balance of my time.

Chairman GOWDY. The gentleman yields back. The gentleman from Missouri is recognized.

Mr. CLAY. Thank you, Mr. Chairman.

And Mr. Krebs, I'd like to discuss some documents about Russian attacks on State election systems in 2016, documents that DHS and the administration have refused to provide to this committee. You are familiar with an October 2017 letter to DHS requesting these documents from Ranking Member Cummings and subcommittee Ranking Member Kelly, correct?

Mr. KREBS. Yes, sir. In fact, I reviewed that letter this morning. Yes, sir.

Mr. CLAY. And you are familiar with the official questions for the record requesting these documents, accompanied by a letter signed by our IT subcommittee chair, Will Hurd, following your testimony at the joint subcommittee hearing last fall. Is that correct?

Mr. KREBS. Yes, sir.

Mr. CLAY. Okay. Back in late January, all oversight committee Democrats wrote to Chairman Gowdy seeking a subpoena for these documents. We were ignored. Ranking Member Cummings, along with ranking members of five other House committees, wrote to Speaker Ryan asking for his assistance in obtaining these documents, they were ignored.

Mr. Chairman, I ask unanimous consent that these four letters be made part of the official record for today's hearing.

Chairman GOWDY. Without objection.

Mr. CLAY. Thank you, sir.

Now Mr. Krebs, back at that November hearing, you stated, and I quote, "If you'll permit me to go back and I commit to you that we will have a more fulsome answer for you."

On February 6, 2018, DHS provided approximately 50 pages of documents, most of which were already publicly available. The production did not include any classified documents, nor did it include documents about the precise nature of these attacks. The number of times these States were targeted, or when they were targeted. And this has been 8 months. That is not a mere fulsome answer to our request. It is just more documents that we did not ask for, and that do not answer our questions. Why are you withholding from Congress documents about how Russia attacked our State?

Mr. KREBS. Sir, I don't believe I'm withholding any information. I need to go back and review the answers we provided to those letters. It has always been my commitment to approach this manner in a bipartisan—in a bipartisan manner, a nonpartisan manner. In fact, I see this as a matter of American security, national security. So if you'll permit me, I'd like to go back and look at the answers and also the range of briefings. As I understand, with my staff, we provided 30 if not more classified and unclassified briefings. I personally participated in the Housewide classified briefing earlier this summer, late spring and provided information on what we were doing and what we saw. So, you know, if you're not satisfied with the information, certainly we can go back and look at what we have provided previously.

Mr. CLAY. We are asking what you at the Department of Homeland Security determined about exactly what the Russians, how they attacked us.

Mr. KREBS. Yes, sir, and I think that information is in the intelligence assessment, the intelligence community assessment. The unclassified version provides a significant amount of detail. The catch here is that on the classified side in terms of the tactics and techniques they used against our State networks, it's not highly classified information. It is technical. In fact, the—I think the recent indictments provide additional information.

Mr. CLAY. Well, how about you initiating the interagency process to obtain clearance to give us these documents? Can you do that?

Mr. KREBS. Sir, I—I will, once again, commit to you that we we'll go back and take a look at this and make sure you get what you need.

Mr. CLAY. You know, in fact, we learn more about what happened in Illinois from reading Special Counsel Mueller's indictment of the 12 Russian intelligence officers than we have received from you. We are just asking for some cooperation here, and for you to actually share with us what you know. That's our function, as Mr. Lynch said, we have the oversight function, and we really need some cooperation.

Mr. Hurd signed a letter asking for these documents. I will yield—I don't have time to yield to him now, but——

Chairman GOWDY. You timed that out perfectly.

Mr. CLAY. Yes. Thank you. I yield back.

Chairman GOWDY. The gentleman from Alabama is now recognized.

Mr. PALMER. Thank you, Mr. Chairman. I think my colleague before, Mr. DeSantis, may have asked this question Mr. Krebs, did Russia determine the outcome of our election?

Mr. KREBS. Sir, based in the cybersecurity technical hacking aspects of State and local election officials, we don't have any information to suggest they had access it to vote tallying, and therefore, any ability to technically change votes.

Mr. PALMER. One of the ways to implement the outcome of an election is not necessarily the vote tally on the day of the election, but voter registration. Is that accurate? It could be.

Mr. KREBS. Well, so, if I can understand your question, you're asking if we can influence votes by disrupting voter registration processes?

Mr. PALMER. Or manipulating the voter registration to register people who are not eligible to vote.

Mr. KREBS. So coming at it from the angle of disrupting the registered voters and their ability to vote, we've already talked a little bit about the resilience of the system. But in terms of adding additional people to the vote, I'm not sure what the question is.

Mr. PALMER. Well, my point is this, is that there are more than one way to influence the outcome of an election. We saw this in 2008 and 2010, a group called ACORN. Their voter registration efforts in Nevada, and Colorado, and Florida and other places where they were registering people. There was Indiana, 2,100 voter registration forms that were invalidated because they were all filled out by the same person.

There was another 5,000 set aside because of that. We had a lady who was leading the 2010 effort in Nevada Project Vote program for ACORN who was under indictment, Amy Busefink, and you had a situation in Colorado where they pressured the Colorado agencies that deal with people who are on public assistance; and their fraudulent registration rate was 4 times the national average.

So there are other ways to influence the outcome of an election other than—trying to manipulate the vote total on election day. Is that a fair assessment?

Mr. KREBS. Sir, I don't have experience in that side of the vote process. I would have to defer to the election officials at the table.

Mr. PALMER. Anyone want to respond to that?

Mr. KREBS. Yeah, there will always be attempts to meddle in elections, whether that be through a cybersecurity attack, or through influencing social media, or through trying to get additional people to register to vote as an election official. As a local election official, I have to focus on the things that I can control, and the things that are within my domain. And so, we recognize that there are all sorts of influence out there, and there will be always. What we do is we make sure that the public is confident in the election process itself and we do that by outreach by candidate, parties.

Mr. PALMER. Do you have a responsibility to protect our election process from all threats, both foreign and domestic. Is that fair?

Mr. KREBS. Absolutely, yeah.

Mr. PALMER. I just want to enter into the record, Mr. Chairman, a report from Capital Research Center on what happened with ACORN, just as a reminder, that when we talk about protecting our elections, we are not talking about just protecting them from foreign influence, but also from domestic influence and it's critical. I agree with my colleagues on both sides of the aisle. It's absolutely critical that people have confidence that the vote count is accurate, it reflects the will of the people, and it hasn't been manipulated. So when we talk about that, I hope that every State is taking this seriously.

It is not just making sure that we're protected from foreign influence, but also from domestic attempts by any group from any side of the aisle that would try to influence outcomes from elections. Is that part of what we're doing here, you're nodding your head, Ms. Toulouse Oliver.

Ms. TOULOUSE OLIVER. Absolutely. And I think the examples that you just gave with regard to ACORN, we had similar situations happen when I was a county clerk in New Mexico, found questionable voter registrations, referred them to law enforcement as appropriate. And I think that goes to what we've been talking about all along, which is that that we have to not only protect our systems, but we can never have a 100 percent secure system. So it's also important to remember that our systems are resilient. And so identifying, finding, rejecting fake registrations, being able to identify if fake registrations were to come in through an online portal as well, that's all part of what we're doing. And absolutely, it doesn't matter who is trying to interfere with our elections, foreign or domestic, that's what we are all focused on.

Mr. PALMER. Mr. Chairman, I appreciate the response of the witnesses. And I just would like to say that each one of us are outraged that Russia's made an attempt, but we should be equally outraged when anyone makes an attempt to deny the American public their hard-fought-for and well-defended right to elect for themselves the representatives that they want.

I yield back.

Chairman GOWDY. The gentleman's unanimous request is not objected to. And the gentleman from Massachusetts is recognized.

Mr. LYNCH. I thank the chairman and the ranking member for his kind words. I want to thank the witnesses for your willingness to be so truthful, and blunt, and honest with your assessment of the fact that the Russians have interfered with our elections in the past, and are likely had to do so in the future.

Actually on this committee, I'm actually the ranking member Democrat on the Subcommittee on National Security. So with my colleagues across the aisle, you know, we travel quite a bit, we spend a fair amount of time in Afghanistan. We've probably got 20 trips to Afghanistan, Pakistan, Iraq, Nigeria, Egypt. And ironically, we look very closely at the rule of law issues, elections. And all of these countries, Pakistan, Afghanistan, Iraq, Nigeria, Egypt, among others, have had problems with their elections. And I have to say that I think it has a corrosive effect on democracy in those countries. You look and there's no independent judiciary. There is a decided and pronounced lack of respect for the rule of law in those countries, because it's not seen as endorsed or supported by

the general public, sort of a top-down system with a lot of corruption.

It's oftentimes inimical to the interests of minority rights and human rights in those countries. So I just worry, I worry that if we allow our electoral process, if we allow doubt to creep into the minds of the American people that the elections are not legitimate, then our leaders are not legitimate, then our laws are not legitimate. It is just, again, a corrosive effect that happens. And I'm just very concerned about that. And I think we ought to be all over this, with much more gusto than the President has invited.

Mr. Krebs, I want to start with just a couple of simple questions. Recently we had—a little while back we had FBI Director Christopher Wray testify before Congress. And he said that he was not specifically directed by the President to address Russian interference. I'm just curious, has the President directed you specifically to address the Russian interference?

Mr. KREBS. Thank you for the question. So——

Mr. LYNCH. I think it would be a yes or no. I don't have a whole lot of time here. Either he did or he didn't.

Mr. KREBS. I have been in a policy meeting where the Secretary—or the President made it very clear that election security is a priority.

Mr. LYNCH. No, no, Russian interference.

Mr. KREBS. Russian interference in our election system, yes, sir, is a priority.

Mr. LYNCH. Good, good. That's a good start.

DNI, the Director of National Intelligence, Dan Coats, said, there was no single agency in charge of our sort of countering Russian interference. Is that still the case, or do you think we have a single agency that's taking that over?

Mr. KREBS. Sir, given the range of authorities and capabilities across the Federal Government, this a team effort, this is a whole-of-government effort.

Mr. LYNCH. Okay. Is there—is there a specific White House guidance on the issue?

Mr. KREBS. The guidance to secure the election, yes, sir.

Mr. LYNCH. Oh, that's it? Okay. I'm just curious. Now, since John Bolton came in as National Security Advisor, he fired Rob Joyce, who was the cybersecurity coordinator at NSC. He said he wanted to streamline things. But a lot of people feel that Rob Joyce was one of the smartest people we had on cybersecurity. As a matter of fact, he didn't just fire him, he eliminated the position, so we don't have a—we don't have an adviser on cybersecurity anymore at the White House. Do you think that's helpful or do you think we should use——

Mr. KREBS. Sir, I don't—I don't mean to contradict you, yet I think Mr. Joyce was on a detail from the NSA and he returned to the NSA on a detail so he was not fired, he's still in the Federal Government.

Mr. LYNCH. Okay. The position has been eliminated, though.

Mr. KREBS. The cyber security coordinator position, as I understand it, has been officially eliminated. There are cybersecurity directors and senior directors in the National Security Council. I think the important thing to note here, though, is that operational

responsibility resides in the technical agency. So I have a very clear job, and my work is to work with—and my job is to work with these folks with me at the table, to provide them the resources and capabilities they need to secure the election.

So, again, I have clarity of mission, clarity of purpose. We know what we are doing every day.

Mr. LYNCH. Everybody feels that way? And Mr. Hicks, Ms. Toulouse Oliver, and Mr. Hatch? We're all on the same page and we're going to secure the election. Is that your general assessment?

Mr. HICKS. That's my sworn duty.

Ms. TOULOUSE OLIVER. Yes, sir.

Mr. LYNCH. Okay. All right. I have exhausted my time I think. I think the gentleman for his courtesy. And I yield back.

Chairman GOWDY. The gentleman yields back. The gentleman from North Carolina, Mr. Meadows.

Mr. MEADOWS. Thank you, Mr. Chairman.

Mr. Krebs, thank you for articulating how clearly you feel the mission is for you and your team. We have all kinds of narratives that are out there. But will you reiterate for this committee, and perhaps for the American people, your primary responsibility to make sure that our election process is secure, and that every vote is counted, counted accurately, not double-counted and not interfered with? Is that correct?

Mr. KREBS. Yes, sir.

Mr. MEADOWS. So and you've had that articulated from the administration to you and that you feel empowered?

Mr. KREBS. I have a very clear guidance from my Secretary, I have received guidance from the White House, I am empowered to do my job, I have clarity of mission, clarity of purpose. I spent 40 to 50 percent of my day focused on the 2018 mid-terms and beyond.

Mr. MEADOWS. Well, I appreciate you reiterating that, because I've talked to the Secretary, and she has articulated that very clearly to me, and it's good. Because sometimes, it doesn't get transferred to those that actually do the work. What you're saying is you have a clear vision. Do the people that work for you have a clear vision?

Mr. KREBS. Sir, I would actually have to defer on answering that question. I would actually ask Secretary Toulouse Oliver if she feels that my folks that work with her on a daily basis are unable to do their jobs. I think that would be the best way to get that answer.

Mr. MEADOWS. Very well. Go ahead.

Ms. TOULOUSE OLIVER. Yes. I actually wanted to make a comment earlier as Mr. Krebs was describing the provisional balloting process, and some of the other technical processes that we undertake. I am so proud that DHS has learned elections from working closely with us, and maybe not completing, but yes, I absolutely do believe so, sir.

Mr. MEADOWS. All right. Thank you both.

So let me give you a to-do, because one of concerns I have is really that paper trail. Obviously, we have a bill that is a bipartisan bill that looks at a paper system. But here's the problem on elections and part of why we're seeing this: We need, from a security standpoint, really a level of this is most secure—kind of like when

you put in a password, you know, you know the longer your password the better it is, but I'm talking about systems. Because in my—I represent 16 counties, and we have multiple different ways to vote within my own congressional district. So I've got paper ballots in part of it, I've got electronic ballots in another part. You know, we have the typical bubble in and scan in one county and we have all electronic. And yet, they are making individual purchases many times on voting systems so it's not necessarily handled at the secretary of State level in some States.

So it would be very good to have a resource where they come and they said, okay, if you're looking at upgrading your system, here are the five things you need to do and this is most secure, this is—because I don't find that, do we have that currently?

Mr. KREBS. So I can speak very briefly, and then we'll quick it over to Commissioner Hicks here.

But we work closely with the EAC. We work through the Government Coordinating Council.

You've got to keep in mind that every State's different. Some are top-down; others are bottom-up. Every county is going to be different in terms of resource, population, the quality of the infrastructure——

Mr. MEADOWS. Listen, you're preaching to the choir. I get that.

Mr. KREBS. So——

Mr. MEADOWS. But the real problem is that there is not a resource at this point at the Federal level. I mean, Mr. Hicks, with all due respect as a Commissioner, this is the first time I've ever heard of the U.S. Election Assistance Commission, you know, and I—and when we see that, when you Google that, it doesn't come up. You're not in the top 10 in terms of search.

How do we make sure that States not only are aware of not just our witnesses today but that there is a real criteria?

Mr. HICKS. That means we're doing our job, because we don't want to be known. We want to make sure that we work with the States to make sure that they get the resources they need to ensure the process functions correctly.

We were down in your State of North Carolina about a month ago with a testing and certification class.

And we do certify voting systems, but it's on a voluntary basis. States come to us and they say, these are the systems we want to have certified through the manufacturers, and those systems are certified.

Right now, we don't have a quorum of commissioners, so we can't do the next iteration of those voting system guidelines. They haven't been updated since about 2007.

Mr. MEADOWS. So is there a Federal guideline on what you would recommend to States in terms of how to secure their system? Is there that?

Mr. HICKS. On how to secure their systems? There are guidelines on that.

Mr. MEADOWS. And are there priorities in terms of, if they're going to the replace equipment, what are the recommendations you make? Do you have——

Mr. HICKS. That's in our Voluntary Voting System Guidelines 2.0, which we can't vote on because we don't have a quorum.

Mr. MEADOWS. All right.

I yield back. Thank you, Mr. Chairman.

Mr. GOWDY. The gentleman yields back.

The gentlelady from Michigan is recognized.

Mrs. LAWRENCE. Thank you, Mr. Chair.

A February 16, 2018, New York Times article titled "Inside a 3–Year Russian Campaign to Influence U.S. Voters" mentioned the painstaking efforts taken by the Russian Government to not only divide our Nation along party lines but also along socioeconomic and racial lines.

And in October, "Woke Blacks," an Instagram account ran by the Internet Resource Agency, carried the message, "Hatred for Trump is misleading the people and forcing Blacks to vote for Killary. We cannot resort to the lesser of two devils. Then we'd surely be better off without voting AT ALL."

Then, just days before the Americans went to the poll, another Instagram account controlled by the Russians called "Black Activists" urged its followers to choose peace and vote for Ms. Stein, who was expected to siphon support from the Clinton campaign. And the message read, "Trust me. It is not a wasted vote."

I also have—and, Mr. Chairman, I ask for it to be entered into the record—I have the February 18th ABC News article "Russian Influence Operation Attempted to Suppress Black Vote." It reveals that the special counsel indictments against 13 Russian nationals in January of 2018 revealed that a key aspect of the assault on the 2016 election was an attempt to suppress the turnout by African-American voters, which papers filed in a Federal court describe in great deal.

Mr. GOWDY. Without objection.

Mrs. LAWRENCE. Our esteemed ranking member, Mr. Cummings, made a very accurate statement in this article: "Of particular concern, the indictments show how the Russians tried to suppress the votes of minorities across the United States in order to help" the current President win his Presidency.

So, to Ms. Oliver and Mr. Hatch, you both represent communities where there are minorities votes. And we have actual investigative data that shows many campaigns across the country of our Nation were targeted at suppressing minority votes. What are you doing to ensure that every vote counts?

Mr. HATCH. Thank you for asking that question, Mrs. Lawrence. In Weber County, the county seat is the city of Ogden, which is approximately one-third Hispanic population, and so we do have a sizable minority population.

As an election official, my focus is on removing barriers for voters and to ensure that they have confidence that when they go to the polls or when they mail their ballot back in, that they have confidence that that ballot will be counted fairly and accurately and that the results will be fair and accurate. And I do those regardless of the nature of the voter, the location of the voter, whether it's in a neighborhood that is known for having more minorities.

The focus is clearly on establishing a process that's full of integrity. And I think by doing that, that allows both those in the majority and those in the minority to know that, as far as election ad-

ministration concerns, we're color-blind and we focus on you as a citizen and your right to vote.

Mrs. LAWRENCE. Ms. Oliver?

Ms. TOULOUSE OLIVER. I would echo those statements. And I would also say that, as election officials, we are also concerned about accurate information on the internet and social media, and so we are always working to make sure that the most accurate, up-to-date information is being provided to the voter.

Another aspect that really impacts minority voters in our communities and across the country is adequate language minority assistance and ensuring that we are in compliance with section 203 of the Voting Rights Act. I have many tribal areas in my State, in addition to Spanish-speaking areas, so that's also incredibly important. We are doing everything within our power to do that. But there can always be more that can be done.

Mrs. LAWRENCE. I want to state, because my colleague from Michigan referenced some training issues that are desperately needed in the State of Michigan, it's unacceptable, because our vote is our democracy.

But, with that being said, training and to have the resources to attack, cyber attacks or meddling in our elections, are two different things. And you cannot say, well, the only thing we need is training. And our Secretary of State has accepted and has stated that she is using our Federal dollars to fight against the interference of the—to protect the integrity of our election. So by no means does it mean that.

My closing question is to you, Mr. Hicks. Mr. Hicks, you have to recognize that this concerted effort to suppress the vote is real, it's been documented, and it's a concerted effort of Russia. Where do you, as on the Commission, stand with that? Do you address it?

Mr. HICKS. That's something for the Department of Justice to address. But, personally, I've always worked towards ensuring that voter confidence remains high when I worked in the House, when I worked in Massachusetts and so forth. So ensuring that people have their right to vote and that they can do so without encumbrance.

Right now, while this committee is having its hearing, the EAC is holding a language summit for folks who have access issues to the polls based on language, over at the Newseum. That's being webcast, and there's about 150 people right there learning more about access.

Mrs. LAWRENCE. Thank you. I yield back.

Mr. GOWDY. The gentlelady yields back.

The gentleman from Texas is recognized.

Mr. HURD. I thank you, Mr. Chairman.

I also thank the gentlewoman and chairwoman from North Carolina for her courtesy.

My opinions on the Russian role in our elections is pretty clear, so I won't get into them today. But I am concerned that some of my friends on the other side of the aisle are implying that DHS or this Congress is not taking this issue seriously.

And so my first question for you, Mr. Hicks and Mr. Krebs: How many meetings, briefings, hearing, phone calls, responses to memos and letters have you had with Congress? And I don't need an exact

amount. Two was mentioned earlier, that there was only two hearings. How many engagements with Congress have you had and your staff had on this issue of securing our election?

Mr. HICKS. Engagements? I wouldn't have the exact numbers, but that's basically a daily occurrence in our agency right now. But that's not our only function.

Mr. HURD. So several dozen?

Mr. HICKS. Of letters from various Members of Congress.

Mr. HURD. Of responses that you've had to give.

Mr. Krebs, do you have an aggregate number?

Mr. KREBS. I've lost count. It'd be a guess. I've personally testified on this matter at least three times.

Mr. HURD. Mr. Krebs, does your division—or does DHS have more money today to deal with support to election than they did in 2016?

Mr. KREBS. Yes, sir. $26.2 million through the FY18 omnibus.

Mr. HURD. Ms. Toulouse—Secretary Toulouse Oliver, excuse me, has your State received more money from the Federal Government to help defend election infrastructure in 2018 than they did in 2016?

Ms. TOULOUSE OLIVER. Yes, sir, we have.

Mr. HURD. Mr. Hatch, your State or your county, whichever you feel comfortable representing?

Mr. HATCH. Yes. $4.1 million for the State.

Mr. HURD. And for both of you election officials, what kind of activity—so let me start with this. I remember, prior to the 2016 election, many secretaries of States were against the idea of establishing our election systems as critical infrastructure. There was a number of hearings prior to the election; there was hearings after the election. And the previous administration designated it critical, and then this current administration continue that.

Is there still opposition from secretaries of State to have our election systems be critical infrastructure?

Ms. TOULOUSE OLIVER. Yes, sir, that is the case. And I believe that that stems from a genuine concern among secretaries that that is——

Mr. HURD. Federalizing elections?

Ms. TOULOUSE OLIVER. Exactly.

Mr. HURD. Because, ultimately, States are responsible for elections, right?

Ms. TOULOUSE OLIVER. That is correct.

Mr. HURD. And, ultimately, States are responsible for defending the elections.

Ms. TOULOUSE OLIVER. That is correct. However, we do conduct Federal——

Mr. HURD. Sure.

Ms. TOULOUSE OLIVER. —State, and local elections. And so I do personally believe that a partnership with the Federal Government is necessary and critical.

Mr. HURD. So are these kinds of conversations happening in capitols around the country, where Governors and State representatives are increasing State funds to ensure that election officials in their States have the resources and tools that they need?

Ms. TOULOUSE OLIVER. I can certainly tell you that that has been happening in the State of New Mexico. And to the extent that our States are receiving these HAVA funds, it is required for the States to provide a match. So each State is providing a 5-percent match, as we heard here today, every single State.

Mr. HURD. So can States be doing more as well?

Ms. TOULOUSE OLIVER. Pardon me?

Mr. HURD. We've heard here today that the Federal Government can do more. And can States be doing more as well, too?

Ms. TOULOUSE OLIVER. Absolutely. States and the Federal Government can both be doing more.

Mr. HURD. Good copy.

Mr. Hatch, in your testimony, you stated that only 9 percent of election officials are members of the Elections Infrastructure ISAC, the Information Sharing and Analysis Center. This seems to me to be concerningly low.

Do you have an opinion on why so few people are actually engaging in the Federal, State, tribal partnerships that's responsible for sharing information on the integrity of our elections?

Mr. HATCH. Thank you for asking that. Yes, it is low. The main reason why is because it's new, and it's only been up and running for just a couple of months. The rate at which counties are joining the EI–ISAC, and States as well, is alarmingly fast, which is really hopeful.

And organizations such as NACO and the International Association of Government Officials, the EAC, NASS, they are all helping——

Mr. HURD. So, Mr. Hatch, I'm sorry to interrupt. My time is limited. But you would encourage your fellow election administrators across the country to join the Elections Infrastructure ISAC?

Mr. HATCH. It's one of my primary jobs.

Mr. HURD. And how do they do that?

Mr. HATCH. They go to the website. They contact any association. It's very easy.

Mr. HURD. Bingo. They can do that through the National Association of Secretaries of State as well, correct?

Mr. HATCH. Yes.

Mr. HURD. And, Mr. Krebs, my question—this last question is to you and Secretary Oliver as well.

When it comes to defending the digital infrastructure, security vulnerability assessments, technical vulnerability assessments, this is something DHS has prepared for and is already doing a lot of work. Our States are doing that.

But my concern is with crisis communications. Who is responsible for dealing with things that happen on the day that is used in a way to mislead potential voters? How is that conversation, how is that coordination happening amongst election officials and secretaries of States and with the Federal Government?

Ms. TOULOUSE OLIVER. So that is something that we've always sort of dealt with on a case-by-case basis. I will say that, through our work with the Government Coordinating Council, we recently developed a communications protocol, and we are working together to develop a comprehensive way in which we approach and talk

about and collectively discuss in the public sphere things that may occur around election time.

Mr. HURD. Mr. Chairman, I yield back the time I do not have.

Mr. GOWDY. The gentleman yields back.

The gentleman from Illinois, Mr. Krishnamoorthi.

Mr. KRISHNAMOORTHI. Thank you, Chairman. Appreciate that.

Secretary Krebs, on April 17th of this year, DHS Secretary Nielsen had this to say about Russian interference in the 2016 elections. She said, quote/unquote, "Two years ago, the Russian Government launched a brazen, multifaceted influence campaign aimed at undermining public faith in our democratic process generally and our elections specifically."

And I think you may have even alluded to some of this before. I assume that the DHS stands by the Secretary's statement, correct?

Mr. KREBS. DHS stands by the Secretary, and the Secretary stands by the intelligence community assessment.

Mr. KRISHNAMOORTHI. And, of course, you do the same. You stand with the Secretary as well as the——

Mr. KREBS. Yes, sir.

Mr. KRISHNAMOORTHI. —intelligence community?

On January 6, 2017, the Office of the DNI had this to say about Russian attacks: Quote/unquote, "We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him."

On July 19th of this year, Secretary Nielsen tweeted the following: Quote/unquote, "I agree with the intel community's assessment, full stop."

I presume DHS stands with Secretary Nielsen's statement, correct?

Mr. KREBS. Yes, sir, we do.

Mr. KRISHNAMOORTHI. And, of course, you stand by Secretary Nielsen's statement, right?

Mr. KREBS. Yes, sir.

Mr. KRISHNAMOORTHI. Okay.

Just—let's see here—25 minutes ago, President Trump just made the following tweet, hot off the tweeter presses: Quote/unquote, "I'm very concerned that Russia will be fighting very hard to have an impact on the upcoming election. Based on the fact that no President has been tougher on Russia than me, they will be pushing very hard for the Democrats. They definitely don't want Trump!"

Obviously, as you saw from the DNI's report from January 6, 2017, the entire intelligence community concluded that Russia was trying to harm Hillary Clinton's campaign and help Donald Trump's campaign.

The question is this: According to the President, the Russians definitely don't want Trump. Mr. Krebs, do you agree with this tweet?

Mr. KREBS. Sir, I have made it a habit to focus on my job and work with State and local governments like this and not interpret headlines or Twitter.

I do know that the President, as soon as—oh, thank you.

I do know that the President endorses the intelligence community assessment. He was very clear on that last Tuesday.

As I said to Congressman Meadows earlier, I have a very clear direction on what my job is, to help State and local officials protect their election systems. Secretary Nielsen has provided me the same guidance. I'm empowered to do so. I have the team and the resources——

Mr. KRISHNAMOORTHI. I understand, but here's my question: Do you know of any evidence, classified or unclassified, suggesting that the Russians are trying to help the Democrats?

Mr. KREBS. Sir, in terms of any intelligence, I'd have to go back and look. I'm not able to speak to any classified matters in this forum.

Mr. KRISHNAMOORTHI. Okay. So you're suggesting that there may be evidence——

Mr. KREBS. No, sir, I am not. No, sir, I am not.

Mr. KRISHNAMOORTHI. You are not. Do you have any knowledge of any evidence that might back up what the President just tweeted?

Mr. KREBS. I think the evidence would be that this administration has launched a series of sanctions, has expelled diplomats. He's taken other actions against the Russian Government.

Mr. KRISHNAMOORTHI. No, but do you have any evidence that they are pushing very hard for the Democrats? That is, the Russians.

Mr. KREBS. Sir, I do not have all—you know, access to the information that informed the President on this, so I'd have to get back to you.

Mr. KRISHNAMOORTHI. Yes, I'd like you to get back to us. Thank you.

Mr. Chairman, this tweet and the substance of this tweet is total fiction. It defies reality, and it contradicts everything our own intelligence officials have concluded.

Mr. Krebs, you must be aware of the fact that the Russians are continuing to target our election infrastructure and the upcoming elections, correct?

Mr. KREBS. So I believe that, as we've stated, DNI Coats has stated, we certainly have not seen anything at the level of 2016. They are continuing to conduct information operations against the American people in general.

Mr. KRISHNAMOORTHI. FBI Director Wray on July 18th said, "The intelligence community's assessment has not changed. My view has not changed, which is that Russia attempted to interfere with the last election, and it continues to engage in malign influence operations to this day."

You don't have any basis for disagreeing with his statement?

Mr. KREBS. No, I agree 100 percent with Director Wray.

Mr. KRISHNAMOORTHI. Okay.

Mr. Trump, the President, was asked a question just last Wednesday: Is Russia still targeting the U.S., Mr. President?

Answer: Thank you very much. No.

Question: No? You don't believe that to be the case?

Answer: No.

Do you agree with the President that Russia is not targeting the 2018 election?

Mr. KREBS. I believe there is some disagreement on exactly what happened in that exchange. But I'll tell you right now that I firmly believe that the Russians continue to target not just our democracy in general but our critical infrastructure in particular.

Mr. KRISHNAMOORTHI. So you disagree with the President?

Mr. KREBS. No, sir, I'm not saying that.

Mr. KRISHNAMOORTHI. You just did.

Mr. KREBS. I don't. No, sir, I——

Mr. KRISHNAMOORTHI. Thank you.

Mr. GOWDY. The gentleman yields back.

The gentlelady from North Carolina is recognized.

Ms. FOXX. Thank you very much, Mr. Chairman.

Mr. Krebs and all of our witnesses today, thank you for being here.

I'm a firm believer that, before any problem can be addressed, we need to find out where the responsibility lies. As we all know, much of the administration of U.S. elections is explicitly delegated to the States through the elections clause of the Constitution.

And before we turn to what's being done at the State level to protect the integrity of our elections, I believe it's necessary to ensure that the Federal house is in order. The findings of our Nation's intelligence agencies and the House Committee on Intelligence leave no doubt that Russia maliciously attempted to influence our elections. Clearly, we need to right the ship on the Federal level to ensure Russia and other harmful actors cannot repeat that behavior.

Unfortunately, the President's recent comments at the U.S.-Russia summit in Helsinki failed to hold Putin accountable for his attacks on our country's interests and deter him from future indiscretions. I believe deterring a foreign adversary from meddling in our elections and disrupting the malign actions of a foreign adversary should be a Federal responsibility.

Can you assure us that the Department of Homeland Security is doing everything in its power, actively, to safeguard our Nation from the kind of meddling that we now know has occurred in the past, including the hacking of our campaigns by Russian intelligence officers?

Mr. KREBS. Yes, ma'am. This is one of our top priorities.

Ms. FOXX. Thank you for that answer, Mr. Secretary.

Shifting to the topic of security clearances of State officials, is it necessary for every State to have an official with a security clearance?

Mr. KREBS. It's certainly useful in the event we need to share information. But we do have the ability to provide 1-day read-ins if there is a very tactical piece of intelligence where, if I needed to share with someone in New Mexico or Utah, I could do that using local resources.

Ms. FOXX. Thank you.

So what is DHS doing to declassify cyber threat indicators to allow for more widespread and timely information-sharing?

Mr. KREBS. So we work very closely with the intelligence community to define not just what the information of interest for this community would be but also help get a better understanding of what

their infrastructure looks like. And so that can go help inform collection. And then, through that process, we can actually identify additional intelligence and then start pushing that into the declassified space.

One thing I'll note, ma'am, is that, in 2016, when the Department of Homeland Security knocked on the doors of State secretaries and election officials and they said, "I've never talked to you before, there's no trust here, but I've got a problem that you need to know about," anyone, by very nature, would probably say, "I'm going to need to know a little bit more information." And the response at the time, because it was classified, was, "I'm sorry, I can't share that with you."

Two things have happened since then. One, we have established that level of trust. So, if someone in New Mexico does not have a clearance and yet I work with Secretary Toulouse Oliver and I knock on the door and say, "Hey, we have a problem, it's classified, I need you to do something," I think, my guess is that the level of acceptance has changed a little bit.

But, at the same time, we are more sophisticated in our information-sharing protocols, we are more sophisticated in our ability to declassify information and take action. And it is all based on trust. We have spent so much time building relationships, building trust with these State and local election officials that we are much more effective than we were even a year ago.

Ms. FOXX. Thank you, Mr. Krebs. I think you have made us feel a lot better about the situation as it exists now, and so we appreciate the effort that you and your colleagues have put into it.

Ms. Toulouse Oliver, were you able to obtain a Federal security clearance?

Ms. TOULOUSE OLIVER. Yes, ma'am.

Ms. FOXX. You were. And how many officials in your State have a security clearance for election-related purposes?

Ms. TOULOUSE OLIVER. I have that clearance, and two of my key staff have that clearance as well.

Ms. FOXX. Thank you.

Mr. Krebs has described a change in behavior and trust level. So has information-sharing between DHS and your office improved, from your perspective, since you were granted a security clearance?

Ms. TOULOUSE OLIVER. I believe that communication has improved in general. I don't think it came as a result of the clearance, but I do think that that contributes to our level of confidence that we will be able to get accurate and timely information.

Ms. FOXX. Right.

One more quick question, Mr. Chairman, if I could.

Do you have an idea of how much information disseminated from DHS and the Federal Government is considered classified or sensitive? Any——

Mr. KREBS. In the election space specifically?

Ms. FOXX. Well, either one of you.

Ms. TOULOUSE OLIVER. My sense is that, quite frankly, there isn't all that much. It would only be if there was a situationally specific piece of information that needed to be conveyed.

Ms. FOXX. Thank you, Mr. Chairman.

Mr. GOWDY. The gentlelady yields back.

The gentleman from Maryland, Professor Raskin.

Mr. RASKIN. Mr. Chairman, thank you very much, and thank you for calling this hearing.

I want to go first to Mr. Hicks, the chair of the Election Assistance Commission.

As you know, I represent the Eighth Congressional District in Maryland proudly. Your offices happen to be in my district, so I follow your work closely.

In Maryland, we were notified just a couple weeks ago by the FBI that the private vendor that our State uses for purposes of election administration management of our voter registration database has close ties to a Russian oligarch connected to Vladimir Putin.

This bizarre revelation, perhaps a coincidence, perhaps not, has raised profound questions about the potential for interference in our elections by compromised private election vendors due to the extraordinary lack of regulation on how election vendors do their business. So I wanted to ask you several questions about this to see how far this problem may indeed go.

After this revelation about ties to a Russian oligarch of our election vendor in Maryland, has there been any way for you to determine what other States may be using this vendor or other vendors who have ties to Vladimir Putin and his oligarchs?

Mr. HICKS. That's an ongoing investigation, and the EAC does not have the wherewithal to comment on that right now. I would defer to my colleague at DHS to talk a little bit more about that.

Mr. RASKIN. Well, okay. I don't have too much time, but, Mr. Krebs, let me ask you. Is there an ongoing investigation at Department of Homeland Security about whether there's some kind of systematic plot by Russia to exercise influence over private election vendors?

Mr. KREBS. So we are looking in specific to the Maryland case. And thank you for your letter on that front. This is actually one of those stories of progress. When the State Board of Elections in Maryland was notified that there was a connection, they immediately reached out to us and asked for help, and we have deployed that assistance.

So we are making progress here. Again, those relationships did not exist a year ago.

Mr. RASKIN. Okay. Forgive me for my sense of urgency, but we have election in, I think it's 107 days, maybe it's 108 days, at this point. It is right around the corner. And so it doesn't give me a lot of comfort to learn that there's progress being made.

So have you determined that there are any other States whose election vendors have been compromised by connections to Russian oligarchs or Vladimir Putin?

Mr. KREBS. This is a broader supply chain conversation. We do know that, in the case of Maryland, that there—at least according to the information I've seen, there was no ability to influence based on that venture capital firm. But we are conducting a broader assessment of the risk environment.

Mr. RASKIN. When do you expect to have the results of this investigation, this ongoing investigation?

Mr. KREBS. I assume that this investigation, because of the nature of procurement cycles, will be ongoing and, frankly, will never end. As we develop more information, we'll act on it.

Mr. RASKIN. Okay, but, Mr. Krebs, forgive me. Are there States who have election vendors today that are running elections in November who have ties to Russian oligarchs or the Putin government?

Mr. KREBS. Sir, at this point, I don't have information to share on that.

Mr. RASKIN. Is there anyone at the Department of Homeland Security who does have that information?

Mr. KREBS. Sir, I do not—I'd have to defer, actually, to the Federal Bureau of Investigation.

Mr. RASKIN. Okay.

Is there anyone on the panel who knows how many States are currently contracting with private election vendors who are using foreign-made parts or foreign software in their election day products?

No one can tell us. Okay.

Mr. Hicks, back to——

Mr. KREBS. So this is a broader——

Mr. RASKIN. I gotcha. I gotcha.

Are vendors currently required by Federal law to adhere to cybersecurity best practices and/or to report to the EAC in the event that there is some breach of cybersecurity?

Mr. HICKS. No.

Mr. RASKIN. Are vendors uniformly required to report any cyber threats to you?

Mr. HICKS. Uniformly, no, because it's a voluntary system.

Mr. RASKIN. Okay. All right. As I thought.

I thank you all for your answers, but they demonstrate why I've introduced H.R. 6435, the Election Vendor Security Act of 2018, which requires election vendors to be owned and controlled only by citizens or permanent residents of the United States, to adhere to cybersecurity best practices, and to report all known or suspected cybersecurity breaches or threats to State and Federal authorities immediately.

I would urge all of my colleagues on both sides of the aisle on this committee to join me in this effort to protect the integrity of our election processes in 2018. This is something that needs to be done right now. And this is not something that can be put off to another day; it's not something that can be postponed. And we cannot be satisfied with vague promises of ongoing progress and investigation. This is a democratic emergency. The elections go right to the heart of democratic self-government in our country.

I yield back, Mr. Chairman.

Mr. GOWDY. Professor Raskin yields back.

The gentleman from Wisconsin is recognized.

Mr. GROTHMAN. Right. I have long had an interest in election integrity, going back to the days when I was involved in State election law in the State of Wisconsin. And I can only imagine what I would do if I was a foreign country trying to influence our elections or make sure that the wrong person won elections. I'm going

to ask you about some areas of election law that, if I were trying to influence our elections, I might take advantage of.

The first thing, in Wisconsin, we finally passed a photo ID law last year. And I think the reason we had that is we want to make sure that the right person is voting. And if I was going to try fix an election, I might try to get people to pretend they were somebody they were not. I know they have photo IDs in Mexico, for example.

Can you guys comment on, in your experience, how many States around the country have done what Mexico does or what Wisconsin does and has a photo ID law? And if you're aware of any States that don't, why wouldn't they do that?

Mr. HICKS. I would have to get back with you on the exact number, but there are a number of States that have photo IDs, and there's a number of States that do not. There are different aspects to verifying the person who is casting a ballot, but there are other ways that people are casting ballots. For instance, there are three States in our Union that entirely vote by mail, that don't require you to send in your photo ID.

But the Help America Vote Act has in it a provision that says, if you register to vote by mail for the first time, you have to submit some form of ID, whether or not that's a bill or electrical outlet—electrical bill or something to that—or——

Mr. GROTHMAN. Why wouldn't you do it? It seems so basic. I always kind of question politicians who wouldn't do that. I mean, the same politicians who require photo IDs for getting maybe lifesaving drugs, a photo ID for a variety of other things, all of a sudden, when it comes to elections, they say no. And I always kind of feel it opens up our elections to fraud.

But does anybody—Ms. Toulouse Oliver, do they have photo ID in New Mexico?

Ms. TOULOUSE OLIVER. No, we don't.

Mr. GROTHMAN. Now, you must be familiar with Mexican law, right across the border. Is what I'm told right? Do they have photo ID in Mexico?

Ms. TOULOUSE OLIVER. I am not an expert on Mexican law, and, unfortunately, I don't know. But I take your word for it.

Mr. GROTHMAN. Okay. Any reason why we don't do that simple thing to guard against nefarious influence in our elections?

Ms. TOULOUSE OLIVER. The main reason is because we have a number of individuals within our State who, for one reason or another, do not have certain types of photo ID that might be required. For example, our tribal people in New Mexico don't have, necessarily, photo ID, don't necessarily want to utilize a photo ID, and we still want to provide the opportunity for them to participate in our elections.

Mr. GROTHMAN. Okay. And I am under the impression—I might be wrong—I'm under the impression from somebody who is Mexican that they one in Mexico, but okay.

The next thing that concerns me—I always feel if I wanted to make sure the—if I wanted to fix an election, I would want to have a lot of people not voting in person. You know, when you vote in person, at least you watch Glenn Grothman go in. He's the guy in there. Nobody else is whispering in my ear. You do some early vot-

ing or absentee voting, you never know if somebody else is really filling out that form or who's filling out that form.

Over time—and maybe Mr. Krebs, maybe Mr. Hicks would know—over time, have we had more people voting in a place in which we can see that they are not being influenced, nobody's whispering in their ear, we can watch who's filling it out? Or over time, have we had more people, like, early voting or voting by mail, where who knows who's really filling out the ballot?

And I would hope our goal would be, over time, more and more people would be voting where we'd have a government official, the local clerk, watching to make sure nobody else is following them in the booth and saying, "Vote for Glenn Grothman," this or that. That seems like a good thing if we want to increase the integrity.

Which way are we going in this country? Are we having more people in which the government official can watch, or are we having more people voting, you know, somewhere where who knows who's really filling out the ballot?

Mr. HICKS. Well, Congressman, I believe that a number of our military and overseas voters vote not in person but by mail and so forth.

Mr. GROTHMAN. Yeah, I know that, but I'm not talking about the military. I'm saying, across the board, of all the people who voted, say, in the election in 2016 compared to 2008 or 1992, which way are we going in this country? We have four experts here.

Mr. HICKS. Every 2 years, the EAC publishes a document, the Election Administration & Voting Survey, where we survey all the jurisdictions about the way that they vote. We can get you a copy of that, which will lay out all that information on who's voting where and how they're voting.

Mr. GROTHMAN. Does anybody know?

Mr. Hatch, you must know. You're a county auditor there. You must know today compared to, say—how long have you had your current job or how long have you been involved in elections down there in Utah?

Mr. HATCH. About 7–1/2 years.

Mr. GROTHMAN. Okay. You must know. In the last—you must work with people who've been around there longer than that—in the last 20 years, has it gone up or down? Do we have more election security where we know that person's voting in the voting booth and nobody's whispering in their ear?

Mr. HATCH. I can clearly and confidently speak about what's happened in Utah. Utah is a virtually completely-by-mail State, although we do have vote centers available early as well as on election day. Anybody who votes by mail must sign the envelope, and we have human eyes look at every single signature before we allow that vote to be cast.

Mr. GROTHMAN. Do you know what the signature should be? Like, if I moved to Utah, you'd know what Glenn Grothman's signature is and it wasn't somebody else's signature?

Mr. HATCH. Yes. In order to register to vote, we will capture your signature.

Mr. GOWDY. The gentleman's time has expired.

Mr. GROTHMAN. Okay. Thank you.

Mr. GOWDY. The gentleman from Maryland is recognized.

Mr. SARBANES. Thank you, Mr. Chairman.

Mr. Krebs, did you say that—you mentioned something called an intruder detection system that had been put—did I understand you to say that 21 States had the benefit of that? What was it you said about that?

Mr. KREBS. At the time in 2016, 21 State election—about 21 State election systems at the State level were behind an Albert sensor, this intrusion detection sensor, yes, sir.

Mr. SARBANES. And were those the States that flagged that there was——

Mr. KREBS. Yes, sir. For the most part, what we were able to do was upload some of the indicators that were provided on other activity, including in the State—the Midwest State, and load it up into the system. It's managed by a group called the Multi-State ISAC. So the indicator was loaded up into the system, and then there were hits across prior traffic.

Mr. SARBANES. I see. So, in those 21 States, there was evidence through this detection system that there had been efforts to hack into the——

Mr. KREBS. There had been visits, yes, sir. So, basically, what we——

Mr. SARBANES. Was the IDS in place in other States or just——

Mr. KREBS. Not on the election systems, but Albert sensors are deployed to every single State. There'd been——

Mr. SARBANES. But, in those 21 States, it was on the election systems.

Mr. KREBS. For the most part, yes, sir.

Mr. SARBANES. So, in the places where the IDS was deployed on election systems, here was a detection of efforts to get in.

Mr. KREBS. We saw traffic.

Mr. SARBANES. You saw traffic.

Mr. KREBS. Yes, sir.

Mr. SARBANES. And so, in all of the places where the IDS system was in place with respect to election systems, they were able to detect traffic.

Mr. KREBS. I don't have information on whether it was all of the systems. I'm just saying in the 21 States where we did have the——

Mr. SARBANES. It sounds as though that system wasn't in place, the IDS, in 29 States. But based on the experience of the 21 States, where they all seemed to get this traffic, one might reach the conclusion that, if that IDS system had been laid on top of the election systems in those other States, based on 100-percent occurrence in the 21, that you might have found evidence there as well.

Mr. KREBS. My operating assumption is all 50 States——

Mr. SARBANES. Yeah, okay. So that's an interesting detail I hadn't focused in on before.

I wanted to talk a little bit again to you, Mr. Krebs, about the process you're going to have when you spot, through DHS or some other—you know, in cooperation with the intelligence community or what have you, that there is an immediate present danger being posed to an election system somewhere in the country, hat you're going to do—what's the process for reaching out in real-time as soon as that threat is picked up to the election administrator in

that State to say, "Look, we've flagged this, red alert, here's what we're hearing," et cetera? Can you just describe how that's going to work?

Mr. KREBS. Sir, it's actually not much more sophisticated than what you just laid out. We have a duty to warn—the intelligence community has a duty to warn when there's an imminent threat.

And so what we would do is, working with the intelligence community, identify that information, identify the target, reach out through some information-sharing protocols that we've developed with the Government Coordinating Council. We will notify the chief election official in the State, the Governor, the homeland security adviser, the chief information officer. So we will hit the big four or five in each State, and we'll say, "Hey, look, this threat is incoming. We need to deal with it now. We are here to help you."

Mr. SARBANES. Okay. So it's not just notification. It's, okay, it's a team effort here, what can we do to help you. And so what kind of resources or response or kind of SWAT team effort then gets brought to bear when the local person says, oh, my god, okay, thank you, and, you know, we're locking the doors and pulling down the shades, but we need your help? What then is forthcoming within, say, 24 hours or less?

Mr. KREBS. So what you're really getting to is that move and that evolution beyond just simply information-sharing. It's actually managing risk. It's asking two questions: One, so what? What does this information mean? And, two, what are going to do about it?

So when I would theoretically or hypothetically contact Secretary Toulouse Oliver and say, "This is the problem you have, run a quick assessment, let me know what you need," I have fly-away teams located in D.C., in Florida, and elsewhere throughout the country that I can deploy within a couple hours' notice, with equipment, on the ground supporting the secretaries.

Now, it's not just DHS; this is a broader effort. If we need to engage the National Guard, we can do that. If we need to engage——

Mr. SARBANES. Can I ask you to do me a favor? I'm going to run out of time. What you're describing sounds good. Based on the experience with what happened with some of the 21 States last time and the way the alert was given but then it seemed like the Federal folks, in a sense, kind of walked away from the enterprise, I didn't have as much confidence about this.

So, if this is going to be the kind of response that you have going forward—and I certainly urge that—it would be nice for us to get some reporting back, particularly if we're in the effected States. Open up a dialogue. Whether it has to be classified or not, you know, that's your judgment, but we need to know in real-time that the alerts are being—that the threats are being taken seriously and it's not just saying, "Hey, you've got a problem," it's saying, "Here's what we're going to do about it." Okay?

Mr. KREBS. Yes, sir.

Mr. SARBANES. And I yield back.

Mr. GOWDY. The gentleman's out of time.

The gentleman from Virginia is recognized.

Mr. CONNOLLY. Thank you, Mr. Chairman.

Mr. Krebs, a number of us have repeatedly asked your department for documents showing how Russia attacked State election

systems in 2016. Those documents, despite our requests, have been withheld since last October.

Eleven days ago, we finally got some information, but not from you. It was from the indictment filed by the special counsel, Mr. Mueller, against 12 Russian military intelligence officials.

Why did DHS withhold this information, when we were able to read about it when DOJ released it in the indictment statement?

Mr. KREBS. Yes, sir. So thank you. That's actually a—I'd hate saying a nuanced answer, because nuance is our enemy here.

The distinction is that the FBI provided investigators to Special Counsel Mueller's investigation. Those investigators have focused on developing the case against Russian operatives. Their information as a result of the investigation stays within the case-building that Special Counsel Mueller has developed.

That has not crossed over the firewall, as it is, into the rest of the administration. So there were details within that indictment that I had not seen before.

Now, that is not to say that if they had found something about an imminent attack that they wouldn't have shared, because they would have.

Mr. CONNOLLY. Well, let me—so your department was kept out of the loop by the Department of Justice.

Mr. KREBS. By Special Counsel Mueller's investigation. They had an investigation to conduct on past activities. I have information sufficient to work with the various secretaries of State and the county officials to provide them cybersecurity expertise.

Mr. CONNOLLY. So, according to that indictment, in July of 2016, Anatoliy Kovalev, a Russian intelligence officer, and his co-conspirators, quote, hacked the website of a State board of elections and stole information related to approximately a half a million voters in that State, including their names, addresses, partial Social Security numbers, dates of birth, and driver's license numbers.

Were you aware of that fact before the indictment?

Mr. KREBS. Sir, I was aware of the fact that there was a State board of elections that was compromised by the Russians. It's in the intelligence community assessment. That, as I understand, is the State of Illinois. So we have been working closely with Illinois since 2016, frankly, on the incident.

Mr. CONNOLLY. So, presumably, you could have answered our queries about documents, going back to October, at least with respect to this, since you knew about it and you knew the State, which was not identified, I believe, in the indictment.

Mr. KREBS. That is correct, sir, but Illinois has come forward and said that they believe that they are——

Mr. CONNOLLY. Right.

Mr. KREBS. —the victim. And they have also said that, yes, they were the State in the IC——

Mr. CONNOLLY. But couldn't you have been responsive to our outstanding document request at least with respect to this?

Mr. KREBS. Sir, I need to go back and look at the information we've provided. I know that we have provided a number of classified and unclassified briefings to the Congress that has included that information.

Mr. CONNOLLY. Well, I guess I'm being a little more specific. There have been document requests by members of this committee. This is the committee of oversight in the United States Congress.

Mr. KREBS. Yes, sir.

Mr. CONNOLLY. And, gosh, I remember—maybe you do too, Mr. Cummings and Mr. Gowdy—I mean, all kinds of times in the previous administration when, even though there might have been tens of thousands of pages of documents provided, that was often not adequate, and threats of contempt and subpoenas were issued because the entirety of the document request had not been met, for whatever reason.

Lord, I seem to remember excoriating, for example, the former IRS Commissioner, John Koskinen, in that regard. Even though he sometimes had difficulty in producing the documents we wanted, that didn't matter.

But, in your case, we've got outstanding requests going back to October. And I—well, let me ask you this: Are you prepared to promise at this hearing that you will cooperate with document requests to the best of your ability going forward?

Mr. KREBS. I have always made that pledge, and I will continue to do so, yes, sir.

Mr. CONNOLLY. All right. Because we're probably going to want to know more about the Illinois case and whether there were other States like that.

Mr. KREBS. Yes, sir.

Mr. CONNOLLY. Okay. Because I know my own home State of Virginia was also probed by these—and final point.

Mr. Hatch, I can't resist, having been in local government. I really appreciated the point you made in your opening statement about local governments. So much of Congress is always focused at the statewide level. Maybe that's because so many of my colleagues come from State legislatures. And they forget that the implementer is local government.

And I think you were the making the point that most local governments are kind of on their own in running elections. They don't get—I don't know whether New Mexico provides its local governments with a lot of assistance. Virginia does not. And so we have to finance our machines. We have to finance a lot of our elections.

And so, when you make big changes, it's a big burden on local governments, and some are better able to absorb that cost than others. I really appreciate that point being made, because I think that escapes a lot of us in Congress, and that's a very salient fact, as we look at reform or tightening up or protecting from cyber attacks.

If the chairman will allow Mr. Hatch to react to that if he wishes, and then I yield back.

Mr. HATCH. Thank you, Mr. Chairman.

And thank you for those comments. We want to put the "local" back in the "State and local" statement.

The good news is States and locals are working together. I have great experience from the State of Utah working with our State, and then other individuals such as Secretary Toulouse Oliver and the efforts that they have been doing. It's not perfect. We're not

there yet. But we really appreciate working with our State partners.

But, yes, you're correct. In virtually every State, it's the local election administrators who have the boots on the ground that are running the day-to-day operations.

Thank you.

Mr. GOWDY. The gentleman from Virginia yields back.

I'll ask my questions last. I want to start by thanking all four of you for your expertise and your comity with one another and also with the members of the committee.

I want to start by addressing some of my colleagues' concerns, because I think they do warrant being addressed. If I understood the concerns earlier in this hearing, it was kind of two-part. Number one, they want an investigation into what Russia did, and they would prefer that that investigation be public.

I'm sure some of my colleagues are aware of this, but for those who are not in Congress, those who may be watching, those who may be reading, I spent the better part of 2017 in a SCIF interviewing more than 70 witnesses on what Russia did to this country.

And I get that some of my colleagues want every single committee of Congress to look into the fact pattern, including the Small Business Administration Committee, including Natural Resources—they want every committee of Congress. But the reality is, given the sensitive nature of this information, that investigation is best handled in a confidential setting, which is where the House Intelligence Committee meets. It's where we met for the better part of 2017. It's where the Senate Intelligence Committee is currently meeting. And they will issue a report.

And it is not lost on me, and perhaps it won't be lost on our four witnesses, there have been a number of references this morning to the indictments that have been issued by the grand jury in the Mueller probe. Anyone sit through the grand jury proceedings? Anyone got a problem with the fact that you didn't sit through the grand jury proceedings? Anyone sat in on any of Bob Mueller's interviews? Any of you have a problem with the fact that you haven't sat in on any of Bob Mueller's interviews?

Everything can't be done in public. We had the most productive classified briefing, I think, that I have ever been part of last week. I really wish my fellow citizens could've participated in it. I wish they could have heard what Inspector General Horowitz told both sides, not just this committee but also Judiciary. Because if you heard what he said, you would not view this as a partisan issue. You would view it as the United States of America was attacked.

So I hope at some point the light of day can be shown on all of what happened in 2016. But I'd just caution my fellow citizens, they do not have any issue with the fact that in every one of their local jurisdictions somewhere some investigation is being done confidentiality, whether it's a grand jury, whether it's deliberations by a petit jury, whether it's deliberations by an appellate court in their State, and they don't have a problem with the fact that certain things are done in confidence.

And when it comes to not tipping off our adversaries as to what we know and how we know it and what we are doing to guard

against it in the future, if there's ever an argument for things to be done in confidence, I think that is the best argument.

Having said that, Madam Secretary, I do not know when you became the secretary of State, so let me start by asking, in 2016, were you in your current position?

Ms. TOULOUSE OLIVER. No, sir, but I was the county clerk in the largest county in New Mexico.

Mr. GOWDY. All right. Well, it would not be fair for me to ask you this question, but to the extent you have any information, I do want you to weigh in.

I never really understood why Jeh Johnson was criticized in 2016, the former DHS Secretary. Elections are predominantly State and local matters, and the notion that he, as a Federal Cabinet-level official, was supposed to summarily decide to inject himself in the 2016 elections I don't think was fair to Jeh.

But there was a decision made in January 2017 to declare our election infrastructure a critical infrastructure. Can any of the four of you address why the decision was not made in the fall of 2016 but it was made in January of 2017?

Not all at once.

Mr. KREBS. That predates my time at the Department.

I'll just add, though, that the way I look at election infrastructure, it is a national critical function. It is essential to the functioning of this government. And the Department of Homeland Security will continue to support State and local governments.

Mr. GOWDY. I guess the reason I've started off by saying, I really wish—I mean, I get that the other 364 days out of the year we're going to quarrel about who should be elected. I would like this to be the 1 day that we just quarrel about making sure the person who is elected actually serves.

So we haven't had hearings about what President Trump discussed with Vladimir Putin, just like we haven't had hearings about what President Obama discussed with Vladimir Putin while the hacking was going on in 2016. We've had no hearings on that.

Madam Secretary of State, final question, because I'm out of time. There are a lot of ways to count votes. The Senate does it. You have to show up in person. The House, you have to show up in person but use a voting card. My wife is a first-grade schoolteacher. They use a combination of raising their hands and voice vote, based on decibel rather than people. So there are a lot of ways to vote.

What, in your judgment, is the safest, most secure way to vote, even accepting that our friends in the media may not know within 45 minutes of the polls closing who won? If you're interested in making absolutely sure it is safe, secure, and, therefore, reliable, what is the safest way to cast a ballot?

Ms. TOULOUSE OLIVER. So it's important to emphasize that every State utilizes the system that's right for them. And, even within those States, some jurisdictions use slightly different systems. So making sure that you're utilizing a system that voters are comfortable with and have confidence in is extremely important.

With that being said, in my personal opinion, the use of paper ballots is absolutely critical, because you have a paper and a voter-verifiable backup at the end of the day. If there's ever a question

as to whether your tabulators were tampered with, your election night reporting system, you are always able to go back and reconstruct the election on the back end utilizing that paper system.

So that, in my opinion, Mr. Chairman, is the safest and most secure way to conduct an election. But with that being said, every State has security and resiliency plans for whatever system they are using, and every State is absolutely, 100-percent dedicated to making sure those systems are protected.

Mr. GOWDY. I know it's a multifactorial analysis. You want to incent people to vote. You want to make it as easy for them as you can. There, obviously, is a speed element. People don't want to wait 3 weeks to see whether or not they won or lost an election.

But in terms of safety, security, reliability, knowing that the person who received the most number of votes actually was elected, in your judgment, at least for New Mexico, that is done with paper ballots.

Ms. TOULOUSE OLIVER. Yes, sir, that's correct.

Mr. GOWDY. All right.

I am out of time, but I was not the only one this morning who went over.

I want to thank our witnesses again for appearing before us today, and I really mean that. I appreciate your expertise. I appreciate your public service even in a sometimes trying environment.

The hearing record will remain open for 2 weeks for any member to submit a written opening statement or questions for the record.

The gentleman from Maryland.

Mr. CUMMINGS. Mr. Krebs, you know, my heart wouldn't let me get out of here without me telling you this. Don't play with us. You said that you read the letter this morning about our request. And time is short.

You know, back when Muhammad Ali was fighting, they used to do something called the rope-a-dope. And I feel like you rope-a-doped us a bit this morning. I'm just telling you how I feel. And it's quite—you know, I wanted to walk out of the room and not say anything, but my heart won't let me do that.

Would you please give us the documents and don't play with us? I'm not—you know, we're asking for something that is reasonable. We're simply trying to do our job. You know, I know you said you've done all these briefings and whatever. Can you let us know when we're going to get the documents?

Mr. KREBS. Sir, I need to go actually look and see what documents we haven't provided that you're still looking for.

Mr. CUMMINGS. Okay.

Mr. KREBS. I have a job to do as well, and my job is to be as transparent as possible with——

Mr. CUMMINGS. Right. That's——

Mr. KREBS. —this body——

Mr. CUMMINGS. There you go.

Mr. KREBS. —and I'm doing it.

Mr. CUMMINGS. That's what I want.

Mr. KREBS. I'm doing it.

Mr. CUMMINGS. Yeah, I want you to be as transparent as possible. And I don't believe, to date, that has been the case. I'm just telling you.

Mr. KREBS. I apologize for that impression, but that has not been my goal. That has not been the direction I've provided my team.

Mr. CUMMINGS. Wonderful. Wonderful. I hope your team is listening so we have now an opportunity to correct that, now that we—we'll start with a new page today.

And let me tell you the reason why I mention the rope-a-dope. The Congress is only going to be in session for a little while, this week basically. Then we are out for August. We've got an election in Maryland—well, all over the country in November. So, I mean, time is of the essence.

And so I'm hoping that your staff will sit down with our staff, and I'm talking about bipartisan, and go over these—get us the documents that we want. Okay?

Mr. KREBS. You have that commitment. This all rolls up to me. I'm responsible.

Mr. CUMMINGS. It's all what?

Mr. KREBS. It all rolls up to me. I'm going to get you what you need.

Mr. CUMMINGS. Thank you very much.

And thank all of you for your testimony. It's been quite helpful.

Mr. GOWDY. The hearing record will remain open for 2 weeks for any member to submit a written opening statement or questions for the record.

Mr. GOWDY. If there's no further business, without objection, the committee stands adjourned.

[Whereupon, at 12:59 p.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

MOTION TO ISSUE SUBPOENA TO DAN COATS

Mr. Connolly moves that the Oversight and Government Reform Committee, pursuant to House Rule XI clause 2(k)(6), authorize and issue the attached subpoena to Dan Coats.

SUBPOENA

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES OF THE CONGRESS OF THE UNITED STATES OF AMERICA

Director of National Intelligence, Dan Coats

To _____

You are hereby commanded to be and appear before the

Committee on Oversight and Government Reform

of the House of Representatives of the United States at the place, date, and time specified below.

☐ **to produce the things identified on the attached schedule** touching matters of inquiry committed to said committee or subcommittee; and you are not to depart without leave of said committee or subcommittee.

Place of production: _____

Date: _____ Time: _____

☐ **to testify at a deposition** touching matters of inquiry committed to said committee or subcommittee; and you are not to depart without leave of said committee or subcommittee.

Place of testimony: _____

Date: _____ Time: _____

☑ **to testify at a hearing** touching matters of inquiry committed to said committee or subcommittee; and you are not to depart without leave of said committee or subcommittee.

Place of testimony: Room 2154, Rayburn House Office Building

Date: July 26, 2018 Time: 10 am

To any authorized staff member or the U.S. Marshals Service

to serve and make return.

Witness my hand and the seal of the House of Representatives of the United States, at the city of Washington, D.C. this 24th day of July, 2018.

_____
Chairman or Authorized Member

Attest:

_____
Clerk

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
115TH CONGRESS
RATIO 24-18
ROLL CALL

Vote on: **Meadows Motion to Table the Connolly Motion**
Date: **Tuesday, July 24, 2018** **VOTE #: 1**

Republicans	Aye	No	Present	Democrats	Aye	No	Present
MR. GOWDY (SC) *(Chairman)*	X			MR. CUMMINGS (MD) *(Ranking)*	X		
MR. DUNCAN (TN)				MS. MALONEY (NY)	X		
MR. ISSA (CA)				MS. NORTON (DC)	X		
MR. JORDAN (OH)	X			MR. CLAY (MO)	X		
MR. SANFORD (SC)				MR. LYNCH (MA)	X		
MR. AMASH (MI)				MR. COOPER (TN)			
MR. GOSAR (AZ)	X			MR. CONNOLLY (VA)	X		
MR. DesJARLAIS (TN)				MS. KELLY (IL)			
MS. FOXX (NC)	X			MS. LAWRENCE (MI)	X		
MR. MASSIE (KY)	X			MS. WATSON COLEMAN (NJ)	X		
MR. MEADOWS (NC)	X			MR. KRISHNAMOORTHI (IL)	X		
MR. DeSANTIS (FL)	X			MR. RASKIN (MD)	X		
MR. ROSS (FL)				MR. GOMEZ (CA)	X		
MR. WALKER (NC)	X			MR. WELCH (VT)	X		
MR. BLUM (IA)	X			MR. CARTWRIGHT (PA)			
MR. HICE (GA)	X			MR. DeSAULNIER (CA)	X		
MR. RUSSELL (OK)				MS. PLASKETT (VI)	X		
MR. GROTHMAN (WI)	X			MR. SARBANES (MD)	X		
MR. HURD (TX)	X						
MR. PALMER (AL)	X						
MR. COMER (KY)	X						
MR. MITCHELL (MI)	X						
MR. GIANFORTE (MT)	X						
MR. CLOUD (TX)	X						

Roll Call Totals: Ayes: 17 Nays: 15 Present:

Passed: X Failed: _____ (REVISED 3/14/18)

For the record

FOR IMMEDIATE RELEASE

July 23, 2018

Contact: David Carl

(505) 288-2465

AG Balderas to Congressional Leaders: "Protect the Integrity of our Elections. Our Democracy Depends on it."

Albuquerque, NM – Today, Attorney General Hector Balderas led a bipartisan coalition of 21 Attorneys General in urging congressional leaders to improve American cyber security and protect the integrity of the upcoming 2018 midterm election, and elections to come, against cyberattacks and infiltrations like the ones committed by Russia in 2016. The latest investigations into that attack shows Russian hackers targeted the American electoral system, stole the private information of hundreds of thousands of people, and infiltrated a company that supplies voting software across the nation, putting the upcoming election at serious risk. These investigations led to the indictment of 12 Russian Intelligence Officers earlier this month.

"The intelligence could not be more clear," said Attorney General Hector Balderas. "In 2016, Russian hackers infiltrated state and local election boards, and stole the sensitive voter information of more than 500,000 Americans. This cannot happen again. It is the vital responsibility of Congressional leaders to safeguard our elections, and prevent yet another dangerous cyber-attack. Nothing short of the fabric of our democracy is at stake."

The coalition of AG's urged three steps in addressing election security concerns.

Prioritizing and acting on election-security legislation. We understand that the Secure Elections Act (S.2261) is before the Senate at this time and may address some of our concerns.

Increasing funding for the Election Assistance Commission to support election security improvements at the state level and to protect the personal data of the voters of our states. Many states lack the resources and tools they need to protect the polls during this year's upcoming elections. Additional funding for voting infrastructure will not only allow states to upgrade election systems, but will also allow for a comprehensive security risk assessment. Unfortunately, past practice has shown that the existing Election Assistance Commission grants are simply insufficient to provide for the upgraded technology needed. More funding is essential to adequately equip states with the financial resources we need to safeguard our democracy and protect the data of voting members in our states.

Supporting the development of cybersecurity standards for voting systems to prevent potential future foreign attacks. It is critical that there be a combined effort between governments and security experts to protect against the increased cyber threats posed by foreign entities seeking to weaken our institutions.

Protecting the integrity of the American voting system is a vital, bipartisan issue, reflected in the bipartisan nature of the Attorneys General joining AG Balderas. In addition to New Mexico, this coalition includes Attorneys General from California, Connecticut, Delaware, The District of Columbia, Hawaii, Illinois, Iowa, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, New Jersey, New York, North Carolina, Oregon, Rhode Island, Virginia and Washington.

A copy of the letter is attached below.

STATE OF NEW MEXICO
OFFICE OF THE ATTORNEY GENERAL

HECTOR H. BALDERAS
ATTORNEY GENERAL

July 23, 2018

House Homeland Security Committee
Chairman Michael McCaul
2001 Rayburn House Office Building
Washington, DC 20515

Senate Rules and Administration Committee
Chairman Roy Blunt
260 Russell Senate Office Building
Washington, DC 20510

Dear Honorable Committee Members:

The undersigned Attorneys General write to express our grave concern over the threat to the integrity of the American election system. As the latest investigations and indictments make clear, during the 2016 election, hackers within Russia's military intelligence service not only targeted state and local election boards, but also successfully invaded a state election website to steal the sensitive information of approximately 500,000 American voters and infiltrated a company that supplies voting software across the United States.

The allegations in these indictments are extremely troubling. They evidence technologically vulnerable election infrastructures and the existence of a malicious foreign actor eager to exploit these vulnerabilities. Moreover, it has never been more important to maintain confidence in our democratic voting process. It is imperative that we protect the integrity of our elections. We must ensure that the upcoming 2018 midterm elections are secure and untainted. Accordingly, we ask for your assistance in shoring up our systems so that we may protect our elections from foreign attacks and interference by:

- Prioritizing and acting on election-security legislation. We understand that the *Secure Elections Act* (S.2261) is before the Senate at this time and may address some of our concerns.

- Increasing funding for the Election Assistance Commission to support election security improvements at the state level and to protect the personal data of the voters of our states. We are concerned that many states lack the resources and tools they need to protect the polls. Additional funding for voting infrastructure will not only allow states to upgrade election systems, but will also allow for a comprehensive security risk assessment. Unfortunately, past practice has shown that the existing Election Assistance Commission grants are simply insufficient to provide for the upgraded technology needed. More

funding is essential to adequately equip states with the financial resources we need to safeguard our democracy and protect the data of voting members in our states.

- Supporting the development of cybersecurity standards for voting systems to prevent potential future foreign attacks. It is critical that there be a combined effort between governments and security experts to protect against the increased cyber threats posed by foreign entities seeking to weaken our institutions.

These changes are essential in order to strengthen public trust in our electoral system. The integrity of the nation's voting infrastructure is a bipartisan issue, and one that affects not only the national political landscape, but elections at the state, county, municipal, and local levels. It is our hope that you agree, and will take swift action to protect our national legacy of fair and free elections.

Respectfully,

Hector Balderas
Attorney General of New Mexico

Xavier Becerra
Attorney General of California

George Jepsen
Attorney General of Connecticut

Matthew P. Denn
Attorney General of Delaware

Karl Racine
Attorney General for the District of Columbia

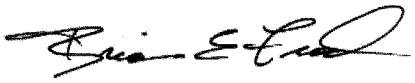
Russell Suzuki
Attorney General of Hawaii

TELEPHONE: (505)490-4060 FAX: (505)490-4883 www.nmag.gov
MAILING ADDRESS: P.O. BOX 1508 - SANTA FE, NEW MEXICO 87504-1508
STREET ADDRESS: 408 GALISTEO STREET - SANTA FE, NEW MEXICO 87501

Lisa Madigan
Attorney General of Illinois

Thomas J. Miller
Attorney General of Iowa

Janet Mills
Attorney General of Maine

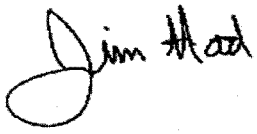


Brian Frosh
Attorney General of Maryland

Maura Healy
Attorney General of Massachusetts

Bill Schuette
Attorney General of Michigan

Lori Swanson
Attorney General of Minnesota

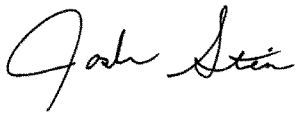


Jim Hood
Attorney General of Mississippi

Gurbir Grewal
Attorney General of New Jersey

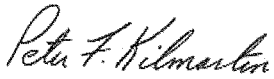
Barbara D. Underwood
Attorney General of New York

TELEPHONE: (505)490-4060 FAX: (505)490-4883 www.nmag.gov
MAILING ADDRESS: P.O. BOX 1508 - SANTA FE, NEW MEXICO 87504-1508
STREET ADDRESS: 408 GALISTEO STREET - SANTA FE, NEW MEXICO 87501

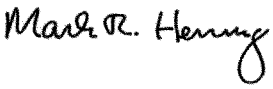


Josh Stein
Attorney General of North Carolina

Ellen Rosenblum
Attorney General of Oregon



Peter F. Kilmartin
Attorney General of Rhode Island



Mark R. Herring
Attorney General of Virginia

Bob Ferguson
Attorney General of Washington

TELEPHONE: (505)490-4060 FAX: (505)490-4883 www.nmag.gov
MAILING ADDRESS: P.O. BOX 1508 - SANTA FE, NEW MEXICO 87504-1508
STREET ADDRESS: 408 GALISTEO STREET - SANTA FE, NEW MEXICO 87501

TREY GOWDY, SOUTH CAROLINA
CHAIRMAN

ONE HUNDRED FIFTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

http://oversight.house.gov

October 20, 2017

The Honorable Robert Kolasky
Acting Deputy Under Secretary
National Protections and Programs Directorate
Department of Homeland Security
Washington, DC 20528

Dear Acting Deputy Under Secretary Kolasky:

Last month, the Department of Homeland Security reportedly notified election officials in 21 states that Russian government hackers had targeted those states during the 2016 election.[1] We are writing to request copies of these notifications and additional documents, as well as a briefing from top Department officials on these matters.

The Department's notifications to these states came nearly a year after the election and three months after the Department publicly disclosed that individuals connected with the Russian government sought to hack voter registration files and public election sites in 21 states.[2] They also came after numerous other reports that Russia engaged in a multifaceted campaign to disrupt the 2016 election, including widespread cyber-attacks on state-election infrastructure systems.[3]

The Department's recent convening of the Government Coordinating Council for the Election Infrastructure Subsector, with representatives from the Election Assistance Commission, the National Association of Secretaries of State and state and local election officials, will hopefully facilitate the sharing of information and expertise.[4]

---

[1] *DHS Tells States About Russian Hacking During 2016 Election,* Washington Post (Sept. 22, 2017) (online at www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html?utm_term=.55b916d66ca3).

[2] *Russians Tried to Hack Election Systems in 21 States, U.S. Officials Say*, Chicago Tribute (June 21, 2017) (online at www.chicagotribune.com/news/nationworld/ct-homeland-security-chief-intelligence-panel-20170621-story.html).

[3] *See, e.g.*, Department of Homeland Security, *Joint Analysis Report: GRIZZLEY STEPPE—Russian Malicious Cyber Activity* (Dec. 29, 2016) (online at www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf); Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* (Jan. 6, 2017) (online at www.dni.gov/files/documents/ICA_2017_01.pdf).

[4] Department of Homeland Security, *DHS and Partners Convene First Election Infrastructure Coordinating Council* (Oct. 14, 2017) (online at www.dhs.gov/news/2017/10/14/dhs-and-partners-convene-first-election-infrastructure-coordinating-council).

We request that you produce, by October 31, 2017, copies of the notifications sent by the Department to these 21 states, as well as all accompanying materials relating to Russian government-backed attempts to hack state election systems.

We also request a briefing from appropriate Department officials within the same timeframe on the following issues:

(1) the types of voting equipment that were attacked;
(2) the timeline by which the Department provided information to these states and the reasons for not sharing additional information sooner;
(3) services and trainings offered to states to detect and prevent cyber-attacks;
(4) plans to work with states to detect and prevent future cyber-attacks; and
(5) the operational plans and goals of the newly convened Election Infrastructure Coordinating Council.

If you have any questions, please contact Jennifer Daehn with the Democratic Committee staff at (202) 225-5051. Thank you for your consideration of this request.

Sincerely,

Elijah E. Cummings
Ranking Member
Committee on Oversight and
Government Reform

Robin Kelly
Ranking Member
Subcommittee on
Information Technology

cc: The Honorable Trey Gowdy, Chairman
Committee on Oversight and Government Reform

The Honorable Will Hurd, Chairman
Subcommittee on Information Technology

TREY GOWDY, SOUTH CAROLINA
CHAIRMAN

ONE HUNDRED FIFTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

http://oversight.house.gov

January 3, 2018

The Honorable Christopher C. Krebs
Senior Official Performing the Duties of the Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security
245 Murray Lane SW
Washington, DC 20528

Dear Mr. Krebs:

Enclosed are post-hearing questions that have been directed to you and submitted to the official record for the hearing that was held on November 29, 2017, titled "Cybersecurity of Voting Machines."

In order to ensure a complete hearing record, please return your written response to the Committee on or before January 19, 2018, including each question in full as well as the name of the Member. Your response should be addressed to the Committee office at 2157 Rayburn House Office Building, Washington, DC 20515. Please also send an electronic version of your response by e-mail to Sharon Casey, Deputy Chief Clerk, at Sharon.Casey@mail.house.gov.

Thank you for your prompt attention to this request. If you need additional information or have other questions, please contact Troy Stock at (202) 225-5074.

Sincerely,

Will Hurd
Chairman
Subcommittee on Information Technology

Gary J. Palmer
Chairman
Subcommittee on Intergovernmental Affairs

cc: The Honorable Robin L. Kelly, Ranking Member
Subcommittee on Information Technology

The Honorable Val Butler Demings, Ranking Member
Subcommittee on Intergovernmental Affairs

Enclosure

Question for Christopher Krebs
Senior Official Performing the Duties of the Under Secretary
National Protection & Programs Directorate
Department of Homeland Security

Ranking Members Robin Kelly and Val Demings
Subcommittee on Information Technology and Intergovernmental Affairs
Committee on Oversight and Government Reform
Hearing on "Cybersecurity of Voting Machines"

November 29, 2017

At the hearing, Rep. Kelly introduced into the record a letter she sent on October 20, 2017, with Ranking Member Elijah Cummings. The letter requested "copies of the notifications" the Department of Homeland Security (DHS) provided to 21 states reportedly targeted by Russian hacking efforts. The letter also requested copies of all documents "related to the Russian government-backed attempts to hack state election systems." Attached is a copy of the letter that Rep. Kelly introduced into the record.

According to press reports, the following states received notifications from DHS that they were identified as targets: Washington, Oregon, California, Colorado, Illinois, Alaska, Arizona, Oklahoma, Texas, North Dakota, Minnesota Wisconsin, Iowa, Ohio, Alabama, Florida, Pennsylvania, Virginia, Maryland, Connecticut, and Delaware.[1]

On the day before the hearing, DHS produced only an email with a short script that DHS employees apparently read over the phone to state election officials. It is only 13 sentences long and does not refer to any specific state or attack. Rather, it is a generic script that provides no specific information.

DHS has yet to produce any of the other requested documents.

1. Please immediately produce copies of all documents related to the Russian government-backed attempts to monitor, penetrate, or hack state election systems during the presidential election campaign of 2016, including but not limited to the tools the attackers used, the tactics they utilized, the results of your conversations with these states, and the steps you took to follow-up.

2. For each of the 21 states, please provide details of your notification to state officials of the attempted cyberattacks, including:

    - the date of the notification;

---

[1] *What We Know about the 21 States Targeted by Russian Hackers*, Washington Post (Sept. 23, 2017) (online at www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?utm_term=.776577e66d8a).

- the names of the state officials or offices that were notified;
- the name of the DHS division that provided the notification;
- whether it was a telephonic notification, or by other means;
- services offered during the notification; and
- the dates of any subsequent communications relating to cyberattacks with state officials.

3. Did DHS notify any other states that their election infrastructure had been targeted by cyberattacks in 2016? If so, please provide similar details of your notifications to those States, using the format above.

TREY GOWDY, SOUTH CAROLINA
CHAIRMAN

ONE HUNDRED FIFTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

Majority (202) 225-5074
Minority (202) 225-5051

http://oversight.house.gov

January 29, 2018

The Honorable Trey Gowdy
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman,

We are writing to request that you issue a subpoena to finally compel the Department of Homeland Security to produce documents it has been withholding from Congress for months relating to Russian government-backed efforts to monitor, penetrate, or otherwise hack at least 21 state election systems in the 2016 election.

Despite repeated requests over the past several months, the Department has refused to provide the Oversight Committee with this information, and to the best of our knowledge, has not provided it to any congressional committee. We have been extremely patient, but we can no longer allow the Trump Administration to defy our requests and withhold this critical information from Congress. The Intelligence Community has warned us that Russia intends to continue interfering with elections in the United States and around the world. It is our responsibility to obtain information about what happened in 2016 so we can adequately prepare for future attempts to interfere with our democracy.

If you decline to issue this subpoena yourself, then we request that you allow Committee Members to debate and vote on a motion to subpoena the Department for these documents at our next regularly-scheduled business meeting.

Multiple Requests Refused by Department of Homeland Security

According to press reports, the Department notified the following 21 states that they were identified as targets of Russian government-linked hacking attempts into their election systems: Washington, Oregon, California, Colorado, Illinois, Alaska, Arizona, Oklahoma, Texas, North Dakota, Minnesota, Wisconsin, Iowa, Ohio, Alabama, Florida, Pennsylvania, Virginia, Maryland, Connecticut, and Delaware.[1]

---

[1] *See, e.g., What We Know About the 21 States Targeted by Russian Hackers*, Washington Post (Sept. 23, 2017) (online at www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?utm_term=.776577e66d8a).

On October 20, 2017, Ranking Member Elijah E. Cummings and Information Technology Subcommittee Ranking Member Robin Kelly sent a letter requesting "copies of the notifications" the Department provided to these states, as well as copies of all documents "related to the Russian government-backed attempts to hack state election systems." They requested these documents by October 31, 2017.[2]

In response, the Department produced just one e-mail with a short script that Department employees apparently read over the phone to state election officials. This script is 13 sentences long and does not refer to any specific state or attack. Rather, it is a generic script that provides no specific information.[3]

On November 29, 2017, during a joint subcommittee hearing on the "Cybersecurity of Voting Machines," Ranking Member Kelly questioned Christopher Krebs, the Senior Official Performing the Duties of the Under Secretary of the National Protection and Program Directorate. Ranking Member Kelly introduced into the official hearing record the request letter from October 20, 2017, and asked Mr. Krebs when these documents would be provided. Although Mr. Krebs assured Ranking Member Kelly that a response would be forthcoming, no further documents were provided.[4]

During the hearing, Mr. Krebs seemed to indicate that he could not provide the requested information because it was provided by the states as part of their "confidential relationship" with the Department. Instead, he suggested that Committee Members "reach back to your states" to obtain the information. He failed to acknowledge that the October 20, 2017, request letter sought information the Department collected from other sources—rather than from the states themselves—including information that led the Department to conclude that these 21 states were at risk, as well as the specific tactics used by Russian government-backed entities.[5]

To follow-up on this request yet again, the Subcommittees sent Mr. Krebs official Questions for the Record on January 3, 2018, that included a request by Ranking Members Cummings and Kelly that the Department produce, by January 19, 2018, the following documents and information:

---

[2] Letter from Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform, and Ranking Member Robin Kelly, Subcommittee on Information Technology, to Robert Kolasky, Acting Deputy Under Secretary, National Protections and Programs Directorate, Department of Homeland Security (Oct. 20, 2017) (online at democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/2017-10-20.EEC%20Kelly%20to%20Kolasky-NPPD%20re%20Cyberattacks%20on%20State%20Election%20Systems.pdf).

[3] Email from Jeffrey Mitchell, Department of Homeland Security, to House Committee on Oversight and Government Reform Staff (Nov. 28, 2017) (online at https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/DHS%20Email%20Response%20to%20EEC%20%26%20Kelly%2010-20-17%20Letter1.pdf).

[4] Subcommittee on Information Technology and Subcommittee on Intergovernmental Affairs, House Committee on Oversight and Government Reform, *Joint Hearing on Cybersecurity of Voting Machines* (Nov. 29, 2017).

[5] *Id.*

1. Please immediately produce copies of all documents related to the Russian government-backed attempts to monitor, penetrate, or hack state election systems during the presidential election campaign of 2016, including but not limited to, the tools the attackers used, the tactics they utilized, the results of your conversations with these states, and the steps you took to follow-up.

2. For each of the 21 states, please provide details of your notification to state officials of the attempted cyberattacks, including:

   - the date of the notification;
   - the names of the state officials or offices that were notified;
   - the name of the DHS division that provided the notification;
   - whether it was a telephonic notification, or by other means;
   - services offered during the notification; and
   - the dates of any subsequent communications relating to cyberattacks with state officials.

3. Did DHS notify any other states that their election infrastructure had been targeted by cyberattacks in 2016? If so, please provide similar details of your notifications to those States, using the format above.

Although the letter transmitting these Questions for the Record was signed by both Subcommittee Chairmen Will Hurd and Gary J. Palmer, the Department has produced none of the requested documents to date.[6]

Request for Subpoena

For the reasons set forth above, we respectfully request that you issue a subpoena to compel the Department to produce, by February 5, 2018, documents concerning the information requested in the Questions for the Record sent to the Department on January 3, 2018.

If you chose not to do so, then we ask that you place this matter on the agenda for our next regularly scheduled business meeting so that all Committee Members will have the opportunity to vote on a motion to issue this subpoena.

---

[6] Letter from Chairman Will Hurd, Subcommittee on Information Technology, House Committee on Oversight and Government Reform and Chairman Gary J. Palmer, Subcommittee on Intergovernmental Affairs, House Committee on Oversight and Government Reform, to Christopher C. Krebs, Senior Official Performing the Duties of the Under Secretary, National Protection and Programs Directorate, Department of Homeland Security (Jan. 3, 2018) (online at democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/Hurd%20Palmer%20to%20DHS%2001-03-18%20QFRs.pdf).

Thank you for your consideration of this request.

Sincerely,

Congress of the United States
Washington, DC 20515

April 10, 2018

The Honorable Paul D. Ryan
Speaker of the House
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Speaker:

We are writing to seek your assistance in obtaining documents that the Trump Administration has been withholding from Congress for months relating to attacks against 21 states before the 2016 election by entities linked to the Russian government.

We have been trying to work through the committee process, but we have faced two obstacles: the Trump Administration is refusing to provide the documents we requested, and Republicans appear to have no interest in compelling the Trump Administration to produce them.

Our goal is not to interfere with the ongoing criminal investigation of the Trump Administration being conducted by Special Counsel Robert Mueller. Our goal is to obtain the documents collected and prepared by our federal agencies about these Russian attacks in order to take concrete steps to help prevent them from happening again. That is our responsibility under the Constitution.

Unfortunately, we are being blocked by Trump Administration officials who refuse to produce these documents to Congress and by Republican Chairmen who refuse to demand them. These actions create the unfortunate perception that House Republicans do not want to obtain these documents relating to the Russian attacks against state election systems.

Numerous Oversight Committee Requests

On October 20, 2017, Rep. Elijah E. Cummings, the Ranking Member of the Committee on Oversight and Government Reform, and Rep. Robin Kelly, the Ranking Member of the Subcommittee on Information Technology, sent a letter to the Department of Homeland Security (DHS) requesting "copies of the notifications" that the Department provided to 21 states, as well as copies of all documents "related to the Russian government-backed attempts to hack state election systems." They requested these documents by October 31, 2017.[1]

---

[1] Letter from Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform, and Ranking Member Robin Kelly, Subcommittee on Information Technology, House Committee on Oversight and Government Reform, to Robert Kolasky, Acting Deputy Under Secretary, National Protections and Programs Directorate, Department of Homeland Security (Oct. 20, 2017) (online at democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/2017-10-20.EEC%20Kelly%20to%20Kolasky-NPPD%20re%20Cyberattacks%20on%20State%20Election%20Systems.pdf).

On November 28, 2017, DHS responded by producing just one e-mail with a short script that Department employees apparently read over the phone to state election officials. This script is 13 sentences long and does not refer to any specific state or attack. Rather, it is a generic script that provides no specific information.[2]

The next day, on November 29, 2017, Christopher Krebs, the Senior Official Performing the Duties of the Under Secretary of the National Protection and Program Directorate at DHS, testified at a joint subcommittee hearing on the "Cybersecurity of Voting Machines." Mr. Krebs assured Committee Members that a further response would be forthcoming.[3]

To follow-up, the Subcommittees sent official Questions for the Record on January 3, 2018, with a request for DHS to produce the following documents and information:

1. Please immediately produce copies of all documents related to the Russian government-backed attempts to monitor, penetrate, or hack state election systems during the presidential election campaign of 2016, including but not limited to, the tools the attackers used, the tactics they utilized, the results of your conversations with these states, and the steps you took to follow-up.

2. For each of the 21 states, please provide details of your notification to state officials of the attempted cyberattacks, including:

   - the date of the notification;
   - the names of the state officials or offices that were notified;
   - the name of the DHS division that provided the notification;
   - whether it was a telephonic notification, or by other means;
   - services offered during the notification; and
   - the dates of any subsequent communications relating to cyberattacks with state officials.

3. Did DHS notify any other states that their election infrastructure had been targeted by cyberattacks in 2016? If so, please provide similar details of your notifications to those States, using the format above.

The letter transmitting these Questions for the Record was signed by both Subcommittee Chairmen Will Hurd and Gary J. Palmer.[4]

---

[2] Email from Jeffrey Mitchell, Department of Homeland Security, to House Committee on Oversight and Government Reform Staff (Nov. 28, 2017) (online at https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/DHS%20Email%20Response%20to%20EEC%20%26%20Kelly%2010-20-17%20Letter1.pdf).

[3] Subcommittee on Information Technology and Subcommittee on Intergovernmental Affairs, House Committee on Oversight and Government Reform, *Joint Hearing on Cybersecurity of Voting Machines* (Nov. 29, 2017).

[4] Letter from Chairman Will Hurd, Subcommittee on Information Technology, and Chairman Gary J. Palmer, Subcommittee on Intergovernmental Affairs, House Committee on Oversight and Government Reform, to Christopher C. Krebs, Senior Official Performing the Duties of the Under Secretary, National Protection and

Having received no response for weeks, all Democratic Members of the Committee sent a letter to Chairman Trey Gowdy on January 29, 2018, requesting that he issue a subpoena to finally compel DHS to produce these documents. If he refused, the Members asked him to allow all Committee Members to debate and vote on a motion to subpoena the Department for these documents at the next regularly-scheduled business meeting.[5] Chairman Gowdy did not respond.

On February 2, 2018, Ranking Member Cummings and Vice Ranking Member Gerald E. Connolly sent another letter to Chairman Gowdy renewing this request and asking for the subpoena motion to be placed on the agenda for the Committee's business meeting on February 6, 2018.[6] Chairman Gowdy did not respond.

On the day of the Committee's business meeting, February 6, 2018, DHS provided approximately 50 pages of documents with information about how Department officials learned about the Russian-backed attacks and communicated with states.[7] Most of the production consisted of publicly available documents. For example, DHS produced a Joint Analysis Report with the FBI entitled "GRIZZLY STEPPE—Russian Malicious Cyber Activity." Although this document was marked "For Official Use Only," DHS released this same document publicly more than a year earlier.[8]

The Trump Administration's response has been woefully inadequate. While there have been classified and unclassified briefings about these Russian-backed attacks, including a classified staff briefing scheduled for this week, we have not received all relevant classified documents about these attacks. We recognize that it is possible that some of these documents fall outside DHS's control. In that case, we would expect DHS to consult with the Intelligence Community or other interagency partners to ensure that we obtain the documents we have requested.

Programs Directorate, Department of Homeland Security (Jan. 3, 2018) (online at democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/Hurd%20Palmer%20to%20DHS%2001-03-18%20QFRs.pdf).

[5] Letter from Ranking Member Elijah E. Cummings et al. to Chairman Trey Gowdy, House Committee on Oversight and Government Reform (Jan. 29, 2018) (online at https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/2018-01-29.OGR%20Dems%20to%20Gowdy%20re%20DHS%20Doc%20Production%20for%20Attacks%20on%20State%20....pdf).

[6] Letter from Ranking Member Elijah E. Cummings and Vice Ranking Member Gerald E. Connolly to Chairman Trey Gowdy, House Committee on Oversight and Government Reform (Feb. 2, 2018) (online at democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/2018-02-02.EEC%20%26%20Connolly%20to%20Gowdy%20re.13%20motions%20for%20Subpoenas.pdf).

[7] Email from Legislative Affairs Advisor for Cybersecurity, Department of Homeland Security, to House Committee on Oversight and Government Reform Staff (Feb. 6, 2018).

[8] Department of Homeland Security and Federal Bureau of Investigation, *GRIZZLY STEPPE—Russian Malicious Cyber Activity* (Dec. 29 2016) (online at www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf).

To our knowledge, the Trump Administration has not provided any Committee in the House of Representatives with these classified documents about Russian-backed attacks against state election systems.

Request for Assistance

The election happened 17 months ago. It is inexcusable that Republican leaders in Congress have done so little to investigate—or address—Russian-backed attacks on our states, despite the fact that we have been asking repeatedly for congressional action on this important matter. We must be able to evaluate the threat that Russia posed—and still poses—but we cannot do our jobs effectively without obtaining the facts.

We have exhausted our efforts at the committee level, and we ask that you now personally intervene to protect the integrity and authorities of the House of Representatives to obtain the documents we need to protect our nation against foreign attacks.

Sincerely,

Elijah E. Cummings
Ranking Member
Committee on Oversight and
Government Reform

Jerrold Nadler
Ranking Member
Committee on the Judiciary

Adam Schiff
Ranking Member
Permanent Select Committee on
Intelligence

Robert A. Brady
Ranking Member
Committee on House Administration

Bennie G. Thompson
Ranking Member
Committee on Homeland Security

Eliot L. Engel
Ranking Member
Committee on Foreign Affairs

cc: The Honorable Trey Gowdy, Chairman
Committee on Oversight and Government Reform

The Honorable Bob Goodlatte, Chairman
Committee on the Judiciary

The Honorable Devin Nunes, Chairman
Permanent Select Committee on Intelligence

The Honorable Gregg Harper, Chairman
Committee on House Administration

The Honorable Michael McCaul, Chairman
Committee on Homeland Security

The Honorable Ed Royce, Chairman
Committee on Foreign Affairs

The New York Times

Inside a 3-Year Russian Campaign to Influence U.S. Voters

By Scott Shane and Mark Mazzetti

Feb. 16, 2018

WASHINGTON — In September, as the first detailed evidence surfaced of Russia's hijacking of social media in the 2016 election, Irina V. Kaverzina, one of about 80 Russians working on the project in St. Petersburg, emailed a family member with some news.

"We had a slight crisis here at work: the F.B.I. busted our activity (not a joke)," she wrote of the project in Russia. "So, I got preoccupied with covering tracks together with the colleagues." She added, "I created all these pictures and posts, and the Americans believed that it was written by their people."

A 37-page indictment, handed up on Friday by a Washington grand jury and charging Ms. Kaverzina and 12 other people with an elaborate conspiracy, showed that she and her colleagues did not, in fact, hide their tracks so well from United States investigators. The charges, brought by Robert S. Mueller III, the special counsel, introduced hard facts to a polarized political debate over Russia's intervention in American democracy, while not yet implicating President Trump or his associates.

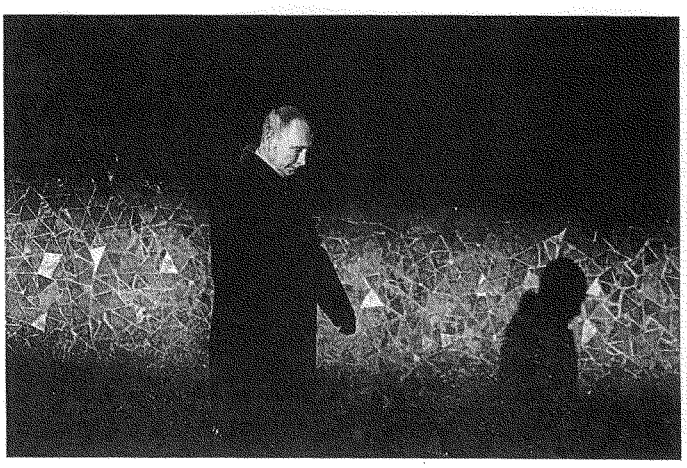
The indictment presented in astonishing detail a carefully planned, three-year Russian scheme to incite political discord in the United States, damage Hillary Clinton's presidential campaign and later bolster the candidacy of Donald J. Trump, along with those of Bernie Sanders and Jill Stein. The precise description of the operation suggested that F.B.I. investigators had intercepted communications, found a cooperating insider or both.

The Russians overseeing the operation, which they named the Translator Project, had a goal to "spread distrust toward the candidates and the political system in general." They used a cluster of companies linked to one called the Internet Research Agency, and called their campaign "information warfare."

The field research to guide the attack appears to have begun in earnest in June 2014. Two Russian women, Aleksandra Y. Krylova and Anna V. Bogacheva, obtained visas for what turned out to be a three-week reconnaissance tour of the United States, including to key electoral states like Colorado, Michigan, Nevada and New Mexico. The visa application of a third Russian, Robert S. Bovda, was rejected.

The two women bought cameras, SIM cards and disposable cellphones for the trip and devised "evacuation scenarios" in case their real purpose was detected. In all, they visited nine states — California, Illinois, Louisiana, New York and Texas, in addition to the others — "to gather intelligence" on American politics, the indictment says. Ms. Krylova sent a report about their findings to one of her bosses in St. Petersburg.

Another Russian operative visited Atlanta in November 2014 on a similar mission, the indictment says. It does not name that operative, a possible indication that he or she is cooperating with the investigation, legal experts said.



President Vladimir V. Putin of Russia has repeatedly denied any government role in hacking and disinformation aimed at the United States. Maxim Shemetov/Reuters

The operation also included the creation of hundreds of email, PayPal and bank accounts and even fraudulent drivers' licenses issued to fictitious Americans. The Russians also used the identities of real Americans from stolen Social Security numbers.

At the height of the 2016 campaign, the effort employed more than 80 people, who used secure virtual private network connections to computer servers leased in the United States to hide the fact that they were in Russia. From there, they posed as American activists, emailing, advising

and making payments to real Americans who were duped into believing that they were part of the same cause.

The playing field was mainly social media, where the Russians splashed catchy memes and hash tags. Facebook has estimated that the fraudulent Russian posts reached 126 million Americans on its platforms alone.

The Russian operatives contacted, among others, a real Texas activist who, evidently assuming they were Americans, advised them to focus on "purple states like Colorado, Virginia & Florida." After that, F.B.I. agents found that the phrase "purple states" became a mantra for the Russian operation.

Clinton Watts, a former F.B.I. agent who has tracked the Russian campaign closely, said that he had no doubt that President Vladimir V. Putin of Russia was behind the effort, which was carried out by companies controlled by his friend and ally, Yevgeny V. Prigozhin. But he noted that the so-called trolls employed by Mr. Prigozhin took elaborate steps to obscure their identities and locations and to avoid leaving government fingerprints.

"From the beginning, they built this so it could be plausibly denied," Mr. Watts said. Mr. Putin has repeatedly denied any government role in hacking and disinformation aimed at the United States, while coyly allowing that patriotic Russians may have carried out such attacks on their own.

Andrew S. Weiss, a Russia specialist at the Carnegie Endowment for International Peace, called the reported origin of the effort in April 2014 "crucially important."

"That's a little more than a month after the annexation of Crimea and the launch of Russia's covert war in eastern Ukraine," Mr. Weiss said. The resulting crisis "vaporized U.S.-Russian relations overnight," he said, setting off multiple Russian efforts "to undermine the United States, both in terms of our leading role in the world, but also via our own domestic political vulnerabilities."

Mr. Weiss said the fact that private companies conducted the social media campaign simply made it cheaper and more difficult to trace.

Mr. Putin has been angry with Mrs. Clinton since at least 2011, when she was secretary of state and he accused her of inciting unrest in Russia as he faced large-scale political protests. Mrs. Clinton, he said, had sent "a signal" to "some actors in our country" after elections that were condemned as fraudulent by both international and Russian observers.

Mr. Mueller's indictment does not present evidence that the campaign overseen by Mr. Prigozhin was ordered by Mr. Putin. American officials have traced other elements of the Russian meddling, notably the hacking and leaking of leading Democrats' emails, to Russian intelligence agencies carrying out Mr. Putin's orders.

While the indictment certainly undermines Mr. Trump's blanket assertions that the Russian interference is a political "hoax," it does not accuse anyone from his campaign or any other American of knowingly aiding in the effort.

By the beginning of 2016, the Russian strategy was in place, and the conspirators began their campaign to sow conflict. An internal message circulated through the Internet Research Agency telling operatives to post content online that focused on "politics in the USA."

"Use any opportunity to criticize Hillary and the rest (except Sanders and Trump—we support them)," the message read.

The scope of the operation was sweeping. The Russians assumed their fake identities to communicate with campaign volunteers for Mr. Trump and grass-roots groups supporting his candidacy. They bought pro-Trump and anti-Clinton political advertisements on Facebook and other social media. They used an Instagram account to try to suppress turnout of minority voters and campaign for Ms. Stein, the Green Party candidate.

Applying nearly two years' worth of political research, the Russians used all of these tactics to target voters in swing states, notably Florida, according to the indictment.

The Internet Research Agency, in St. Petersburg, Russia, was said to be the hub of the operation.
Dmitry Lovetsky/Associated Press

By summer 2016, the Russian operatives were mobilizing efforts for coming "Florida Goes Trump" rallies across the state, all planned for Aug. 20. Using false identities, they contacted Trump campaign staff in Florida to offer their services. One operative sent a message to a campaign official saying that the group Being Patriotic was organizing a statewide rally "to support Mr. Trump."

"You know, simple yelling on the internet is not enough," the message read, according to the indictment. "There should be real action. We organized rallies in New York before. Now we're focusing on purple states such as Florida."

Taking to Facebook, the Russians used the pseudonym Matt Skiber to advertise the rally. "If we lose Florida, we lose America. We can't let it happen, right? What about organizing a YUGE pro-Trump flash mob in every Florida town?" the message read, using one of Mr. Trump's favorite verbal flourishes.

They reached out to local organizations to build momentum for the coming rallies and assign specific tasks.

They paid one unwitting Trump supporter to build a cage on a flatbed truck that housed another person wearing a costume that portrayed Mrs. Clinton in a prison uniform.

After the rallies in Florida, the group applied similar tactics to organize rallies in Pennsylvania, New York and elsewhere.

Weeks before the election, the Russians ratcheted up social media activity aimed at dampening support for Mrs. Clinton.

In mid-October, Woke Blacks, an Instagram account run by the Internet Research Agency, carried the message "hatred for Trump is misleading the people and forcing Blacks to vote Killary. We cannot resort to the lesser of two devils. Then we'd surely be better off without voting AT ALL."

Then, just days before Americans went to the polls, another Instagram account controlled by the Russians — called Blacktivist — urged its followers to "choose peace" and vote for Ms. Stein, who was expected to siphon support from Mrs. Clinton's campaign.

"Trust me," the message read, "it's not a wasted vote."

A version of this article appears in print on Feb. 17, 2018, on Page A1 of the New York edition with the headline: Mueller Chronicles a Social Media War

The ABC News article titled, "Russian Influence Operation Attempted to Suppress Black Vote: Indictment," can be found at: https://abcnews.go.com/Politics/russian-influence-operation-attempted-suppress-black-vote-indictment/story?id=53185084.

ORGANIZATION TRENDS

ACORN Lives!: The Ban on Federal Funding Expires

by Matthew Vadum
NOVEMBER 1, 2010

ACORN Lives!: The Ban on Federal Funding Expires

By Matthew Vadum (*Organization Trends*, November 2010 PDF here)

Summary: ACORN temporarily lost its federal grants and is lying low, but its Project Vote affiliate is still registering voters–even though its leaders are on trial for violating state election laws. The voter mobilization effort is being led by an ACORN official under indictment in Nevada for conspiracy to violate election laws. Project Vote is also working with "rebranded" ACORN state chapters that are waiting to reemerge after the November election. ACORN is expanding overseas to shake down Wal-Mart and other U.S. businesses in emerging markets like India. Will the federal ban on grants to ACORN be renewed? Stay tuned.

Like a zombie in a horror movie, ACORN is *alive*! The Association of Community Organizations for Reform Now staged an elaborate prank on April Fool's Day by pretending to die. That's when chief organizer Bertha Lewis said the group planned to dissolve its national structure. But ACORN remains in business and

Lewis continues to send out direct mail solicitations for funds. (ACORN was profiled in the November 2008 editions of *Foundation Watch* and *Labor Watch*.)

ACORN closed many of its offices, but Lewis is working with a skeleton staff to reorganize the empire of leftist activism. Investigators for the House Oversight and Government Reform Committee say Lewis is consolidating power and hoarding the group's assets. They estimate that ACORN has $20 million in cash in more than 800 bank accounts and that its affiliates hold another $10 million.

While ACORN currently operates below the radar, it plans to resurface under a new name after the upcoming elections, according to activist John Atlas, author of *Seeds of Change*, a book sympathetic to ACORN. Meanwhile, ACORN chapters in at least 13 states and the District of Columbia are changing their names and seeking separate nonprofit status as 501c4 advocacy groups. (*See* ACORN Rebranding Chart at page 5.)

Atlas elaborated on ACORN's plan during a panel discussion in June at the left-wing "America's Future Now" conference. "The good news is that a lot of people who were involved in ACORN, members and leaders as well as their allies, are organizing in over a dozen states to resurrect ACORN using its model, focusing on the same constituency, learning from ACORN's strengths as well as its mistakes. So it is happening."

Project Vote: Amassing Money and Preparing for 2012

Project Vote, ACORN's scandal-plagued voter mobilization division, remains open for business. Project Vote has been part of the ACORN network since at least 1992 when Barack Obama ran its highly successful Illinois voter drive to

elect Democrat Carol Moseley Braun to the U.S. Senate. Project Vote continues to operate out of ACORN's Washington, D.C. headquarters, which earlier this year hosted a meeting at which another "new" ACORN group was organized. The group, Communities United, is active in the District of Columbia and Maryland.

Inside sources say Project Vote is lying low during the current election cycle and plans to return in full force for President Obama's reelection campaign in 2012. Earlier this year I was told that Project Vote was having a banner year despite ACORN's troubles and may be raking in *more* money than in 2008. According to its 2008 tax return, Project Vote (formal name: Voting for America Inc.) received $14,635,002 in contributions and grants that year.

Project Vote says it is working with at least eight groups on voter mobilization drives in battleground states. One of those groups is Pennsylvania Neighborhoods for Social Justice (PNSJ), a "new" group operating out of ACORN's offices on Philadelphia's North Broad Street.

Longtime ACORN national board member Carol Hemingway is on the board of PNSJ and its sister nonprofit, Pennsylvania Communities Organizing for Change (PCOC). Both nonprofits filed their incorporation documents on Jan. 8, 2010.

Not until long after the 2010 elections will we learn whether Project Vote matched its earlier $14 million war chest and how it used the money. That's because nonprofit tax returns generally don't become public until one or two years after they file with the IRS.

Guess Who's Running ACORN's Voter Drive?

Amy Busefink is an ACORN employee who is currently under indictment in Nevada for violating election laws. Guess what? She is leading Project Vote's 2010 get out the vote (GOTV) drive.

Her official Project Vote biography says:

"As Project Vote's Field Director, Amy Busefink is responsible for the development and execution of field activities across Project Vote's many program areas. Working with the Election Administration program, she works to develop field strategies for moving issues in several states, including the preregistration of 16 and 17-year-old citizens and voter registration on high school campuses. Over the last two years, Ms. Busefink has participated in the successful fight against legislation that creates barriers to voters, including photo ID efforts in Missouri. She continues to develop voter participation and voter registration field programs, utilizing new and exciting technology for Get-Out-the-Vote efforts."

The bio adds that Busefink "came to Project Vote as its national voter registration director in June 2006, when she assumed responsibility for Project Vote's 2006 voter registration program." She also "ran field operations for Project Votes [sic] 2008 voter registration program, *which collected 1.1 million applications*." [emphasis added]

Well, yes, ACORN and Project Vote did collect more than one million voter registration applications in 2008, but one detail is missing: 400,000 applications "were rejected by election officials for a variety of reasons, including duplicate registrations, incomplete forms and fraudulent submissions." (New York Times, Oct. 24, 2008)

Why does Project Vote acknowledge on its website that a potential felon is running its GOTV effort? Perhaps ACORN thinks no one will notice that she has been indicted for criminal election law violations in Nevada.

Busefink came to the attention of authorities in October 2008 when Nevada law enforcement officials executed a warrant to seize computers and documents in ACORN's Las Vegas office. In May 2009, Nevada's Attorney General, Catherine Cortez Masto, and Secretary of State Ross Miller, both Democrats, made public voter registration-related charges against two senior ACORN employees—Busefink, ACORN's deputy regional director at the time, and Christopher Edwards, then ACORN's Las Vegas field director. Both were implicated in a massive conspiracy in which they *and* ACORN as a corporate entity were charged with violating election law. Edwards pleaded guilty and has turned state's evidence. At the time of writing, the trial against ACORN and Busefink was scheduled to begin on Nov. 26, 2010.

ACORN complained that the raid was a "stunt" calculated to frustrate efforts to register minority voters. The group further said that it was following strict quality assurance procedures to detect fraudulent registrations, a boast that Las Vegas chief elections officer Larry Lomax called "pathetic." Lomax pointed out that ACORN gave voter registration jobs to 59 inmates from a work-release program and that several of the inmates who were made voter registration supervisors had gone to prison for identity theft.

The state's charges list 26 felony counts of voter fraud and 13 of providing unlawful extra compensation to those registering voters, a practice forbidden under Nevada law because it incentivizes fraud. The complaint says voter registration canvassers were paid between $8 and $9 an hour and that their continued employment was conditioned on registering a quota of 20 voters per shift.

"From July 27 through Oct. 2 ACORN also provided additional compensation under a bonus program called 'Blackjack' or '21+' that was based on the total number of voters a person registered." Canvassers bringing in 21 or more completed forms per day would receive a $5 bonus. The complaint says Edwards created the illegal bonus scheme and that "ACORN timesheets indicate that corporate officers of ACORN were aware of the Blackjack bonus program and failed to take immediate action to stop it."

Starting later this month Project Vote will have some explaining to do.

Groups that Work with Project Vote

Project Vote says that in 2010 it is "working with community-based nonprofit leaders to reach low-propensity voters in Arkansas, Colorado, Connecticut, Florida, Kentucky, Illinois, Michigan, Missouri, Ohio, Pennsylvania, Texas, and Wisconsin."

Besides the rebranded and newly incorporated ACORN group Pennsylvania Neighborhoods for Social Justice, Project Vote's partner groups this year are the Colorado Progressive Coalition, Florida Consumer Action Network, Jobs with Justice, Michigan Forward, Missouri ProVote, Ohio Voice, and Wisconsin Voices. They represent a cross-section of the kind of groups that will do whatever it takes to expand the base of left-wing voters.

**Colorado Progressive Coalition*

A well-organized and well-funded infrastructure of "progressive" organizations is responsible for Republicans' fall from power in Colorado, reports former state representative Rob Witwer in his book ***The Blueprint: How the Democrats Won Colorado (and Why Republicans Everywhere Should Care). The*** Colorado Progressive Coalition is an important part of that infrastructure. Big donors to the group include the Tides Foundation ($302,500 since 2001), Needmor Fund ($180,000 since 1999), and Gill Foundation ($174,800 since 2003).

*Florida Consumer Action Network (FCAN)

FCAN is another left-leaning but much smaller state coalition of grassroots groups affiliated with the Consumer Federation of America and US Action. The group insists that voter fraud is a myth. "It just simply does not happen" said FCAN director Bill Newton, who argues that requiring people to produce identification when they vote is racist. "The intent is keeping certain people from voting," he has said. FCAN is an active supporter of Florida Amendments 5 and 6, ballot initiatives funded by liberal special interests, including ACORN, to redraw state legislative districts.

*Jobs with Justice Education Fund

This front group for organized labor reports $1.6 million in 2009 annual revenue, which allows director Sarita Gupta to organize protests and demonstrations against "corporate greed." It lists as "Friends & Allies" ACORN, the late Saul Alinsky's Industrial Areas Foundation, Rev. Jim Wallis's Sojourners magazine, the Association of Trial Lawyers of America, and the small 'c' communist National Lawyers Guild and Center for Constitutional Rights.

Big JwJ funders include the Ford Foundation ($1,780,000 since 2002), Rockefeller Foundation ($1,685,000 since 2000), and the Nathan Cummings Foundation ($1 million since 2001). The Woods Fund of Chicago, whose past board members include Barack Obama and Bill Ayers, has given Jobs with Justice $60,000 since 2005.

*Michigan Forward

Founded in Detroit in 2008, Michigan Forward aims to be an urban think tank, an unlikely partner in Project Vote's GOTV drive. In late 2009 it reported it had not yet received tax-exempt status from the IRS.

*Missouri ProVote

ACORN is listed as a "board member" on the 2008 tax return of the Missouri Progressive Voter Coalition, coalition of 40 community groups and labor unions. Other board members include Americans for Democratic Action, Planned Parenthood, and units of AFSCME, the American Federation of Teachers, Communications Workers of America, SEIU, and the Teamsters. The Tides Foundation has given Missouri ProVote $20,000 since 2000.

Like ACORN, Missouri ProVote is a magnet for vote fraud felons and political extremists. Deidra Humphrey, who registered voters for ACORN and Missouri ProVote in 2008, was convicted of mail fraud for forging voter registration cards for nursing home residents. Tony Pecinovsky, a ProVote St. Louis area board member, is also Missouri/Kansas District Organizer of the Communist Party USA, in addition to his work with Jobs with Justice and the Communications Workers of America.

*State Voices

An umbrella group for 600 left-wing organizations in 16 states, State Voices was founded in 2005 by "state and local organizations dedicated to winning shared policy and civic engagement victories and building long-term power."

One notable member of its board is Ken Grossinger, a protégé of Marxist academic Richard Cloward, who with his wife Frances Fox Piven devised the strategy bearing their names that seeks to flood government with impossible demands in order to force a radical transformation of society. Grossinger is also on the board of Social Policy, an ACORN magazine, and he helped to found the Committees of Correspondence, a Communist Party USA (CPUSA) splinter group. He was previously director of legislative field operations for the AFL-CIO and is now executive director of the CrossCurrents Foundation. (See *Foundation Watch*, October 2010)

State Voices has received grants totaling $932,100 from the Tides Foundation (since 2004) and $100,000 from George Soros's Open Society Institute (2007). It received grants totaling $3.4 million from the Beldon Fund, a leftist grantmaker founded by the founders of Steelcase office furniture. The Fund voluntarily ceased operations in May 2009. During its 10-year existence, it distributed $120 million in grants, including $1 million to ACORN and $250,000 to the American Institute for Social Justice, an ACORN affiliate (2006).

*Ohio Voices

Once called the Center for Civic Participation, Ohio Voice is part of State Voices. Interim director Gregory T. Moore is president of GTM Consulting Services LLC, a "political consulting firm that specializes in program development, public-policy analysis and election services," according to the State Voices website. GTM's clients include the Democratic National Committee's Voting Rights Institute and SEIU. Moore was formerly chief of staff and legislative director to House Judiciary Committee chairman Rep. John Conyers (D-Mich.) as well as executive director of the NAACP National Voter Fund, whose program was plagued by voter registration fraud.

*Wisconsin Voices

The director of this State Voices affiliate is Linda Honold, previously chairman of the Wisconsin Democratic Party and an executive director of Citizen Action of Wisconsin.

"Rebranding" ACORN

ACORN state affiliates have been rapidly changing their names and filing new nonprofit applications with the IRS to avoid the taint of the multiple scandals that have weakened ACORN. For instance, ACORN's California chapter quickly rebranded itself the Alliance of Californians for Community Empowerment (ACCE). Clearly, it wants to keep the tax dollars and foundation grants flowing into its coffers. The chapter, which boasts 37,000 dues-paying members, is critical to the ACORN empire.

ACCE claims that it is "up and running as an independent state-wide organization with no legal, financial or structural ties to ACORN." We know ACCE is lying.

How do we know this? For starters, ACCE's executive director is Amy Schur. Schur is a loyal 20-plus year ACORN employee who has shown her willingness to get her hands dirty for the cause. Marcel Reid, a former member of ACORN's national board, said Schur is corrupt and hopelessly tainted. "If there was true reform, why would Amy Schur be the head of ACCE?" she said.

Reid, who with other ACORN whistleblowers formed a group called ACORN 8, was expelled from ACORN in 2008 when she tried to investigate a nearly $1 million embezzlement by founder Wade Rathke's brother who was in charge of the group's finances. According to the ACORN 8, Schur participated in an eight-year long cover-up of the theft whose exposure in 2008 led to Rathke's ouster. Not long after the theft became public knowledge the group's major financial backers, including the Catholic Campaign for Human Development, publicly severed their ties to ACORN.

Insiders say Schur has intimate knowledge of how ACORN operates. Schur has been in charge of the group's national campaigns and may testify in November in Nevada when ACORN goes on trial for illegally paying canvassers bonuses to register Nevada voters in the 2008 presidential campaign. Under cross-examination Schur may be forced to unearth many of the group's skeletons.

ACCE registered with the California secretary of state's office on Dec. 8, the day after an "independent" review by former Massachusetts Attorney General Scott Harshbarger claimed to clear ACORN of wrongdoing. Interestingly, ACCE's office address is 3655 S. Grand Ave., Suite 250, Los Angeles 90007. That address happens to be the address of California ACORN's headquarters.

ACORN is a tangled mess of interlocking directorates and affiliated tax-exempt groups. But there is no reason to believe ACCE won't be centrally controlled by ACORN, just as other ACORN affiliates are.

Sleight-of-hand is how ACORN always does business. It plays a game of musical chairs. When an affiliate does something admirable, ACORN emphasizes its ties. When an affiliate does something wrong, ACORN plays dumb. Its byzantine structure lets it claim plausible deniability.

Such chicanery is standard operating procedure at ACORN, according to the group's lawyer Elizabeth Kingsley. In an internal legal memo in 2008 Kingsley described the hoops that ACORN jumps through to create the façade that its affiliates are independent of each other.

Key ACORN affiliates argue that they are not "'affiliated,' 'related,' or 'controlled' by or with each other, for various legal purposes, while allowing actual control to be exercised in a highly coordinated manner," she wrote. ACORN has "an organizational culture that resembles a family business more than an accountable organization."

Longtime ACORN ally Rep. Maxine Waters (D-Calif.) has welcomed ACCE to the community organizing fold. But Fannie Brown, a former California state delegate on ACORN's national board, is skeptical of the "new" group. "They started washing it a little bit and then they poured some bleach on it and kind of polished it up a little more to make it look good," said Brown, who with Reid is a member of ACORN 8.

Congress's Ban on Funding ACORN Lapses

ACORN Housing is the ACORN network's primary vehicle for getting its hands on federal tax dollars, and it too recently acquired a new name: Affordable Housing Centers of America. But in September federal investigators recommended that by whatever name it operates government funding for it be cut off immediately. The inspector general for the Department of Housing and Urban Development found that ACORN Housing could not account for millions of dollars in federal grants and appeared to have committed massive fraud.

The investigators must have felt it was necessary to urge a speedy funding cutoff because the federal government's prohibition on funding ACORN is *not* a permanent ban. Because the ban was attached to annual appropriations bills it ran out at the end of September.

Many Americans –and some lawmakers–believe Congress permanently cut off ACORN from funding last year, but this belief is unfounded. Quirks of parliamentary procedure and the complexity of the appropriations process explain the confusion. The funding ban that passed in fall 2009 is contained in legislation that covers only the fiscal year that ended on September 30 (i.e. Public Law 111-68).

That the funding ban is not permanent was first noticed by ACORN's lawyers and by Judge Roger J. Miner. Miner was the appellate court judge who in August overturned Judge Nina Gershon's perverse ruling that Congress's funding ban was unconstitutional because it punished ACORN without a trial. Miner noticed that all the appropriations laws passed by Congress that prohibited grants to ACORN "or any of its affiliates, subsidiaries, or allied organizations" applied only to federal spending that ended on Sept. 30, 2010.

Stop-gap legislation signed into law by President Obama on Sept. 30 that allows the government to continue spending money until new appropriations are passed by Congress does *not* contain the ACORN funding ban. The Trans-

portation-HUD appropriations bill does prohibit funding for ACORN during the fiscal year that begins on Oct. 1, 2010, but it's anyone guess whether lawmakers will pass the bill during the current "lame duck" session with the ACORN funding ban intact.

The Obama Administration Stonewalls

Meanwhile, the Obama administration is stonewalling Capital Research Center's Freedom of Information Act (FOIA) request that seeks correspondence between HUD Secretary Shaun Donovan and ACORN. HUD rules state that FOIA requests must be answered within 45 days but our request has been pending for seven months.

The request was filed because Donovan is a longtime ally of ACORN. He worked closely with ACORN for five years when he was New York mayor Michael Bloomberg's housing development commissioner.

"Perhaps no administration official has had more interaction with Acorn than" Donovan, the New York Times reported (Oct. 16, 2009). ACORN chief organizer Bertha Lewis admitted as much. "We grew to respect him, and he grew to respect us."

Donovan has remained silent about his relationship with ACORN.

ACORN—and Wade Rathke—Go Worldwide

Whatever happens to ACORN stateside, the group's overseas affiliates are thriving – with the help of the Obama administration.

Earlier this year the Obama administration helped the group spread the gospel of left-wing community organizing in India. President Obama's ambassador to India, Timothy J. Roemer, met with ACORN India's representative Vikram Adige and lent his name and the prestige of the U.S. government to Adige's efforts to organize rag-pickers in Mumbai (formerly known as Bombay). Roemer is a former Democratic congressman who represented an Indiana district.

ACORN India reports to ACORN International, which also has a new name: Community Organizations International. ACORN International is as an umbrella organization for the various national organizations conducting ACORN's business outside the U.S. Its Facebook website describes the group's mission as "building community groups in low income communities across the world to organize for power." In reality, the group was created to allow ACORN to apply its corporate shakedown techniques against Western corporations as they expand into rapidly developing markets such as India.

ACORN International is active in Argentina, Canada, Dominican Republic, Honduras, India, Kenya, Mexico, and Peru.

ACORN International is headed by ACORN founder Wade Rathke. Like a modern-day Karl Marx in exile, Rathke is doing his best to redistribute wealth around the globe using the shakedown techniques he mastered in the U.S.

"Countries like India are the next frontiers of significant market expansion for multi-national corporations; and these corporations are now starting to apply extreme pressure on the government of India for unfettered access," says the ACORN India website. "[The] Indian market is facing an onslaught of both foreign and domestic corporate retailers, the most notable of which is Walmart."

ACORN has long set its sights on Wal-Mart, which like ACORN, was founded in Arkansas. ACORN created an affiliate, WARN (Wal-Mart Alliance for Reform Now), specifically to organize unions in Wal-Mart stores.

Rathke has traveled extensively in India using the same aggressive, in-your-face organizing tactics that ACORN uses in the U.S. ACORN India's website says the group helps to defend the "socialist legacy" of Jawaharlal Nehru, prime minister of India from 1947 to 1964. That legacy is "now in danger from the onslaught of the march of global corporatism."

ACORN's national board fired Rathke as its "chief organizer" in June 2008 after discovering his role in covering-up his brother's $1 million embezzlement of ACORN funds. But this separation is belied by Rathke's ongoing involvement in ACORN International, another entity supposedly "independent" of ACORN. Rathke also remains publisher of ACORN's periodical, Social Policy magazine, and he is chief organizer of United Labor Unions Local 100 in Louisiana, Arkansas, and Texas, a position he has held since 1979. The union local disaffiliated from the Service Employees International Union last fall.

"For better or worse, Rathke plans on spending the remaining years of his life implementing his ACORN vision to an organization that will have influence the world over," Chicago-based blogger Michael Volpe wrote last month.

"When asked if he thought his name would one day be used like Alinsky, as a verb in community organizing, Rathke simply responded, 'yes.'"

Matthew Vadum is Editor of Organization Trends.

OT

Question#:	1
Topic:	Documents
Hearing:	Cyber-securing the Vote: Ensuring the Integrity of the U.S. Election System
Primary:	The Honorable Elijah E. Cummings
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: On October 20, 2017, Rep. Robin Kelly, the Ranking Member of the Subcommittee on Information Technology, and I sent a letter to the Department of Homeland Security (DHS) requesting copies of all documents "related to the Russian government-backed attempts to hack state election systems." On November 28, 2017, DHS responded by producing just one e-mail with a short script that Department employees apparently read over the phone to state election officials. This script is 13 sentences long and does not refer to any specific state or attack.

On November 29, 2017, you testified at a joint subcommittee hearing on the "Cybersecurity of Voting Machines" and assured Members that DHS would provide additional documents relating to Russian hacking of state election systems in 2016.

To follow-up, the Subcommittees sent official Questions for the Record on January 3, 2018, with a letter signed by both Subcommittee Chairmen Will Hurd and Gary J. Palmer. That letter requested "all documents related to the Russian government-backed attempts to monitor, penetrate, or hack state election systems during the presidential election campaign of 2016."

On February 6, 2018, DHS provided only 50 pages of documents with information about how DHS officials learned about the Russian-backed attacks and communicated with states. Most of the production consisted of publicly available documents. This production did not include any classified documents, nor did it include documents relating to the precise nature of these attacks, the number of times these states were targeted, or when they were targeted.

Please produce copies of all documents, including classified documents, related to Russian government-backed attempts to monitor, penetrate, or hack state election systems during the presidential election campaign of 2016, including but not limited to: the tools the attackers used; the tactics they utilized; communications within DHS or between DHS and other federal, state, or local government entities regarding this Russian activity; and the results of your conversations with states regarding this Russian activity, and the steps you took to follow-up.

If there are any responsive documents that you will not produce, please provide a brief description of each document and the specific reason for withholding each document.

Question#:	1
Topic:	Documents
Hearing:	Cyber-securing the Vote: Ensuring the Integrity of the U.S. Election System
Primary:	The Honorable Elijah E. Cummings
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Response: The Department of Homeland Security (DHS) has provided significant documentation to the Committee regarding the 2016 election. DHS has met with Committee staff to walk through the documents provided by DHS and to answer additional questions about what occurred in 2016. DHS will continue to meet with the Committee and answer questions to ensure the Committee has a full understanding of what occurred. However, it is not appropriate for DHS to share documents owned by other departments or non-federal entities, whether they are unclassified, contain investigative law enforcement information, or are classified intelligence products. DHS recommends the Committee should continue to engage with other relevant federal and non-federal entities to obtain the relevant information that they own and that is of interest to the Committee.

Question#:	2
Topic:	Cybersecurity Coordinator
Hearing:	Cyber-securing the Vote: Ensuring the Integrity of the U.S. Election System
Primary:	The Honorable Elijah E. Cummings
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: At the hearing, you testified that, separate from the eliminated position of Cybersecurity Coordinator, "there are cybersecurity directors and senior directors in the National Security Council."

In what ways do those individuals coordinate interagency election security efforts?

How do their responsibilities compare with those of the Cybersecurity Coordinator before that position was eliminated?

Response: The Department of Homeland Security (DHS) coordinates regularly with the White House and other Federal agencies on national security matters. DHS's roles and responsibilities are defined by statutes, executive orders, and Presidential policies and strategies. Changes to the National Security Council staff related to the Cybersecurity Coordinator position have had no impact on DHS's ability to execute its mission. Previously, the Senior Directors for Cybersecurity reported to the Cybersecurity Coordinator, and those positions remain today. DHS defers to the National Security Council to define the responsibilities of the Senior Directors and Directors. The President has provided clear direction to DHS and other national security agencies, stating that they are empowered and expected to execute their authorities and responsibilities. Since the creation of the position, the interagency processes have matured considerably. DHS and our interagency partners continue to coordinate regularly, either through the National Security Council staff on policy matters or through operational centers for day-to-day operations.

Question#:	3
Topic:	White House Guidance
Hearing:	Cyber-securing the Vote: Ensuring the Integrity of the U.S. Election System
Primary:	The Honorable Elijah E. Cummings
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: Separate from general guidance or direction about election security, what specific direction has President Trump provided to you or, to your knowledge, Secretary Kirstjen M. Nielsen on taking steps to protect our elections from Russian interference?

Response: The Department of Homeland Security (DHS) is focused on protecting our elections from interference by Russia or other malicious actors. The President has made it clear that his Administration will not tolerate foreign interference in our elections from any nation state or other malicious actor. The Administration is focused on working with state and local election officials to ensure that every American's vote counts and is counted correctly. The President reiterated that election security is national security. The Administration will continue to provide the support necessary to the owners of election systems – state and local governments – to secure their election processes.

Question#:	4
Topic:	POCs
Hearing:	Cyber-securing the Vote: Ensuring the Integrity of the U.S. Election System
Primary:	The Honorable Elijah E. Cummings
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: Please provide the name and position of your primary point(s) of contact in the White House on cybersecurity matters and election security matters, including individuals working for or serving on the National Security Council.

Response: Senior leadership of the Department and I regularly interact with the National Security Advisor, Ambassador John Bolton, and his direct reports on the National Security Council staff.

Question#:	5
Topic:	Work with Cybersecurity Coordinator
Hearing:	Cyber-securing the Vote: Ensuring the Integrity of the U.S. Election System
Primary:	The Honorable Elijah E. Cummings
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: Please describe your office's work with then-White House Cybersecurity Coordinator Rob Joyce prior to the elimination of that position in April 2018.

In what ways has the decision to eliminate the position of White House Cybersecurity Coordinator affected or changed your office's interaction and work with the White House?

Response: The Department of Homeland Security (DHS) coordinates regularly with the White House and other federal agencies on national security matters. DHS's roles and responsibilities are defined by statutes, executive orders, and Presidential policies and strategies. DHS worked well with Cybersecurity Coordinator Rob Joyce when he served on the National Security Council staff, and our work with the National Security Council has not changed since his departure. Changes to the National Security Council staff related to the Cybersecurity Coordinator position have had no impact on DHS's ability to execute its mission.