

SECURING AMERICA'S ELECTIONS PART II: OVERSIGHT OF GOVERNMENT AGENCIES

HEARING BEFORE THE COMMITTEE ON THE JUDICIARY U.S. HOUSE OF REPRESENTATIVES ONE HUNDRED SIXTEENTH CONGRESS SECOND SESSION

OCTOBER 22, 2019

Serial No. 116-60

Printed for the use of the Committee on the Judiciary



Available via: <http://judiciary.house.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2021

COMMITTEE ON THE JUDICIARY

JERROLD NADLER, New York, *Chair*
MARY GAY SCANLON, Pennsylvania, *Vice-Chair*

ZOE LOFGREN, California	DOUG COLLINS, Georgia, <i>Ranking Member</i>
SHEILA JACKSON LEE, Texas	F. JAMES SENSENBRENNER, Jr.,
STEVE COHEN, Tennessee	Wisconsin
HENRY C. "HANK" JOHNSON, JR., Georgia	STEVE CHABOT, Ohio
THEODORE E. DEUTCH, Florida	LOUIE GOHMERT, Texas
KAREN BASS, California	JIM JORDAN, Ohio
CEDRIC L. RICHMOND, Louisiana	KEN BUCK, Colorado
HAKEEM S. JEFFRIES, New York	JOHN RATCLIFFE, Texas
DAVID N. CICILLINE, Rhode Island	MARTHA ROBY, Alabama
ERIC SWALWELL, California	MATT GAETZ, Florida
TED LIEU, California	MIKE JOHNSON, Louisiana
JAMIE RASKIN, Maryland	ANDY BIGGS, Arizona
PRAMILA JAYAPAL, Washington	TOM MCCLINTOCK, California
VAL BUTLER DEMINGS, Florida	DEBBIE LESKO, Arizona
J. LUIS CORREA, California	GUY RESCHENTHALER, Pennsylvania
SYLVIA R. GARCIA, Texas	BEN CLINE, Virginia
JOE NEGUSE, Colorado	KELLY ARMSTRONG, North Dakota
LUCY MCBATH, Georgia	W. GREGORY STEUBE, Florida
GREG STANTON, Arizona	
MADELEINE DEAN, Pennsylvania	
DEBBIE MUCARSEL-POWELL, Florida	
VERONICA ESCOBAR, Texas	

PERRY APELBAUM, *Majority Staff Director & Chief Counsel*
BRENDAN BELAIR, *Minority Staff Director*

C O N T E N T S

TUESDAY, OCTOBER 22, 2019

	Page
OPENING STATEMENTS	
The Honorable Mary Gay Scanlon, Vice-Chair, Committee on the Judiciary	1
The Honorable Doug Collins, Ranking Member, Committee on the Judiciary Written Testimony	6
The Honorable Jerrold Nadler, Chairman, Committee on the Judiciary Written Testimony	48
WITNESSES	
Matt Masterson, Senior Cybersecurity Advisor, Department of Homeland Security Oral Testimony	12
Written Testimony	14
Nhikki Floris, Deputy Assistant Director, Counterterrorism, Federal Bureau of Investigation Oral Testimony	22
Written Testimony	24
Adam Hickey, Deputy Assistant Attorney General, National Security Division, Department of Justice Oral Testimony	29
Written Testimony	31
Ben Hovland, Vice Chair, U.S. Election Assistance Commission Oral Testimony	42
Written Testimony	44
LETTERS, STATEMENTS, ETC. SUBMITTED FOR THE HEARING	
An article for the record from The Hill, submitted by the Honorable Matt Gaetz	72
An article for the record from The New York Times, submitted by the Honorable Matt Gaetz	78
An article for the record from The Kyiv Post, submitted by the Honorable Matt Gaetz	86
A report for the record from Graphica, submitted by Joe Neguse	104
APPENDIX	
Questions for the record, Matt Masterson, Senior Cybersecurity Advisor, Department of Homeland Security	146
Responses for the record, Adam S. Hickey, Deputy Assistant Attorney General	153
Questions for the record, Ben Hovland, Vice-Chair Election Assistance Commission	168
Questions for the record, Nikki Floris, Deputy Assistant Director, Counterintelligence Division	173
Responses for the record, Masterson, senior cybersecurity advisor, the Department of Homeland Security	178

SECURING AMERICA'S ELECTIONS PART II: OVERSIGHT OF GOVERNMENT AGENCIES

Tuesday, October 22, 2019

HOUSE OF REPRESENTATIVES

COMMITTEE ON THE JUDICIARY

Washington, DC

The Committee met, pursuant to call, at 10:10 a.m., in Room 2141, Rayburn Office Building, Hon. Mary Gay Scanlon, presiding.

Present: Representatives Nadler, Lofgren, Jackson Lee, Cohen, Johnson of Georgia, Deutch, Cicilline, Jayapal, Correa, Scanlon, Garcia, Neguse, McBath, Stanton, Dean, Murcarsel-Powell, Escobar, Chabot, Gohmert, Gaetz, Biggs, Lesko, Reschenthaler, Cline, and Steube.

Staff present: Arya Hariharan, Deputy Chief Oversight Counsel; David Greengrass, Senior Counsel; Madeline Strasser, Chief Clerk; Moh Sharma, Member Services and Outreach Advisor; Sarah Istel, Oversight Counsel; Priyanka Mara, Professional Staff Member/Legislative Aide; Kerry Tirrell, Oversight Counsel, Antitrust, Commercial, and Administrative Law Subcommittee; Matt Robison, Counsel, Courts and Intellectual Property Subcommittee; Brendan Belair, Minority Staff Director; Bobby Parmiter, Minority Deputy Staff Director/Chief Counsel; Jon Ferro, Minority Parliamentarian/General Counsel; Ryan Breitenbach, Minority Chief Counsel, National Security; and Erica Barker, Minority Chief Legislative Clerk.

Ms. SCANLON. The House Committee on the Judiciary will come to order.

Without objection, the chair is authorized to declare recesses of the Committee at any time.

We welcome everyone to this morning's hearing on Securing America's Elections Part II: Oversight of Government Agencies. I will now recognize myself for an opening statement.

Last month, this Committee held part one of a series of hearings on securing America's elections. In that hearing, 3 witnesses, who had been jointly selected by the committee, testified unequivocally that our Nation's elections are under attack. Debora Plunkett, former director on the National Security Council under both President Clinton and President George W. Bush, warned, "We must bold, decisive, and must take expeditious steps to address cyber threats. We must treat election security as imperative for safeguarding our democracy." Secretary of State Kathy Boockvar from the Commonwealth of Pennsylvania elaborated: "Election security

is a race without a finish line, and our adversaries are not slowing down.”

This testimony has been confirmed by the leaders of our intelligence community. Last month, the director of national intelligence testified that, “Foreign actors will view the 2020 elections as an opportunity to advance their interests. We expect them to refine their capabilities and add new tactics as they learn from each other’s experiences and efforts in previous elections.” In short, there is no question that our elections, the cornerstone of our free and democratic society, are exposed. Protecting our Nation’s democratic processes from foreign attack must be among our top priorities, and we are committed to doing that work.

Today we have representatives from the four Federal agencies leading the charge on election security: The Department of Homeland Security, the Federal Bureau of Investigation, the Department of Justice, and Election Assistance Commission. At their core, elections are run at the State and local level, but our Federal Government must provide critical support to help States to defend themselves from hostile foreign actors. Protecting our elections requires a whole of society approach that relies on coordinated actions by government agencies at all levels, including the agencies represented here today.

Federal agencies responsible for protecting our elections have made significant progress since 2016. These efforts are important and commendable, but significant vulnerabilities in our system remain. To start, our efforts must be integrated and coordinated. A simple Google search of “report election security issues” turns up results for over 20 different groups across these agencies and others. There must be clear lines of authority to ensure that States know which of the multiple programs across these agencies is in charge.

Equally important, we must do more to ensure better Federal and State collaboration. That requires earning the trust of States. At a public speech on October 3rd, 2018, DHS Director Krebs explained that in 2016 when the Federal Government called State officials to alert them of threats, there was, as he said, no trust and there was no certainty or confidence in the ability of the Federal Government. One way to strengthen trust is through enhanced transparency.

In 2016, the specific intent of the Russians was not initially made public. Today we can do better. We can educate State and local officials and the public about influence operations. By bringing our adversaries’ tactics to light, we can prevent them from succeeding. In addition, we must ensure that the development and maintenance of our systems matches the evolving nature of cyber threats. For example, current EAC Federal guidelines for our certification processes were created in 2005 and are woefully out of date. As our witness, Mr. Byrd of Microsoft, testified last month, “This process is more than a decade old, and it is too slow and too burdensome to enable voting officials to respond as quickly as needed to our agile adversaries.”

Finally, and most importantly, we must ensure that State and local officials, the frontline defenders of democracy, have the resources and support they need to protect our systems. DHS has

made it clear that it requires additional resources to fulfill this task. It has requested, for example, 20 additional advisors to help States in anticipation of the 2020 election cycle. On May 15th, 2019, the EAC likewise testified before the Senate that the U.S. currently lacks sufficient funding in critical areas to protect our 2020 elections.

Unfortunately, however, President Trump and his Administration, rather than listening to the warnings of Federal agencies about the seriousness of the threat picture and request for more resources to secure our elections, has done the opposite. The Trump Administration has cut senior cyber positions, downsized by half DHS' election security teams, and proposed significant budget cuts to DHS' major election security program. All these actions leave us more vulnerable to the ongoing threat to our democracy. We will not let this happen. Elections cannot be a partisan issue. They must be an American issue.

This Committee is committed to working together to protect our democracy from all threats to our elections in all forms, whether to our physical election infrastructure or the ongoing disinformation campaigns coming from adversaries like Russia. I thank each of our witnesses for being here today. My colleagues and I are looking forward to hearing your testimony about your ongoing efforts to secure our elections and what important work remains to be done.

Without objection, the Ranking Member's statement, Doug Collins, will be placed in the record, and all other opening statements will be included in the record.

[The information follows:]

MR. COLLINS FOR THE OFFICIAL RECORD

**Statement of Ranking Member Doug Collins
Hearing on “Securing America’s Elections Part II: Oversight of
Government Agencies”
Tuesday, October 22, 2019**

Voting is sacrosanct activity for Americans. We can’t tolerate internal and external threats against our democratic elections. For this reason, I sincerely hope we will work together legislatively to safeguard America’s elections for generations to come.

The Trump Administration devoted significant resources toward securing the 2018 congressional midterm elections. No one can point to problems on the order of magnitude we saw in the 2016 presidential election originating largely from Russia. While Russia and many other foreign adversaries will continue to seek methods and avenues to influence our elections, I firmly

believe we can deter and prevent malicious tampering if our government remains vigilant.

Republicans have offered multiple bills to deter and prevent tampering. Our bills have included sound measures to secure elections and to punish those who attempt to infiltrate the nation's election infrastructure. Democrats, however, actively choose to ignore solutions simply because they emanate from the party of President Trump. Judiciary Democrats are not using their majority, or their newfound time, to advance viable solutions for protecting future elections. Unfortunately, we're still waiting for reasonable, effective legislative action.

In November of 2018, then-Judiciary Ranking Member Nadler wrote your agencies and said, "this Administration has no coordinated strategy to respond to

attacks on our elections—and the Trump White House has shown little interest in this grave threat to our democratic system.” While the Chairman’s forecast was obviously proven false—evidenced by the success of the 2018 midterms in preventing election attacks against our nation—it appears he blamed the wrong President and administration for failing to place the necessary focus on external threats to our democracy. The Democrats have been quite consistent in their two-year quest to derail a democratically elected President, but conveniently fail to address the fact that, under President Obama, our government allowed foreign election incursions in the first place. Why are they so anxious to take the focus off what is in plain sight? Why, while we hold a second hearing on election security, aren’t Democrats asking the inconvenient questions many Americans still want

answered: What are the lessons learned from the Obama Administration's failure to secure our elections from foreign influence? How has the Trump Administration worked to correct its predecessor's missteps?

Each of the elected representatives sitting on this dais are the beneficiaries of voters who have confidence that their vote is safe, and protected from manipulation by criminals or other countries. If their confidence is shaken, our Republic suffers. Therefore, each of you in your leadership roles in your respective agencies has an important role in assuring the American people their votes are secure, accurately accounted for, and immune from corrupt foreign influence.

I look forward to hearing from each of the agency representatives today on their efforts to secure future national, state, and local elections.

Ms. SCANLON. I will now introduce today's witnesses. Matt Masterson is the senior cybersecurity advisor at the Department of Homeland Security, where he manages election security under the National Protection and Programs Directorate. From 2014 to 2018, he served as a U.S. Election Assistance Commissioner. Prior to his appointment, Mr. Masterson served as interim chief of staff for the Ohio secretary of state, deputy chief information officer, and deputy director of elections. Mr. Masterson received his B.S. and B.A. from Miami University in Oxford, Ohio, and his J.D. from the University of Dayton School of Law.

Nikki Floris is the deputy assistant director of the Counterintelligence Division of the FBI, where she oversees the intelligence branch, which includes the Foreign Influence Task Force System. Ms. Floris entered the Bureau in 2005 as an intelligence analyst and served in many other positions, including deputy assistant director of Operations Branch III in the Counterterrorism Division, where she oversaw terrorism financing operations, strategic operations, and counterterrorism analysis. Ms. Floris has a bachelor's degree in psychology from the University of Rhode Island and a master's degree in criminology from George Washington University.

Adam Hickey is a deputy assistant attorney general of the National Security Division at the Department of Justice. In that role, he manages the Division's effort to combat national security threats, including threats to our election systems. Before joining the Department of Justice, Mr. Hickey clerked for Judge Jed Rakoff of the U.S. District Court for the Southern District of New York, and Judge Robert Katzmann of the U.S. Court of Appeals for the Second Circuit. Mr. Hickey received his bachelor's degree from Harvard College and his J.D. from Yale Law School.

Ben Hovland is the vice chair of the Election Assistance Commission, where he is the designated Federal officer for the Technical Guidelines Development Committee, which develops the voluntary voting system guidelines. Before being appointed vice chair, Commissioner Hovland served as the acting chief counsel for the U.S. Senate Committee on Rules and Administration. Commissioner Hovland received his B.A. from the University of Central Arkansas and his J.D. from the University of Oregon.

Please note that each of your written statements will be entered into the record in its entirety. Accordingly, I ask that you summarize your testimony in 5 minutes. To help you stay within that time, there is a timing light on your table. When the light switches from green to yellow, you have 1 minute to conclude your testimony. When the light turns red, it signals your 5 minutes have expired.

We want to thank you all for participating in today's hearing. If you would please rise, I will begin by swearing you in.

Do you swear or affirm under penalty of perjury that the testimony you are about to give is true and correct to the best of your knowledge, information, and belief, so help you God?

[A chorus of ayes.]

Ms. SCANLON. You may be seated. Let the record show that the witnesses have answered in the affirmative.

All right, Mr. Masterson, you may begin, and you have to push to button to turn your microphone on before you start. Thank you.

TESTIMONY OF MATTHEW MASTERSON

Mr. MASTERSON. Well, thank you, and good morning, Members of the committee. Thank you for this opportunity to testify regarding the cybersecurity and infrastructure security agencies' efforts to help secure our election infrastructure across this country. My name is Matt Masterson. I'm the election lead for CISA and the former chair of the U.S. Election Assistance Commission, as well as an election official in the State of Ohio.

CISA has a strong relationship with our federal partners seated here at the table and with State and local election officials across the country. Our election-related mission is clear: To support election officials and their private sector partners to identify and manage risk to their systems. Elections are run at the State and local level by dedicated professionals across America's more than 8,800 election jurisdictions, and we work to ensure those officials don't have to defend themselves from sophisticated and persistent threats on their own.

Over the last 3 years, we've worked tirelessly to strengthen our partnership with the election community. We already provide free and voluntary resources and services to all 50 States, over 2,100 local and territorial election jurisdictions, 6 election associations, 12 election technology providers, and political organizations, including presidential campaigns. Our approach has been and continues to be threefold: one, making sure the election community has the information they need to defend their systems; Two, making sure they have the technical support and tools to identify and mitigate risks to their election infrastructure; and three, building enduring partnerships to advance security efforts together.

CISA is laser focused on building scalable, repeatable mechanisms to dramatically grow our information-sharing capabilities. We share contextualized threat intelligence and actionable information through our close partnerships with the intelligence community, law enforcement, and the private sector. More importantly, State and local election officials are sharing what they see on their networks with us. We deploy intrusion detection capabilities, or Albert sensors, to provide real-time detection capabilities of malicious activity on election infrastructure in all 50 States.

Second, we provide technical support and services to election officials and vendors. As we refine our understanding of election officials' needs, we are shifting to capabilities that are quicker, lesser intrusive, and can scale to more jurisdictions. For instance, in 2018 and 2019, we deployed a remote penetration testing capability, thanks in part to the funding provided by Congress. This remote penetration testing capability allows us to identify risks and vulnerabilities to network-connected election systems without having to deploy teams into local election offices, and without interrupting both their time and people.

CISA has also been working closely with election technology providers to ensure that election systems and other technologies undergo testing to discover and fix vulnerabilities in their software. This scalability is critical because while our initial efforts in 2016

were primarily targeted at State election officials, we recognize the need to increase our support to counties and municipalities who operate elections. For example, the Last Mile Initiative provides no-cost information sharing tailored to those jurisdictions to identify cyber risks to their infrastructure and a checklist of action items to mitigate those risks.

The final area of focus has been building on enduring partnerships towards our collective defense. It may seem mundane, but governance, communication, coordination, training, and planning are the critical foundation elements of our efforts to secure our Nation's elections. For this election cycle, CISA has built off the lessons learned for the 2018 election and is expanding our work to prioritize the following lines of effort: One, expanded engagement to local election officials. We continue to work with election officials to improve both their and our understanding of risk to their systems. For instance, in June of this year, we did our second annual tabletop devote exercise where 47 States, thousands of local election officials, the private sector, and Federal Government, worked together through scenarios to share information and understand how we would all collectively respond to threats to our election infrastructure. With a better understanding of risk, we can identify and provide the resources they need to secure their election systems.

CISA has expanded our level of engagement and sharing of best cybersecurity practices with political organizations as well, including the DNC and RNC. CISA has joined FBI and ODNI in offering briefings to the Presidential campaigns who register with the FEC and has engaged directly with campaigns to offer our services. CISA, in coordination with our interagency partners, is committed to helping Americans recognize and avoid foreign disinformation operations impacting our elections through innovative efforts, like our War on Pineapple Campaign, where we educated Americans on the tactics of foreign influence campaign using a topic everyone can relate to, the divisive issue of pineapple on pizza. We will continue to put out educational material to build resilience in the American public on foreign influence operations.

Finally, we're working closely with our intelligence community and the private sector to increase the quantity, quality, and timeliness of intelligence analysis and production at the unclassified levels to help election officials and the public identify and expose foreign influence operations. We at CISA are committed to working with Congress to ensure our efforts cultivate a safer, more secure, and resilient homeland.

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

[The statement of Mr. Masterson follows:]



Testimony

Matthew Masterson
Senior Cybersecurity Advisor
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

***SECURING AMERICA'S ELECTIONS PART II:
OVERSIGHT OF GOVERNMENT AGENCIES***

**BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY**

Tuesday, October 22, 2019

Washington, DC

Chairman Nadler, Ranking Member Collins, and Members of the Committee, thank you for the opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) progress in reducing and mitigating risks to our Nation's election infrastructure. DHS has worked to establish trust-based partnerships with state and local officials who administer our elections, as well as political parties and campaigns, and I look forward to sharing with you an update on our work during the 2018 midterm elections and our priorities through the 2020 election cycle.

Leading up to the 2018 midterms, DHS worked hand in hand with federal partners, state and local election officials, and private sector vendors to provide them with information and capabilities to enable them to better defend their infrastructure. On the Federal level, DHS has coordinated closely with the Federal Bureau of Investigation (FBI), the Office of the Director of National Intelligence (ODNI), and Department of Defense (DOD) on these efforts. This partnership led to a successful model that we aim to continue and improve upon in the 2020 election cycle.

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

CISA and the Election Assistance Commission (EAC) have convened federal government and election officials regularly to share cybersecurity risk information and to determine an effective means of assistance. Since 2017, the Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) has worked to establish goals and objectives, to develop plans for the EIS partnership, and to create an EIS Sector-Specific Plan. Participation in the council is voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

CISA and the EAC have also worked with election equipment and service vendors to launch, in 2017, an industry-led Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed council with industry leadership designated by SCC members. The SCC serves as the industry's principal entity for coordinating with the Federal Government on critical infrastructure security activities related to sector-specific strategies. This collaboration is conducted under CISA's authority to provide a forum in which federal and private sector entities can jointly engage in a broad spectrum of activities to coordinate critical infrastructure security and resilience efforts, which is used in each of the critical infrastructure sectors established under Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*. The SCC has helped CISA further its understanding of the systems, processes, and relationships particular to operation of the EIS.

Within the context of today's hearing, I will address our efforts in 2018 to help enhance the security of elections that are administered by jurisdictions around the country, along with our

election related priorities through 2020. While there was activity targeting our election infrastructure leading up to the midterms, this activity was consistent with typical malicious activity targeting networked IT systems. DHS along with the Department of Justice (DOJ), “concluded that there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political/campaign infrastructure used in the 2018 midterm elections used for the United States Congress.”¹

Assessing the Threat

The Department, with and through DHS’ Office of Intelligence and Analysis (I&A), regularly coordinates with the Intelligence Community (IC) and law enforcement partners on potential threats to the Homeland. Among non-federal partners, DHS has engaged with state and local officials, as well as relevant private sector entities, to assess the scale and scope of malicious cyber activity potentially targeting election infrastructure in the United States. 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. Since 2016, state and local election offices and their private sector partners have robustly shared information with DHS regarding activity targeting their systems. As with all networked IT systems, officials are seeing scanning and probing of their networks on a daily basis. Election infrastructure is a target for nation-state and non-state actors seeking access to systems containing sensitive data or what they perceive to be valuable information. DHS and our IC partners continue to assess that the 2020 election remains a likely cyber and influence target for our adversaries. In short, the threat to our elections remains and it is incumbent on all levels of government to work together to respond.

Enhancing Security

During the 2018 midterms, CISA provided a coordinated response from DHS and its federal partners to plan for, prepare for, and mitigate risk to election infrastructure. Working with election infrastructure stakeholders was essential to ensuring a more secure election. CISA and our stakeholders increased awareness of potential vulnerabilities and provided capabilities to enhance the security of U.S. election infrastructure, and shared best practices with other nations facing similar threats.

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, CISA will continue to provide free, voluntary, prioritized services to support their efforts to secure elections in the 2020 election cycle.

¹ “Acting Attorney General and Secretary of Homeland Security Submit Joint Report on Impact of Foreign Interference on Election and Political/Campaign Infrastructure in 2018 Elections.” February 5, 2019. Retrieved from: <https://www.dhs.gov/cisa/news/2019/02/05/acting-attorney-general-and-secretary-homeland-security-submit-joint-report>

Improving Coordination with State, Local, Tribal, Territorial and Private Sector Partners

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

Working with the EI-ISAC

CISA works with the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) to provide threat and vulnerability information to state and local officials. Through funding by CISA, the Center for Internet Security created and continues to operate the EI-ISAC. The EI-ISAC has representatives co-located with CISA's operations center to enable regular collaboration and access to information and services for election officials.

Providing Technical Assistance and Sharing Information

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

Cyber hygiene service for Internet-facing systems: Through this automated, remote scan, CISA provides a weekly 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 (both onsite and remote): We have prioritized state and local election systems upon request, and increased the availability of risk and vulnerability assessments. These in-depth, on-site or remote 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 CISA. Upon request, the CISA can provide assistance in identifying and remediating a cyber incident. Information reported to CISA is also critical to the Federal Government's ability to broadly assess malicious attempts to infiltrate election systems. This

technical information will also be shared with other state officials so they have the ability to defend their own systems from similar malicious activity.

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

Classified information sharing: To most effectively share information with all of our partners—not just those with security clearances—DHS and its Office of I&A work with the IC to rapidly declassify relevant intelligence or provide as much intelligence as possible at the lowest classification level possible. While DHS prioritizes declassifying information to the greatest extent possible, DHS also provides classified information to cleared stakeholders, as appropriate. DHS has been working with state chief election officials and additional election staff in each state to provide them with security clearances. These clearances have helped enable I&A and the IC to deliver a number of classified in-person and secure video teleconferences for a broad audience of state and local elections officials, in the lead-up to the 2018 Midterms and into 2019.

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

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

Election Security Efforts Leading up to the 2018 Midterms

In the weeks leading up to the 2018 midterm elections, CISA officials supported a high degree of preparedness nationwide. CISA provided free technical cybersecurity assistance, continuous information sharing, and expertise to election offices and campaigns. All 50 states, over 1,500 local and territorial election offices, 6 election associations, and 12 election vendors were engaged in information sharing and receipt of assistance from EI-ISAC.

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

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

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

Countering Foreign Influence

In 2018, DHS, in coordination with the FBI and other Federal partners, supported interagency efforts to secure the mid-term elections from foreign malign influence through two lines of effort – operational support and raising public awareness. In the National Cybersecurity Situational Awareness Room, DHS CISA staff served as liaisons between state and local election officials and social media platforms; relaying disinformation reported by election officials, including through the national network of fusion centers, to the relevant social media platforms, ensuring they had the necessary information to take action based on their terms of service. CISA partnered with the National Association of Secretaries of State and the National Association of State Election Directors to develop products and messaging designed to drive voters to reliable sources for information.

In advance of the 2020 Federal Election, DHS’s Countering Foreign Influence Task Force (CFITF) is expanding on both operational support activities and public awareness and engagement. DHS established CFITF to facilitate public awareness, partner engagement, and information sharing as it relates to foreign influence threats including those targeting United States elections. These efforts are done in close coordination with and support to the FBI and its malign influence efforts. The CFITF is growing the number of participants, increasing lines of communication between the platforms being exploited and the victims of that exploitation.

CISA, in coordination with our interagency partners, is also committed to helping Americans recognize and avoid foreign disinformation operations impacting our elections through innovative efforts like the #WarOnPineapple campaign. The #WarOnPineapple is aimed at educating Americans on the use of foreign influence campaign tactics, by highlighting a topic that citizens can easily relate to: the divisiveness of pineapples on pizza. Through this work, CISA is helping Americans recognize and avoid foreign disinformation operations impacting homeland security, including our elections. For more information on CISA's work on the #WarOnPineapple campaign and election security more broadly, please visit www.dhs.gov/cisa/protect2020. DHS I&A is supporting interagency efforts to counter foreign influence through increased quantity, quality, and timeliness of intelligence analysis and production at unclassified levels.

Priorities for the 2020 Election Cycle

For the 2020 elections, CISA has identified the following lines of effort to guide the Department's work:

- Protecting Election Infrastructure,
- Supporting Campaigns and Political Infrastructure,
- Raising Public Awareness and Building Resilience, and
- Efficiently Sharing Actionable Intelligence and Identifying Threats.

These priorities include broadening the reach and depth of information sharing and assistance that CISA is providing to state and local election officials, deepening our understanding of the elections risk environment, highlighting the need for regular and consistent resourcing of election infrastructure, extending the CISA suite of services for protecting networks to political campaigns and partisan organizations at the national level, increasing public understanding of foreign influence operations, and providing intelligence and threat reporting to the election community. For more information on these priorities, please visit: www.dhs.gov/cisa/protect2020

In addition, CISA is working towards improving the efficiency and effectiveness of election audits, incentivize the patching of election systems, and working with the National Institute of Standards and Technology (NIST) and the states to develop cybersecurity profiles utilizing the NIST Cybersecurity Framework for Improving Critical Infrastructure. The Department will continue to engage any political entity that wants our help. We are continuously working to mature our understanding of risks to this sector, improve our offerings, and to provide meaningful security guidance leveraging leading practices.

CISA has made tremendous strides on these efforts and goals and has been committed to working collaboratively with those on the front lines of administering our elections to secure election infrastructure from risks. In February, CISA officials provided updates to the Secretaries of State, state election directors, and members of the GCC and SCC on the full package of election security resources that are available from the Federal government, along with a roadmap on how to improve coordination across these entities. DHS also worked with our IC partners to provide a classified one day read-in for these individuals regarding the current threats facing our election infrastructure.

In June, CISA hosted another “*Tabletop the Vote*” exercise with our federal partners, state and local election officials, and private sector vendors to review coordination protocols and incident response plans. The *Tabletop* covered a number of pre-, post- and day of election scenarios, including voter registration compromises, equipment issues, and misinformation distributed over news and social media. Participants included representatives from 47 states, thousands of local election officials, the District of Columbia, U.S. Virgin Islands, along with our Federal partners.

In July, DHS joined ODNI, DOJ, and DOD in briefing the full Congress on the federal government’s coordinated approach to protecting the 2020 elections. DHS highlighted the increase in threat information that is now shared with state, local, territorial governments, the number of intrusion detection sensors, known as Albert sensors, deployed across the country, and the prioritization of intelligence sharing with state and local officials on cyber threats and foreign interference.

CISA, through the EI-ISAC, now provides threat alerts to all 50 states and more than 2000 local and territorial election offices. CISA also provides weekly vulnerability scans for 37 states, 145 local partners, one territory, and 10 private sector partners. In addition, all 50 states, 110 localities, and two territories now have intrusion detection sensors. These sensors are operated and monitored by EI-ISAC as part of the Multi-State Information Sharing and Analysis Center’s (MS-ISAC) Albert intrusion detection system. DHS shares intelligence and other cyber threat information with EI-ISAC for use in Albert, which assists with identifying specific threats to election infrastructure networks. EI-ISAC has also deployed Albert sensors within election vendor environments, to protect their networks that host voter registration systems in five states.

CISA is also expanding our level of engagement with political organizations. We have worked in close coordination with both the Democratic National Committee (DNC) and the Republican National Committee (RNC) to share information and best practices. CISA has also engaged directly with Presidential and Congressional campaigns. These efforts have included a joint threat briefing with the FBI and ODNI for all Presidential campaigns registered with the FEC as well as engaging directly with campaigns to offer services and share information.

We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure. It will take continual investment from all levels of government to ensure that election systems across the nation are upgraded, patched and better secured, with older more vulnerable systems retired. These efforts require a whole of government approach.

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

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

Ms. SCANLON. Thank you very much. Ms. Floris?

TESTIMONY OF NIKKI FLORIS

Ms. FLORIS. Thank you. Good morning, Members of the committee. Thank you for the opportunity to appear before you today to discuss the FBI's effort to secure America's elections. As you've just heard, I'm Nikki Floris, deputy assistant director for the FBI's Counterintelligence Division.

The FBI is the Federal lead for identifying and combatting malign foreign influence operations which target U.S. democratic institutions and values. This also includes the investigation of election-related cyber intrusions and crimes. To achieve their strategic geopolitical objectives, foreign adversaries use malign influence operations to shift U.S. policy, distort U.S. political sentiment and discourse, undermine confidence in U.S. democratic institutions and values, or interfere with U.S. electoral processes.

Most widely reported these days have been the attempts by foreign adversaries to discredit U.S. individuals and institutions using false personas and fabricated stories on social media platforms. These operations have aimed to spread disinformation, sow civil discord, and ultimately undermine the confidence in our democratic institutions and values. Foreign influence operations involve a wide spectrum of activities. However, it is the subversive, undeclared criminal and coercive aspects of these activities that forms the basis of FBI investigative interests. It is why we talk about malign foreign influence. This is by no means a new problem. However, global interconnectedness and online anonymity have changed the character of the overall foreign influence threat and how the FBI and its partners must address it.

In my role at the FBI, I oversee the Foreign Influence Task Force, or what we call the FITF. In the fall of 2017, Director Wray established the FITF to combat foreign influence operations targeting the United States. The FITF is led by the Counterintelligence Division and is comprised of agents, analysts, and professional staff from the Counterintelligence, Counterterrorism, Cyber, and Criminal Investigative Divisions. Following the 2018 midterm elections, the FBI expanded the scope of the FITF. Previously our efforts were focused solely on the threat posed by Russia. However, we now have units working to confront malign foreign influence operations, not just from Russia, but also from China, Iran, and other global adversaries. We have refined and focused our strategy.

Through the FITF, the FBI takes a three-pronged approach to the serious threat. The first prong focuses on our investigations and operations. The FITF works with the FBI's 56 field offices to open investigations with a foreign influence nexus. You might think of the FITF as a hub with FBI field offices and its personnel as the spokes. Our investigative approach seeks to impose costs on our adversaries, specifically key influencers, and enablers. Investigations with a cyber nexus are worked collaboratively with the FBI Cyber Division and Cyber Task Forces. This way, the FBI can quickly respond to threats to election infrastructure. Moreover, the FBI Cyber Division works closely with the U.S. intelligence community to work to determine attribution.

The second prong centers on information and intelligence sharing. The FBI works closely with our fellow intelligence community agencies as well as with State and local law enforcement partners and election officials to share intelligence to help, disrupt, and deter our adversaries. In 2018, that effort led to the creation of Protected Voices, a joint initiative between the FBI, Department of Justice, Department of Homeland Security, United States Secret Service, and the ODNI. Through Protected Voices, we developed a series of videos to help political campaigns better understand this threat and made them available through the FBI's public website.

In the past months, we have expanded Protected Voices, providing webinars and in-person briefings to the Presidential campaigns on cyber and malign influence threats. Currently, we are expanding the audience to include congressional campaigns and the general public. We collaborate extensively with our U.S. government partners to provide information to State and local governments, election officials, private election vendors, and social media companies so that they can harden their systems against cyberattacks. Collaboration builds a common understanding of the threat landscape.

The last prong of our approach is private sector partnerships. Technology companies have a frontline responsibility to secure their own networks, products, and platforms. We're doing our part by providing actionable intelligence to better enable them to address abuse of their platform by foreign actors. The FBI has established relationships with these technology and social media companies and maintains an ongoing dialogue to enable a rapid exchange of threat information.

Across all these prongs, the FBI is constantly reviewing the effectiveness of its coordination and its outreach. To our knowledge, no foreign government has attempted to tamper with U.S. vote counts. However, even doubts about whether it has occurred can be damaging. We do know our adversaries are actively trying to influence electoral processes and outcomes in advance of the 2020 election. While our focus today is on election security, I want to note these adversaries seek to influence our national policies and public opinions in important ways beyond just elections.

We look forward to continuing this important work and appreciate the support of this committee. Thank you again for the opportunity to appear before you today. I'm happy to answer any questions you may have.

[The statement of Ms. Floris follows:]



Department of Justice

STATEMENT OF

**NIKKI FLORIS
DEPUTY ASSISTANT DIRECTOR
COUNTERINTELLIGENCE DIVISION
FEDERAL BUREAU OF INVESTIGATION**

BEFORE THE

**COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES**

**AT A HEARING ENTITLED
"SECURING AMERICA'S ELECTIONS PART II:
OVERSIGHT OF GOVERNMENT AGENCIES"**

PRESENTED

OCTOBER 22, 2019

STATEMENT OF
NIKKI FLORIS
DEPUTY ASSISTANT DIRECTOR
COUNTERINTELLIGENCE DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
“SECURING AMERICA’S ELECTIONS PART II: OVERSIGHT OF GOVERNMENT AGENCIES”

PRESENTED
OCTOBER 22, 2019

Chairman Nadler, Ranking Member Collins, and Members of the Committee, I am pleased to appear before you today to discuss the FBI’s efforts to combat foreign influence operations.

As Director Wray described during his all House and Senate briefing on this issue, we face multi-faceted foreign threats to our election security. And while our focus today is on election security, these adversaries are seeking to influence our national policies and public opinion in important ways beyond electoral cycles.

Foreign influence operations—which include covert, coercive, or corrupt actions by foreign governments to influence U.S. political sentiment or public discourse, or interfere in our processes themselves—are not a new problem. But the interconnectedness of the modern world, combined with the anonymity of the Internet, have changed the nature of the threat and how the FBI and its partners must address it. The goal of these foreign influence operations directed against the United States is to mislead, sow discord, and, ultimately, undermine confidence in our democratic institutions and values.

Foreign influence operations have taken many forms and used many tactics over the years. Most widely reported these days are attempts by adversaries—hoping to reach a wide swath of Americans covertly from outside the United States—to use false personas and fabricated stories on social media platforms to discredit U.S. individuals and institutions.

The FBI is the lead federal agency responsible for investigating foreign influence operations. In the fall of 2017, Director Christopher Wray established the Foreign Influence Task Force (“FITF”) to identify and counteract malign foreign influence operations targeting the United States.

The FITF is led by the Counterintelligence Division and is comprised of agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions. It is specifically charged with identifying and combating foreign influence operations targeting democratic institutions and values inside the United States. In all instances, the FITF strives to protect democratic institutions and public confidence; develop a common operating picture; raise adversaries' costs; and, reduce their overall asymmetric advantage.

The task force brings the FBI's national security and traditional criminal investigative expertise under one umbrella to prevent foreign influence in our elections. This better enables us to frame the threat, to identify connections across programs, to aggressively investigate as appropriate, and – importantly – to be more agile.

Coordinating closely with our partners and leveraging relationships we have developed in the technology sector, we had a number of instances where we were able to quickly relay threat indicators that those companies used to take swift action, blocking budding abuse of their platforms.

Following the 2018 midterm elections, we reviewed the threat and the effectiveness of our coordination and outreach. As a result of this review, we further expanded the scope of the FITF. Previously, our efforts to combat malign foreign influence focused solely on the threat posed by Russia. Utilizing lessons learned over the last year and half, the FITF is widening its aperture to confront malign foreign operations of China, Iran, and other global adversaries. To address this expanding focus and wider set of adversaries and influence efforts, we have also added resources to maintain permanent “surge” capability on election and foreign influence threats.

We have also further refined our approach. All efforts are based on a three-pronged approach, which includes: investigations and operations; information and intelligence sharing; and, a strong partnership with the private sector.

Investigations and operations:

Our Foreign Influence Task Force partners with the 56 field offices across the country on open FBI investigations with a foreign influence nexus. Think of the Task Force as the hub, with spokes out to our 56 field offices, and our expansive front line agents, analysts, and professional staff. Investigations with a cyber nexus are worked collaboratively with our Cyber Division and the Cyber Task Forces throughout the nation to quickly respond to these threats to protect systems and work with the Intelligence Community to determine attribution.

Our investigative approach also seeks to affirmatively impose costs on our adversaries, particularly key influencers or enablers. Just last fall, we charged Elena Khusyaynova, a Russian national, with criminal violations stemming from her efforts to influence the 2016 and 2018 elections in her role as Chief Accountant for Project Lakhta—a Russian disinformation

organization (connected to the Internet Research Agency) that had budgeted over \$10 million in the first half of 2018 alone for initiatives to undermine the U.S. political system and candidates.

Another Russian national, Maria Butina, was sentenced in federal court a few months ago for conspiring with a Russian intelligence service to influence unwitting American political organizations and advocacy groups.

Information and intelligence sharing:

Make no mistake, we are working closely with our partners at every level to establish a common understanding of the threat landscape, share intelligence, and detect, disrupt, and deter our adversaries. In 2018, that effort culminated in the creation of *Protected Voices*.

Through this program, we developed a series of videos, available through the FBI's public website, to help political campaigns better understand this threat. In the past months, we have expanded Protected Voices, providing webinars and in-person briefings to the presidential campaigns on cyber and malign foreign influence threats. In the coming months, the FBI will further expand the audience to include congressional campaigns and their many supporting entities.

The FBI, in partnership with ODNI and DHS, is working to update and expand this resource for the 2020 election season, to provide even more information on how to identify and report foreign intelligence efforts against campaigns and their staffs.

We also are collaborating extensively with our U.S. Government partners, particularly DHS, to provide information nationwide to state governments, local election officials, private election vendors, and others so they can harden their systems against cyberattacks. The majority of technical information the FBI has been able to provide these groups and the public since 2016 was a direct result of self-reporting and cooperation with the FBI from social media companies and election officials and vendors. By partnering with the FBI, these groups are helping the nation combat our adversaries' activities.

Relationship with the private sector:

Technology companies have a front-line responsibility to secure their own networks, products, and platforms. We have provided actionable intelligence to help them address abuse of their platforms by foreign actors. In turn, social media companies have passed to FBI several hundred previously unknown accounts being used by bad actors, which we, in turn, have shared with our partners in the wider Intelligence Community.

In the run up to the 2018 mid-term elections, social media companies deactivated more than 1,000 inauthentic social media accounts linked to malign foreign influence actors. The companies made these decisions informed by dialogue and information exchanges with the FBI and other government agencies.

Our relationship with social media companies works best when they also give us notice when they see foreign threat actors testing out new techniques and tactics online. That helps us refine, enhance, and sharpen our efforts to tackle this threat.

Conclusion

To our knowledge, no foreign government has attempted to tamper with U.S. vote counts. We do know that our adversaries are actively trying to influence public opinion and electoral processes in advance of the 2020 election.

We must continue to take this threat seriously, be ready to evolve as it inevitably will, and keep tackling it with fierce determination and focus.

We look forward to continuing this important work and appreciate the support of this committee. Thank you for the opportunity to appear before you today. I am happy to answer any questions you may have.

Ms. SCANLON. Thank you very much. Mr. Hickey?

TESTIMONY OF ADAM HICKEY

Mr. HICKEY. Good morning, distinguished Members of the committee, and thank you for the opportunity to testify on behalf of the Justice Department concerning our efforts to ensure the safety and security of our Nation's election infrastructure and to combat malign foreign influence.

By "malign foreign influence," I'm referring to covert actions by foreign governments intended to affect U.S. political sentiment and public discourse, sow divisions in our society, or undermine confidence in our democratic institutions. And these can range from computer hacking that targets election infrastructure or political parties to state-sponsored media campaigns. This issue, protecting our Nation's democratic processes, has been and remains a top priority of the Department. Our principle role here is the investigation and prosecution of Federal crimes, but malign foreign influence efforts extend beyond efforts to interfere with elections, and they require more than law enforcement responses alone.

Recognizing that, we approach this national security threat the same as any other, by using our own legal tools as well as supporting the tools and authorities of others. To the best of our ability, we try to prevent crimes from occurring or disrupt them in progress, in part by sharing information with people and institutions to allow them to better protect themselves.

Reflecting the priority of these issues, last year the Attorney General's Cyber Digital Task Force analyzed the types of foreign influence operations and laid out a framework to guide our responses. Since the 2016 election, we have taken a number of steps to combat malign foreign influence and support secure elections. First, as an intelligence-driven organization and member of the intelligence community, the FBI pursues tips and leads, including from classified information, to identify, investigate, and disrupt illegal foreign influence activities. To that end, and as DAD Floris already explained, the FBI established the Foreign Influence Task Force to lead its response to ensure information flow, resource allocation, and coordination, both within the Department and among the Department, our Federal partners, and the private sector.

Second, together with other agencies through a series of outreach and education efforts, we've been helping public officials, candidates, and social media companies to harden their own networks and platforms against malign foreign influence operations. Third, we have improved enforcement of the Foreign Agents Registration Act, one of the statutory tools that helps ensure transparency in the activities of foreign entities and individuals. Effective FARA enforcement makes it more difficult for those entities and individuals to hide their role in activities occurring with the United States.

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

financial sanctions imposed by the Secretary of the Treasury. Finally, even outside the context of criminal charges, we have used the information from our investigations both to warn and to reassure potential victims and the general public alike about malign foreign influence activities.

Now, victim notifications, defensive counterintelligence briefings, and public safety announcements are traditional Department activities, but they must conduct with particular sensitivity in the context of foreign influence and elections. In some circumstances, exposure can be counterproductive or otherwise imprudent. Given countervailing considerations, the Department has adopted a public policy for evaluating whether and how to disclose malign foreign influence activities, and among its first principles, partisan political considerations must play no role in our decisions.

Our adversaries will undoubtedly change their tactics, and we will need to be nimble in our response, but the framework we have developed to respond will have staying power. As you can see, the Department plays an important role in combatting foreign efforts to interfere in our elections. There are limits to our role and that of the Federal Government as a whole. Combatting malign foreign influence requires a whole of society approach that relies on coordinated actions by government agencies at various levels, support from the private sector, and the active engagement of an informed public.

Thank you again, and I look forward to your questions.

[The statement of Mr. Hickey follows:]



Department of Justice

STATEMENT OF

**ADAM S. HICKEY
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE**

BEFORE THE

**COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES**

AT A HEARING ENTITLED

**"SECURING AMERICA'S ELECTIONS PART II:
OVERSIGHT OF GOVERNMENT AGENCIES"**

PRESENTED

OCTOBER 22, 2019

STATEMENT OF
ADAM S. HICKEY
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE
COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
“SECURING AMERICA’S ELECTIONS PART II:
OVERSIGHT OF GOVERNMENT AGENCIES”

OCTOBER 22, 2019

Good morning, Chairman Nadler, Ranking Member Collins, and distinguished Members of the Committee. Thank you for the opportunity to testify on behalf of the Department of Justice concerning our efforts to ensure the safety and security of our nation’s elections and to combat malign foreign influence.

Protecting our Nation’s democratic processes, including our elections, is among the Department’s top priorities, and malign foreign influence operations targeting those processes are among the most pressing threats our Nation faces. The Department appreciates the Committee’s interest in making sure that we have the tools we need to target those who may seek to do us harm by interfering in our elections.

As I describe below, the Department’s principal role in combatting election interference is the investigation and prosecution of Federal crimes, but our investigations can yield more than criminal charges to protect national security. Malign foreign influence efforts extend beyond efforts to interfere with elections, and they require more than law enforcement responses alone. I will cover three areas in my testimony today. First, I will describe what we mean by the term “malign foreign influence operations” and provide examples of operations we have observed in the past. Second, I will discuss how the Department has categorized recent malign foreign influence operations targeting our elections. Third, I will explain how the Department is responding to those operations and how our efforts fit within the “whole of society” approach that is necessary to defeat malign foreign influence operations.

I. Background on Malign Foreign Influence Operations

For these purposes, malign foreign influence operations include covert actions by foreign governments intended to affect U.S. political sentiment and public discourse, sow divisions in

our society, or undermine confidence in our democratic institutions to achieve strategic objectives.

Malign foreign influence operations aimed at the United States are not a new problem. These efforts have taken many forms across the decades, from covertly funding newspapers and forging internal government communications to more recently creating and operating false U.S. personas on Internet sites designed to attract U.S. audiences and spread divisive messages. The nature of the problem, however—and how the U.S. government must combat it—are changing as advances in technology allow foreign actors to reach unprecedented numbers of Americans covertly and without setting foot on U.S. soil. Fabricated news stories and sensational headlines like those sometimes found on social media platforms are just the latest iteration of a practice foreign adversaries have long employed in an effort to discredit and undermine individuals or organizations in the United States. Although the tactics have evolved, the goals of these activities remain the same: to spread disinformation and to sow discord on a mass scale in order to weaken the U.S. democratic process, and ultimately to undermine the appeal of democracy itself.

As one deliberate component of this strategy, malign foreign influence operations have targeted U.S. elections. Indeed, elections are a particularly attractive target for malign foreign influence campaigns, because they provide an opportunity to undermine confidence in a core element of our democracy: the process by which we select our leaders. As explained in the January 2017 report by the Office of the Director of National Intelligence (“ODNI”) addressing Russian interference in the 2016 U.S. presidential election, Russia has had a “longstanding desire to undermine the U.S.-led liberal democratic order,” and that nation’s recent election-focused “activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations.”¹ Russia’s malign foreign influence campaign, according to ODNI, “followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or ‘trolls.’”²

Russia’s malign foreign influence campaign did not end with the 2016 election. On the eve of the 2018 midterm election, ODNI, the Department of Homeland Security, the Department of Justice, and the Federal Bureau of Investigation (“FBI”) informed the public: “Americans should be aware that foreign actors—and Russia in particular—continue to try to influence public sentiment and voter perceptions through actions intended to sow discord. They can do this by spreading false information about political processes and candidates, lying about their own interference activities, disseminating propaganda on social media, and through other

¹ Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, at ii (Jan. 2017) (“ODNI Report”), available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf (last accessed Oct. 7, 2019).

² ODNI Report at 2.

tactics.”³ After the election, the Director of National Intelligence confirmed: “Russia, and other foreign countries, including China and Iran, conducted influence activities and messaging campaigns targeted at the United States to promote their strategic interests.”⁴ Last month, the Department of the Treasury sanctioned Russian actors who “used fictitious personas on social media and disseminated false information in an effort to attempt to influence the 2018 U.S. midterm elections and try to undermine faith in U.S. democratic institutions.”⁵ Importantly, however, the Departments of Justice and Homeland Security jointly concluded that “there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political/campaign infrastructure used in the 2018 midterm elections for the United States Congress.”⁶

Malign foreign influence operations are not limited to elections and voter perceptions. They also attempt to influence public policy, including by leveraging businessmen, exploiting credible surrogates like law firms, using media organizations, and targeting student organizations and funding on our college campuses. China, in particular, has been working to influence American public opinion in its favor. As the Vice President said last October, quoting the Intelligence Community (“IC”): “China is targeting U.S. state and local governments and officials to exploit any divisions between federal and local levels on policy. It’s using wedge issues, like trade tariffs, to advance Beijing’s political influence.”⁷ The Department remains “concerned that Beijing may use its economic leverage over businesses to covertly influence American policy, may covertly influence student groups on campus to monitor or retaliate

³ Joint Statement on Election Day Preparations (Nov. 5, 2018), available at: <https://www.dhs.gov/cisa/news/2018/11/05/joint-statement-election-day-preparations> (last accessed Oct. 7, 2019).

⁴ Daniel R. Coats, Director of National Intelligence, Statement on the Intelligence Community’s Response to Executive Order 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election (Dec. 21, 2018), available at: <https://www.dni.gov/index.php/newsroom/press-releases/item/1933-dni-coats-statement-on-the-intelligence-community-s-response-to-executive-order-13848-on-imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election> (last accessed Oct. 7, 2019).

⁵ U.S. Department of the Treasury, Treasury Targets Assets of Russian Financier who Attempted to Influence 2018 U.S. Elections (Sept. 30, 2019), available at: <https://home.treasury.gov/news/press-releases/sm787> (last accessed Oct. 7, 2019).

⁶ Acting Attorney General and Secretary of Homeland Security Submit Joint Report on Impact of Foreign Interference on Election and Political/Campaign Infrastructure in 2018 Elections (Feb. 5, 2019), available at: <https://www.justice.gov/opa/pr/acting-attorney-general-and-secretary-homeland-security-submit-joint-report-impact-foreign> (last accessed Oct. 7, 2019).

⁷ Vice President Mike Pence’s Remarks on the Administration’s Policy Towards China (Oct. 4, 2018), available at: <https://www.hudson.org/events/1610-vice-president-mike-pence-s-remarks-on-the-administration-s-policy-towards-china102018> (last accessed Oct. 7, 2019).

against fellow students, or may exercise undisclosed control over media organizations in the United States.”⁸ Malign foreign influence operations, from any adversary, require a strong response.

II. Types of Foreign Influence Operations

To help identify how the Department can more effectively accomplish its mission in this vital and evolving area, the Department drafted an analysis of the types of foreign influences that can target democratic and electoral processes as well as the Department’s responses to counter them. That analysis is included in the first chapter of the Report of the Attorney General’s Cyber-Digital Task Force, released in July 2018.⁹ It includes a framework for categorizing the types of foreign influence activity our adversaries could engage in:

1. Cyber operations targeting election infrastructure. Such operations could seek to undermine the integrity or availability of election-related data. For example, adversaries could employ cyber-enabled or other means to target election infrastructure, such as voter registration databases and voting machines. Operations aimed at removing otherwise eligible voters from the rolls or attempting to manipulate the results of an election (or even just disinformation suggesting that such manipulation has occurred) could undermine the integrity and legitimacy of elections, as well as public confidence in election results. To our knowledge, no foreign government has succeeded in perpetrating ballot fraud,¹⁰ but raising even the doubt that it has occurred could be damaging.

2. Cyber operations targeting political organizations, campaigns, and public officials. These operations could seek to compromise the confidentiality of private information of the targeted groups or individuals, as well as its integrity. For example, adversaries could conduct cyber or other operations against U.S. political organizations and campaigns to steal confidential information and use that information, or alterations thereof, to discredit or embarrass candidates, undermine political organizations, or impugn the integrity of public officials.

3. Covert influence operations to assist or harm political organizations, campaigns, and public officials. For example, adversaries could conduct covert influence operations to provide assistance that is prohibited from foreign sources to political organizations, campaigns, and government officials. These intelligence operations might involve covert offers of financial,

⁸ *China’s Non-Traditional Espionage Against The United States: The Threat And Potential Policy Responses: Hearing before the Senate Judiciary Committee* (Dec. 12, 2018) (statement of John C. Demers, Assistant Attorney General for National Security), available at: <https://www.judiciary.senate.gov/imo/media/doc/12-12-18%20Demers%20Testimony.pdf> (last accessed Oct. 7, 2019).

⁹ Countering Malign Foreign Influence Operations, in Report of the Attorney General’s Cyber-Digital Task Force, at 1-21 (July 2, 2018), available at: <https://www.justice.gov/ag/page/file/1076696/download> (last accessed Oct. 7, 2019).

¹⁰ “The term “ballot fraud” in this context includes fraud in the processes by which voters are registered or by which votes are cast or tabulated.

logistical, or other campaign support to, or covert attempts to influence the policies or positions of, unwitting politicians, party leaders, campaign officials, or even the public.

4. Covert influence operations, including disinformation operations, to influence public opinion and sow division. Using false U.S. personas, adversaries could covertly create and operate social media pages and other forums designed to attract U.S. audiences and spread disinformation or divisive messages. These messages need not relate directly to campaigns. They may seek to depress voter turnout among particular groups, encourage third-party voting, or convince the public of widespread voter fraud in order to undermine confidence in election results.

5. Overt influence efforts, such as the use of foreign media outlets or other organizations to influence policymakers and the public. For example, adversaries could use state-owned or state-influenced media outlets to reach U.S. policymakers or the public. Governments can disguise these outlets as independent, while using them to promote divisive narratives and political objectives.

III. The Department of Justice's Role in Addressing Malign Foreign Influence Operations

The Department of Justice, including the FBI, has a significant role in investigating and disrupting foreign government activity inside the United States that threatens U.S. national security. Through our own authorities and in close coordination with our partner Departments and agencies, the Department can act against threats posed by malign foreign influence operations in several ways.

First, as an intelligence-driven organization and member of the IC, the FBI can pursue tips and leads, including from classified information, to identify, investigate, and disrupt illegal foreign influence activities. With both law enforcement and intelligence authorities, the FBI is the lead Federal agency responsible for investigating foreign influence operations. The FBI also works closely with its IC partners, as well as the Department of Homeland Security ("DHS"), to detect and disrupt cyber threats to election infrastructure, including by monitoring real-time election incidents and providing real-time reporting.

Second, the Department assists election officials, other public officials, candidates, and social media companies in hardening their own networks, products, and platforms against malign foreign influence operations. For example, the FBI, DHS, and ODNI have developed joint briefings—to provide officials and candidates with steps they can undertake to mitigate such threats, and the FBI has developed a "Protected Voices" online initiative to raise their awareness about the best ways to fend off possible attempts to infiltrate their infrastructure.¹¹ In conducting these efforts, we are mindful that States and localities are primarily responsible for administering federal elections under Article I, Section 4 of the Constitution, and we are committed to avoiding any interference with their lawful processes. Further, primarily through the FBI, the Department maintains strategic relationships with social media providers, which are responsible for securing

¹¹ FBI, Protected Voices, available at: <https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices> (last accessed Oct. 7, 2019).

their own products, platforms, and services from malign foreign influence threats. By sharing information with them, the FBI can help providers with their own initiatives to track malign foreign influence activity, to enforce terms of service that prohibit the use of their platforms for such activities, and to refer identified malign foreign influence operations back to the FBI. (This approach is similar to the Department's approach in working with social media providers to address terrorists' use of social media.)

Third, the Department identifies and exposes foreign influence operations through the National Security Division's enforcement of the Foreign Agents Registration Act, 22 U.S.C. § 611 *et seq.* ("FARA"), among other statutes. FARA helps to ensure transparency in the activities of foreign entities and individuals, and makes it more difficult for those entities and individuals to hide their role in activities occurring in the United States. It requires persons who engage in certain conduct as agents of foreign principals to register with DOJ and to file periodic reports thereafter. The filings must disclose all aspects of the agent's relationship with the foreign principal, including activities by the agent within the United States on behalf of the foreign principal. FARA's purpose is to ensure that the American public and our lawmakers know the source of information that is provided at the behest of a foreign principal, where that information may be intended to influence U.S. public opinion, policy, and laws. The statute enhances the public's and the government's ability to evaluate such information.

While the Department has always enforced FARA, we have recently stepped up enforcement efforts, including by educating prosecutors nationwide about the importance of the statute, expanding our outreach to individuals and entities who may be obligated to register, and raising public awareness. In 2018 alone, more than 20 individuals and entities were criminally charged with violations involving FARA—more than the total number charged in the prior 50 years. The increased enforcement efforts also include the use of civil enforcement actions, which the Department used for the first time since 1991 to obtain a court order in May 2019 requiring a U.S. agent of a Russian state-owned media enterprise to register.¹² The Department's efforts have resulted in the registrations of multiple foreign-media entities that had not fulfilled their FARA obligations, including the U.S. agents of Russian state-funded media networks RT and Sputnik and of China's state-controlled television network, CGTN. At current rates, the Department is on track to double the number of new registrants and new foreign principals registering annually as of 2016. The Department has likewise increased the number of inspections of existing registrants, to audit compliance with their record-keeping and reporting obligations, by more than 30 percent compared to prior years. Moreover, the Department has adopted a new online system for filing, reviewing, and searching registrations to facilitate compliance with FARA, enhance public access to FARA registrations, and make information on foreign political activities more transparent.¹³ Optical character recognition technology has

¹² See Department of Justice, Court Finds RM Broadcasting Must Register as a Foreign Agent (May 13, 2019), available at: <https://www.justice.gov/opa/pr/court-finds-rm-broadcasting-must-register-foreign-agent> (last accessed Oct. 7, 2019).

¹³ See Department of Justice, The Department of Justice Announces Launch of New Process for Filing Documents Pursuant to the Foreign Agents Registration Act of 1938 (FARA)

rendered online historical filings text-searchable and permits bulk download of results for analysis. We continually seek to improve the efficiency, transparency, and utility of the FARA website¹⁴ to the extent possible in light of technology and funding.

Increased FARA enforcement and transparency is also a critical prong of the Department's China Initiative. Under the Initiative, the Department educates American colleges and universities about potential threats to academic freedom and open discourse from covert Chinese malign influence efforts, raises awareness among the business community that acting as an agent of the Chinese government could trigger obligations to register under FARA, and continues to evaluate whether foreign media organizations operating under the editorial direction or control of a foreign government are complying with FARA.

Fourth, the Department's investigations may expose conduct that warrants criminal charges. Foreign influence operations, though not always illegal, can implicate several U.S. Federal criminal statutes. For example, FARA includes a criminal penalty for willful violations, 22 U.S.C. § 618, and another statute, 18 U.S.C. § 951, prohibits agents of foreign governments from acting in the United States without prior notification to the Attorney General.¹⁵ Criminal charges uphold the Constitution's prescription that the President "shall take care that the laws be faithfully executed," U.S. Const. art. II, § 3, pursue justice, and deter similar conduct in the future. We work with other nations to obtain custody of foreign defendants whenever possible, and those who seek to avoid justice in U.S. courts will find their freedom of travel significantly restricted. Criminal charges also provide the public with information about the activities of foreign actors we seek to hold accountable and raise awareness of the threats we face.

For example, in July 2018, a Russian national named Mariia Butina was charged with conspiring to act as a Russian agent within the United States by taking direction from the Russian government to develop backchannels of communication with Americans in an effort to influence them for Russia's eventual advantage.¹⁶ She pleaded guilty and, in April 2019, was

(Sept. 25, 2019), available at: <https://www.justice.gov/opa/pr/department-justice-announces-launch-new-process-filing-documents-pursuant-foreign-agents> (last accessed Oct. 7, 2019).

¹⁴ Department of Justice, National Security Division, Foreign Agents Registration Act, available at: <https://www.justice.gov/nsd-fara> (last accessed Oct. 7, 2019).

¹⁵ Other statutes that the Department may use to prosecute unlawful foreign influence operations include, but are not limited to, 18 U.S.C. § 371 (conspiracy to defraud the United States); 18 U.S.C. § 1001 (false statements); 18 U.S.C. § 1028A (aggravated identity theft); 18 U.S.C. § 1030 (computer fraud and abuse); 18 U.S.C. §§ 1343, 1344 (wire fraud and bank fraud); 18 U.S.C. § 1519 (destruction of evidence); 18 U.S.C. § 1546 (visa fraud); and 52 U.S.C. §§ 30109, 30121 (foreign contributions, donations, or expenditures).

¹⁶ See Department of Justice, Russian National Charged in Conspiracy to Act as an Agent of the Russian Federation Within the United States (July 16, 2018), available at:

sentenced to 18 months in prison.¹⁷ And in September 2018, the Department filed a criminal complaint against Elan Alekseevna Khusyaynova, who is alleged to have been the chief accountant for the Internet Research Agency's Project Lakhta, a Russian malign influence operation that included efforts to influence the 2018 midterm election.¹⁸ The complaint alleged that the operation's goal was to sow division and discord in the U.S. political system, including by influencing the 2018 midterm election through "information warfare against the United States" conducted through fictitious U.S. personas on social media platforms and other Internet-based media. Over the last two years, the Department has brought several other cases against Russian actors exposing malign influence activities.¹⁹

<https://www.justice.gov/opa/pr/russian-national-charged-conspiracy-act-agent-russian-federation-within-united-states> (last accessed Oct. 7, 2019).

¹⁷ See Department of Justice, Russian National Sentenced to 18 Months in Prison for Conspiring to Act As an Agent of the Russian Federation within the United States (Apr. 26, 2019), available at: <https://www.justice.gov/opa/pr/russian-national-sentenced-18-months-prison-conspiring-act-agent-russian-federation-within> (last accessed Oct. 7 2019).

¹⁸ See Department of Justice, Russian National Charged with Interfering in U.S. Political System (Oct. 19, 2018), available at: <https://www.justice.gov/usao-edva/pr/russian-national-charged-interfering-us-political-system> (last accessed Oct. 7, 2019).

¹⁹ In February 2018, 13 Russian nationals and three Russian companies, including the Internet Research Agency and its alleged financier Yevgeny Prigozhin, were indicted on conspiracy charges related to a Russian malign influence effort designed to interfere with the 2016 election. See Department of Justice, Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System (Feb. 16, 2018), available at: <https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere> (last accessed Oct. 7, 2019). In July 2018, 12 Russian officials of the Main Intelligence Directorate of the General Staff ("GRU") were indicted on charges related to the hacking and leaking of emails as part of the Russian effort to interfere in the 2016 election. See Department of Justice, Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election (July 13, 2018) <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election> (last accessed Oct. 7, 2019).

The Department's efforts in this regard are not limited to malign influence activities targeting elections. In October 2018, seven Russian officers in the GRU were indicted on computer hacking and other charges related to a Russian malign influence effort designed to undermine, retaliate against, and otherwise delegitimize the efforts of international anti-doping organizations and officials who had publicly exposed a Russian state-sponsored athlete doping program and to damage the reputations of athletes around the world. See Department of Justice, U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations (Oct. 4, 2018), available at: <https://www.justice.gov/opa/pr/us->

Fifth, the Department's investigations can support the actions of other U.S. government agencies using diplomatic, intelligence, military, and economic tools. For example, in several recent cases, the Secretary of the Treasury has imposed financial sanctions on defendants abroad under executive orders that authorize the imposition of sanctions for malicious cyber-enabled activity or for election interference.²⁰ Treasury's action blocked all property and interests in property of the designated persons subject to U.S. jurisdiction and prohibited U.S. persons from engaging in transactions with the sanctioned individuals. The Department has also worked with ODNI, DHS, and other Federal partners to carry out its responsibilities under Executive Order 13848, *Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election* (Sept. 12, 2018). Pursuant to that Executive Order, the FBI provided information to support ODNI's classified assessment to the President of any information indicating that a foreign government, or any person acting as an agent of or on behalf of a foreign government, acted with the intent or purpose of interfering in the 2018 midterm election. Subsequently, on February 4, 2019, the Departments of Justice and Homeland Security submitted their own classified joint report to the President evaluating the impact of foreign activities identified in ODNI's assessment on the security or integrity of election infrastructure or the infrastructure of political organizations, campaigns, or candidates used in the 2018 midterm election (referenced above).

Finally, in appropriate cases, information gathered during our investigations can be used—either by the Department or in coordination with our U.S. government partners—to alert targets, other affected individuals, and the public to malign foreign influence activities. Victim notifications, defensive counterintelligence briefings, and public safety announcements are traditional Department activities, but they must be conducted with particular sensitivity in the context of foreign influence and elections. In many circumstances, exposing foreign interference operations can be an important means of rendering them less effective and maintaining confidence in our democratic processes and institutions. In some circumstances, however, exposure can be counterproductive or otherwise imprudent, for example, if it may amplify an operation or create undue public alarm, harm, or confusion. Given the countervailing considerations, the Department has adopted a policy for evaluating whether to disclose malign foreign influence activities.²¹ The policy recognizes that exposing such activity may play an important role in mitigating the effect of malign foreign influence efforts, provides relevant factors for consideration, and requires that partisan political considerations must play no role in efforts to disclose malign foreign influence activities.

charges-russian-gru-officers-international-hacking-and-related-influence-and (last accessed Oct. 7, 2019).

²⁰ Executive Order 13694 (Apr. 1, 2015), as amended by Executive Order 13757 (Dec. 29, 2016); Executive Order 13848 (Sept. 12, 2018).

²¹ See Justice Manual 9-90.730 (Sept. 2018), adopting DOJ Policy on Disclosure of Foreign Influence Operations, in *Report of the Attorney General's Cyber-Digital Task Force*, pp. 16-17 & nn.18-20 (July 2, 2018), available at: <https://www.justice.gov/ag/page/file/1076696/download> (last accessed Oct. 7, 2019).

In taking these actions, we are alert to ways in which current law may benefit from reform. By providing ready access to the American public and policymakers from abroad, the Internet makes it easier for foreign governments to evade restrictions on undeclared activities in the United States and mask their identities while reaching an intended audience. We welcome the opportunity to work with Congress to combat malign foreign influence operations, including those aimed at our elections, by clarifying or expanding our laws to provide new tools or sharpen existing ones, if appropriate.

IV. Conclusion

The nature of malign foreign influence operations will continue to change as technology and our foreign adversaries' tactics continue to change. Our adversaries will persist in seeking to exploit the diversity and richness of today's information space, and the tactics and technology they employ will continue to evolve.

The Department plays an important role in combating foreign efforts to interfere in our elections. At the same time, it cannot and should not attempt to address the problem alone. There are limits to the Department's role—and the role of the U.S. government more broadly—in addressing malign foreign influence operations aimed at sowing discord and undermining our institutions. Combating malign foreign influence operations requires a “whole of society” approach that relies on coordinated actions by Federal, State, and local government agencies; support from the private sector; and the active engagement of an informed public.

* * *

I want to thank the Committee again for providing me this opportunity to discuss these important issues on behalf of the Department. We look forward to continuing to work with Congress to improve our ability to respond to this threat. I am happy to answer any questions you may have.

Ms. SCANLON. Thank you very much. Mr. Hovland?

TESTIMONY OF BEN HOVLAND

Mr. HOVLAND. Good morning, Members of the committee. I thank you for the opportunity to testify before you this morning to detail the work of the U.S. Election Assistance Commission, better known as the EAC, to fulfill its mission under the Help America Vote Act, or HAVA. I also appreciate this opportunity to highlight the great work of State and local election officials around the country.

As you know, our Nation's elections are run at the State and local levels, with each of the 50 States and U.S. territories running elections in different ways. Election officials in over 8,000 local jurisdictions are ultimately responsible for conducting our elections, and their work truly protects and ensures the most fundamental pillar of our democracy, the vote.

Since 2016, there has been enormous increase and focus on the security of our elections, which is just one of the many responsibilities' election officials must address. I'm pleased to report from my vantage point the elections community has responded in an impressive fashion considering the challenges we face. Nearly every conference I attend while traveling around the country has a substantial focus on security and protecting the integrity of elections is a constant topic in meetings with election administrators, our Federal partners, and external stakeholders.

Even so, we need to ask ourselves a key question: Will that be enough if election officials do not have the sustained resources they need to defend our democracy against potential threats? The good news is that following the Department of Homeland Security's designation of election infrastructure as critical infrastructure, there has been a sea change in information sharing between the Federal Government and State and local officials. This includes the creation of a Government Coordinating Council, which brings together State and local officials with Federal partners, as well as a Sector Coordinating Council, which has helped organize private sector vendors and nonprofit entities that support local election officials.

We've also seen the creation of the Election Infrastructure Information and Sharing Analysis Center, or EIISAC, which now has over 2,100 Members, including every State chief election official's office. The deployment of Albert monitors, hardening of systems, increased trainings, and promotion of tabletop exercises around cyber events have all exponentially increased since 2016. The Fiscal Year 2018 appropriations of \$380 million of HAVA funding, which the EAC distributed within months of its allocation, has largely contributed to these improvements. It doesn't cover everything election officials need, but States have had the ability to essentially choose from a menu of reforms, improvements, and priorities that could address their most pressing needs and vulnerabilities.

As Chairwoman McCormick testified earlier this year, the EAC projects that 85 percent of the Fiscal Year 2018 money will be spent in advance of 2020. We've seen some States use the funding to replace aging or paperless equipment. Other States have replaced their statewide voter registration database or added additional security measures, like multi-factor authentication. Some

have hosted essential training and tabletop exercises ahead of 2020 to give election officials a hands-on experience that can help them prepare for various threats.

One of my personal favorite uses of the Fiscal Year 2018 funding is the implementation of cyber navigator programs. Essentially, the State recognizes that many local jurisdictions do not have the capacity or need for a full-time election cybersecurity expert, so the State employs individuals with regional responsibilities, and they provide technical assistance to several counties or municipalities. This is the kind of innovative program that will help bolster our cybersecurity defenses and improve how States conduct elections. It's also a model that the EAC would like to help amplify nationwide should our funding support such an effort.

Unfortunately, not all the news is good. As you know, the threat of foreign adversaries remains real, and ultimately our State and local election officials do not have the resources to thwart a truly determined and sophisticated nation-state actor. That is why we must take action to build resilience here at home and implement policies that deter adversaries abroad, such as a real sanctions regime. Additional funding is crucial to allow States to continue to make necessary improvements that increase the strength and resiliency of our election systems.

When we talk about election Administration, we are talking about the infrastructure of our democracy. To make meaningful and lasting change requires a consistent investment over time. It cannot just be about 2020 or any one election, but about all our elections going forward. During a Senate Rules Committee hearing in May, I shared a recent discovery that the EAC's operating budget of \$7.95 million is less than the amount Kansas City spends on potholes. It's startling to think that one city with a population of around 500,000 people invests more to protect its residents' car titles and alignment than our country invests in the only Federal agency dedicated completely to improving election Administration and helping more than 200 million registered voters cast their ballot.

I thank you for your time, and I'm happy to answer any questions you may have.

[The statement of Mr. Hovland follows:]



U.S. ELECTION ASSISTANCE COMMISSION
1335 EAST-WEST HIGHWAY, SUITE 4300
SILVER SPRING, MD 20910

U.S. House of Representatives Committee on the Judiciary
“Securing America’s Elections Part II: Oversight of Government Agencies”
October 22, 2019
Ben Hovland, Vice Chair
United States Election Assistance Commission (EAC)

Good morning Chairman Nadler, Ranking Member Collins, and Members of the Committee. I thank you for the opportunity to testify before you this morning to detail the work of the U.S. Election Assistance Commission, better known as the EAC, to fulfill its mission under the Help America Vote Act of 2002 (HAVA). I also appreciate this opportunity to highlight the great work of state and local election officials around the country.

As you know, our nation’s elections are run at the state and local levels, with each of the 50 states and the U.S. territories running elections in different ways. Election officials in over 8,000 local jurisdictions are ultimately responsible for conducting our elections, and their work truly protects and ensures the most fundamental pillar of our democracy – the vote.

Since 2016, there has been an enormous increase in focus on the security of our elections, which is just one of the many responsibilities election officials must address. I am pleased to report that, from my vantage point, the elections community has responded in an impressive fashion considering the challenges we face. Nearly every conference I attend while travelling around the country has a substantial focus on security, and protecting the integrity of elections is a constant topic in meetings with election administrators, our federal partners, and external stakeholders. The consideration, time and treasure devoted to this serious issue is as persistent and relentless as the threats we face. Even so, we need to ask ourselves a key question: Will that be enough if election officials do not have the sustained resources they need to defend our democracy against potential threats?

The good news is that following the Department of Homeland Security’s designation of election infrastructure as critical infrastructure, there has been a sea change in information sharing between the federal government and state and local officials. This includes the creation of a Government Coordinating Council, which brings together state and local officials with federal partners, as well as a Sector Coordinating Council, which has helped organized private-sector vendors and non-profit entities that support local election officials. We have also seen the creation of the Election Infrastructure Information Sharing and Analysis Center (or EI-ISAC), which now has nearly 2000 members, including every state chief election official’s office.

The deployment of Albert monitors, hardening of systems, increased trainings and promotion of table-top exercises around cyber events have all exponentially increased since 2016. The FY 2018 appropriation of \$380 Million HAVA funding, which the EAC distributed within months of its allocation, has largely contributed to these improvements. It doesn’t cover everything election

officials need, but states have had the ability to essentially choose from a menu of reforms, improvements, and priorities that could address their most pressing needs and vulnerabilities.

As Chairwoman McCormick testified earlier this year, the EAC projects that 85% of the FY 2018 money will be spent in advance of 2020. We have seen some states use the funding to replace aging or paperless equipment. Other states have replaced their statewide voter registration database or added additional security measures like multi-factor authentication. Some have hosted essential training and tabletop exercises ahead of 2020 to give election officials “hands on” experience that can help them prepare for various threats.

One of my personal favorite uses of the FY2018 funding is the implementation of “cyber navigator” programs. Essentially, the state recognizes that many local jurisdictions do not have the capacity or need for a full-time election cybersecurity expert, so the state employs individuals with regional responsibilities and they provide technical assistance to several counties or municipalities. This is the kind of innovative program that will help bolster our cybersecurity defenses and improve how states conduct elections. It’s also a model that the EAC would like to help amplify nationwide should our own funding support such an effort.

Unfortunately, not all of the news is good. As you all know, the threat of foreign adversaries remains real and, ultimately, our state and local election officials do not have the resources to thwart a truly determined and sophisticated nation-state actor. That is why we must take action to build resilience here at home and implement policies that deter adversaries abroad, such as a real sanctions regime.

Additional funding is crucial to allow states to continue to make necessary improvements that increase the strength and resiliency of our election systems. When we talk about election administration, we are talking about the infrastructure of our democracy. To make meaningful and lasting change requires a consistent investment over time. It cannot just be about 2020 or any one election, but about all of our elections going forward.

During a Senate Rules Committee hearing in May, I shared a recent discovery that the EAC’s operating budget of \$7.95 million dollars is less than the amount Kansas City spends on potholes. It is startling to think that one city with a population of around 500,000 people invests more to protect its residents’ car tires and alignment than our country invests in the only federal agency dedicated completely to improving election administration and helping more than 200 million registered voters cast their ballot.

I thank you for your time and am happy to answer any questions you may have.

Chairman NADLER. [Presiding.] I thank the witnesses. I ask unanimous consent that my opening statement be entered into the record.

Without objection.

[The information follows:]

MR. NADLER FOR THE OFFICIAL RECORD

**Opening Remarks for the Honorable Jerrold Nadler,
Chairman, House Judiciary Committee, for the Hearing on
Securing America's Elections Part II:
Oversight of Government Agencies**

**Tuesday, October 22, 2019, at 10:00 a.m.
2141 Rayburn House Office Building**

In 2016, our elections were attacked. Three years later, our intelligence community has universally confirmed that foreign actors have redoubled their efforts and are preparing, as we speak, to attack our 2020 elections.

We know the threat picture. But three years since the 2016 attacks, we have not done enough to combat these threats.

We know—through our agencies and our independent experts—what must be done. Our agencies and experts have set forth concrete recommendations. It is now our responsibility to make sure those recommendations get implemented – to ensure that all levels of our

government are taking the steps needed to safeguard our democratic processes.

But despite the severity of the threat, and the universal consensus that more government aid is required, the President and his Administration have *blocked* security efforts and have consistently *cut* programs designed to safeguard our elections.

For example, according to multiple senior officials, including the former Secretary of Homeland Security, President Trump's chief of staff issued instructions not to mention election security "in front of the President."

Another senior Homeland Security official reported that despite his Department's conclusion that the U.S. needs to "significantly step up its efforts" to block foreign influence campaigns, his Department was "stymied by the White House's refusal to discuss it."

Moreover, on January 3, 2018, the White House disbanded the Commission on Election Integrity. Shortly thereafter, the White House eliminated the cybersecurity coordinator position on the National Security Council. In February 2019, Homeland Security officials revealed that the Executive Branch dramatically downsized two teams fighting foreign election interference. And the President's 2020 budget proposed cutting funding for the Cybersecurity and Infrastructure Security Agency—our main election security agency—even further.

Our enemies are agile, persistent, and constantly intensifying their methods of attack. I am extremely troubled that the Administration's policies will handicap our agencies in their efforts to secure our elections. We must *listen* to our agencies when they ask for more resources, and *strengthen* our efforts to match the evolving threat – not, as the Administration has done, cut resources where they are most needed.

But what is most disturbing is that the latest threat to the integrity of our elections has come from the President himself.

We now have concrete evidence that the President has directly solicited foreign leaders to *interfere* in our elections. President Trump said to President Zelensky of Ukraine: “I would like you to do us a favor though because our country has been through a lot and Ukraine knows a lot about it. . . . I would like to have the Attorney General call you or your people and I would like you to get to the bottom of it. . . . There’s a lot of talk about Biden’s son, . . . so whatever you can do with the Attorney General that would be great.”

The President of our country reached out to a foreign leader and asked him point blank to meddle in our elections. And he did not stop there. Earlier this month, the President publicly stated that, “China should start an investigation into the Bidens.”

The President has defended these actions, which should no longer come as a surprise. During the 2016 elections, then-candidate Trump publicly asked Russia to hack into his opponent's e-mails: "Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing," he publicly stated on television. As candidate for President, Trump encouraged a foreign adversary to illegally hack into his opponent's emails and release sensitive information. And in June of this summer, the President told an ABC reporter that he would do it again—when asked what he would do if a foreign government offered him information on his opponent in the next election, President Trump said without hesitation: "I think I'd take it."

The President's actions are unacceptable. If we ask other governments to interfere in our elections, if we undermine the public's confidence in the integrity of our voting processes, we are doing our adversaries' work for them.

We cannot continue to undermine our own democratic values on the world's stage.

Regardless of the President's actions and statements, we must work together to secure our democratic processes. Election Security cannot be a partisan issue – it must be an American issue.

Even with all of our efforts, our systems will be targeted—they may even be breached.

It is how we respond that will define us.

And I am confident that working together, we will be up to the task of defending our voting systems.

I thank this Committee, including Ranking Member Collins, for joining me in this task. I thank the witnesses from our federal agencies for appearing here today, for your ongoing work to protect our elections, and for your continued willingness to improve your efforts. I look forward to hearing your testimony, and to finding ways to work together to ensure that each and every American feels confident in the accuracy and integrity of his or her vote.

Chairman NADLER. We will now proceed under the 5-minute Rule with questions. I will begin by recognizing myself for 5 minutes. Let me thank, before I start that, thank Vice Chair of the committee, Mary Gay Scanlon, for presiding while I was testifying in another committee.

In 2016, our elections were attacked. Three years later, our intelligence community has universally confirmed that foreign actors have redoubled their efforts and are preparing as we speak to attack our 2020 elections. Yet the President has blocked security efforts and cut programs designed to safeguard our elections. His chief of staff, for example, apparently issued instructions not to mention election security “in front of the President.” The President also has disbanded the Commission on Election Integrity, eliminated the cybersecurity coordinator position on the National Security Council, and dramatically downsized the two teams fighting foreign election interference. The President’s 2020 budget proposed cutting funding for the Cybersecurity and Infrastructure Security Agency, our main election security agency, even further.

The President is handicapping our agencies from securing our elections. Most disturbing, the latest threat to our elections comes from the President himself. The President asked a foreign leader, President Zelensky of Ukraine, to interfere in our elections. This isn’t the first time. In 2016, President Trump, then a candidate, publicly encouraged Russia to illegally hack his adversary’s emails. This past June, President Trump said on national television that if offered information on his adversary in 2020 from a foreign government, he would take it. Just this month, President Trump publicly suggested “China should start an investigation into the Bidens.”

I want to be clear. I believe it is unacceptable to ask foreign adversaries to interfere in any way in America’s elections. If we ask other governments to interfere our elections, if we undermine the public’s confidence in the integrity of our voting processes, we are doing our adversaries’ work for them. We cannot continue to undermine our own democratic values on the world stage. The President’s own officials agree. Ambassador Sondland testified, “Let me State clearly, inviting a foreign government to undertake investigations for the purpose of influencing an upcoming U.S. election would be wrong.”

Each of you sitting here today are responsible for protecting the integrity of, and public confidence in, our elections. So, I would like to hear from each of you in turn, yes or no, do you think it is appropriate for the President of the United States to ask a foreign government to investigate its political opponent in the 2020 elections. Mr. Masterson, yes or no.

Mr. MASTERSON. No.

Chairman NADLER. Ms. Floris?

Ms. FLORIS. No, sir.

Chairman NADLER. Mr. Hickey?

Mr. HICKEY. I am not going to comment on the President’s activities, but we are committed to confronting violations of the law wherever we found them.

Chairman NADLER. Do you think it is appropriate for a president, never mind this President, to ask for a foreign government to investigate opponents in an election?

Mr. HICKEY. I am focused on enforcing the criminal law.

Chairman NADLER. You won't answer. Mr. Hovland?

Mr. HOVLAND. No.

Chairman NADLER. Thank you. The Mueller report concluded that, "On approximately June 2016, the GRU, a Russian intelligence organization, compromised the computer network of the Illinois State Board of Elections," and "gained access to a database containing information on millions of registered Illinois voters." The report confirms that the Russian hackers successfully breached the databases but failed to alter or delete voting records. Last month, I asked our expert witnesses about the possible impact on our elections if the Russians had been able to alter the database. Ms. Plunkett, former director of the National Security Council under Presidents Bush and Clinton, testified that altering those databases would have been "devastating," including because tens of thousands of voters could have been turned away at the polls.

Our intelligence communities have confirmed that the threat of this happening again is very real. The President, however, had made it harder for Federal agencies to do their job and keep our democratic processes safe. Indeed, the White House has intentionally cut your budget and cut your staff going into an election our intelligence community has confirmed is under the biggest threat that our Nation has seen. The inspector general reported that DHS' staff shortages are making it difficult for DHS to do its job.

So, Mr. Masterson, let's say that in 2020 on Election Day, a county reports that its voter registration poll books seem incorrect, resulting in long lines and many voters being turned away, like what we saw in Durham. What is the specific plan for how DHS will ensure that it is immediately informed about any such issues on Election Day? What is the plan to remedy any such breach that occurs, and do you have sufficient staff to protect against these types of threats?

Mr. MASTERSON. Thank you, Mr. Chairman, for the question. That preparation begins long before Election Day with the work we are doing now with State and local election officials across the country. At its core, our work is to work with the election officials to build resilience. That is that ability to detect if there is an issue with the voter rolls, and then identify what the issues are and recover.

So that is the purpose of items like our tabletop devote exercise, to work with those State and local election officials about when or if they identify that information, how they will communicate it both with the local election officials, State election officials in their jurisdiction, with the Federal Government, and what processes they and we have in place to respond. For instance, DHS has incident response capabilities both remotely and teams that can come and support election officials in anticipation of possible or in reporting of incidents.

In addition, we are working with State and local election officials on preparations. For instance, having in place provisional ballot

materials such that if there is an issue with the voter rolls on Election Day, they are prepared to administer provisional ballots broadly and ensure that every voter, while it may be messy, has the ability to cast their vote and know that their vote was counted as cast.

Chairman NADLER. So, are you confident now that you have the funding and the ability so that should a county, a large county, let's say, in a key State is successfully hacked and the voter rolls are messed up, that you will be able to step in instantly and give whatever assistance is necessary, so we won't have a long post-election dispute over a couple hundred thousand votes not being properly cast?

Mr. MASTERSON. I am confident that the level of funding, starting with the \$33 million we got last year and the proposed funding now, allows us to maintain that level of support to ensure that election officials have what they need as they head into Election Day, yes.

Chairman NADLER. Thank you very much. My time has expired. The gentleman from Ohio.

Mr. CHABOT. Thank you, Mr. Chairman. We have wasted so much time this year on a bogus Russian collusion allegation and on various messaging bills which are ultimately not going to go anywhere, that it is nice that we actually have the Departments of Justice, Homeland Security, the FBI, and the U.S. Election Assistance Commission before us to talk about a real issue, and that is protecting America's elections from foreign influence.

There are various pieces of legislation that would, I believe, help better protect our elections in the future. For example, I am an original co-sponsor of H.R. 3442, which would deny entry into the United States any individual who interferes with our election. Let's hope that maybe this Committee could work together in a bipartisan fashion to make sure our elections are once again the gold standard, what the rest of the world looks to as how you do it, how you get it right. We generally have been that gold standard over the years, so we need to get back to that.

Ms. Floris, let me begin with you, if I could. I will start by asking you a question that relates to H.R. 3442, the legislation that I just mentioned. What is the standard for determining what kind of content posted by a foreign agent or agents that rises to the level of being a foreign influence operation? Is there a certain type of verbiage or rhetoric that the FBI looks for, and do you think engaging in such behavior online should bar an individual from entering the United States?

Mr. HICKEY. Thank you, sir, for your question. So, I will start by saying that the FBI does not content or police information on the internet. That is certainly not our job and not something that we plan to get into. What we look at is actually known nefarious actors, so if we have identified a foreign actor who is participating in influence operations, and as part of those operations seeks to propagate this information or post derogatory content, that is of investigative interest to us. We absolutely do not start with content and work our way back.

Mr. CHABOT. Thank you. Mr. Hickey, would you agree with that, and is there anything you would like to elaborate on?

Mr. HICKEY. No, I think the DAD got it exactly right. We focus on known actors and tip the providers in a way that helps them make determinations under their terms of service.

Mr. CHABOT. Is there anything that the Department of Justice is doing to work with social media companies in advance of the 2020 elections?

Mr. HICKEY. Principally through the FITF, but we also support the FITF's efforts and sometimes accompany them in working with the providers.

Mr. CHABOT. Okay. Are there any other countries other than Russia that you have seen or that you believe is showing some interest in disrupting our elections in 2020 or in the future in general?

Mr. HICKEY. We have spoken and the IC has spoken about foreign influence activities, malign foreign influence activities from China, and we are certainly concerned about others. Of course, in our FARA enforcement, obviously we have seen actions by agents of other nations, like Turkey and Ukraine.

Mr. CHABOT. This is to any of the witnesses. What was your agency's role in securing the 2018 congressional midterm elections, and what specific efforts were made in that effort? Mr. Masterson?

Mr. MASTERSON. Yeah, thank you, sir. Our role, as it is now in helping to secure the 2018 midterm elections, was to provide information sharing, support, and services to State and local officials to help them manage risk to their systems. So, we started by building those trusted relationships with those State election officials that are, I think, appropriately skeptical of a Federal role in elections and by providing value, right? That the information we provide, the services, help them identify and manage the risk to their systems.

So, we are doubling down on those efforts for 2020 to reach those local election officials across the State, like Cheryl in Jackson County, Ohio. How do we get to her and get her the information sharing she needs to manage risk to her systems?

Mr. CHABOT. Thank you very much, and I am getting close to being out of time. Mr. Floris, let me ask you this. Would you agree that the FBI's reputation was significantly damaged by political bias against the President, President Trump specifically, that was exhibited by a number of top-level officials in your organization?

Ms. FLORIS. Sir, I am not going to comment on any damage or lack of damage to our reputation. Thank you.

Mr. CHABOT. Okay. Well, it really was. People like Peter Strzok and others, I think, very much damaged it. It is unfair to the rest of the organization because the FBI is truly a great organization, one of the best in this Nation. Thank you very much. I yield back.

Chairman NADLER. The gentleman yields back. Let me just say for the record that I think Peter Strzok acted in the highest traditions of government workers. The gentlelady from California.

Ms. LOFGREN. Thank you, Mr. Chairman, and thank you to all the witnesses for not only your testimony, but your service to our country. It is recognized and appreciated. Just a note to the gentleman from Ohio. The bill that he has co-sponsored, and there are some variations on that theme about denying visas to those who are interfering in our elections, will be made part of the SHIELD

Act through a manager's amendment. I just wanted him to know that, that we are taking that good idea and moving it forward.

You know, the Mueller report describes evidence that the then Trump Campaign chairman, Paul Manafort, shared with a Russian operative, Kilimnik, the campaigns, and this is a quote from the report, "strategy for winning Democratic votes in Midwestern States," and "internal polling data of the campaign," which is I have always thought, what was going on there. Why the internal polling data to this Russian agent? Ms. Floris, I wouldn't ask you to comment on that particular item because that is a fact. Generically, why would a campaign's internal polling data and strategy for battleground States be helpful to someone who was seeking to impact our elections? Specifically, what could a hostile actor do to such information with any campaign if they got internal polling data?

MS. FLORIS. Thank you, ma'am, for that question. I will answer from a strategic perspective. When you look at countries like China, like Russia, they essentially take a whole of government approach when it comes to their foreign influence operations. They are not only looking at our Federal elected officials, but they are also looking at State and local elected officials as well because any one of those individuals can potentially influence policy moving forward.

So, because they take this whole of government approach, any bit of information could help inform their decisions and how they move forward with their operations. So though on the surface it might not seem as a great benefit to them, rest assured that particularly China and Russia will use every tool in their toolbox to get information that they deem potentially as valuable.

MS. LOFGREN. Now, you all are the FBI and government investigators. Each one of us, on both sides of the aisle, have been candidates, and one of the things we know is that you could do ads. If you were interested in polling data, you couldn't do a poll without being caught. So, the only way you would get his information was from a campaign that had actually legitimately done a poll.

A report this month was released by the Senate Intelligence Committee on Russia interference in our elections, and it said that the Russian government used Facebook's geographic targeting features to channel advertisements to intended audiences in specific locations. And about 25 percent of the ads purchased by IRA were targeted down to the State, city, or, in some instances, university level. For example, in Michigan and Wisconsin, they were targeted with advertisements overwhelmingly focused on the subject of police brutality to move populations in one direction or another.

Mr. Hickey, if a campaign made its internal information, such as polling data, readily available to a foreign government that then used it to target voters via social media, would that be something the Department of Justice would investigate, or is there no law on that that would allow or stimulate an investigation?

MR. HICKEY. So, there are two basic categories of laws. One I know. One I am less an expert in. I don't know whether campaign finance, public corruption, fraud, or other statutes would apply. With respect to the national security statutes I am familiar with, they tend to focus on whether an American is acting as an agent

of a foreign government, meaning under the direction or control of the foreign government. So, in the example you have posited, you would have to analyze whether the American is the reverse of that, whether they are directing and controlling or procuring something from the foreign government, in which they wouldn't be an agent of the foreign government.

Ms. LOFGREN. Well, I would just note that we will have an opportunity to, in the near future, to make this much clearer by approving the SHIELD Act, which would prohibit the sharing of internal data, campaign data, by an American campaign with agents of a foreign power so that you would have a very clear basis to proceed on that. I hope that we can get strong bipartisan support for that measure. With that, Mr. Chairman, my time has expired, and I yield back.

Chairman NADLER. The gentlelady yields back. The gentleman from Arizona.

Mr. BIGGS. Thank you, Mr. Chairman. I would love to spend this time talking about election security. I think that is really critical. I think that I have prepared to ask those questions, but we come to these hearings, and it is impeachment all the time. That is what this is. We were told by Chairman about the impeachment inquiry, but here we sit. Well, if you want to ask the questions or want to mischaracterize the telephone conversations, you probably ought to go try to get down into the closed hearing downstairs. Well, you know what? You can't get in because I have tried to get in.

So, when I hear Chairman open up with his opening statement about the Ukrainian phone call and suggest that the President asked President Zelensky to interfere in the 2020 election, I have read the transcript. It is out there. It for everybody to read. You can characterize it any way you want to, but I would suggest that that isn't the proper characterization. The telephone call itself mentioned CrowdStrike, Ukrainian interference in the 2016 election, and that was what President Trump was asking that President Zelensky look into. Now, when he mentions Biden, here is my question. We have got FBI here. We got DOJ there. So here is my question for you. Do you think that a person who has admitted criminal conduct should have immunity from investigation because that individual is a potential political opponent in an upcoming election? What do you think?

Mr. HICKEY. So, I think nations should follow facts and law where they lead in the course of criminal investigations honestly—

Mr. BIGGS. Regardless of whether they are a potential political candidate or not.

Mr. HICKEY. Regardless of status or without fear or favor.

Mr. BIGGS. Right. The other thing that we are subjected to in this Committee a lot is if I ask questions and Chairman doesn't like the responses or the statement I make, when I am done, he will offer his comment on it. That is why he said Peter Strzok represented the highest ideals or highest standards of the Agency. That is really unusual because normally if he wants to make that comment, he is going to ask somebody else to yield some time to him so he can rebut the comment that he disagreed with. That happens perpetually here because it is convenient. Got a mike. I am Chairman. I can do whatever I want. I would suggest to you

that is merely an opinion with regard to Mr. Strzok because I think Mr. Strzok does exactly the opposite. His misconduct actually reflected poorly and has caused much division and heartache in this country. That is just the way it is.

So, we have focused a lot on Russian interference in the 2016 election, the malign foreign influence of the Russians. Are there other nation-states that engaged in 2016 and might engage in 2020 elections?

Ms. FLORIS. So, sir, I will hit on the one big country that we are focused on as we roll into 2020 outside of Russia, and that is certainly China. Make no mistake, China is aggressively pursuing foreign influence operations. They do a bit of a different tactic than the Russians. They certainly prefer a face-to-face interaction. They use economic levers. Their end goal is really to cede us as a global economy superpower. So, as we roll into 2020, though Russia was certainly a threat in 2016, 2018, and will continue to be so in 2020, we are also aggressively looking at China as well.

Mr. BIGGS. Did you see other states in 2016 besides China and Russia involved?

Ms. FLORIS. I would refer back to the ICA, sir, that was released after 2016, I believe in 2017.

Mr. BIGGS. In fact, in the 2018 midterm elections, DOJ and DHS found that there was no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political campaign infrastructure used in the 2018 midterm elections. That goes to what you said, Ms. Floris, when you said there was no hard evidence that any number of votes were actually changed through the system. Mr. Hovland, I have seen your biography. You previously worked on voter registration list maintenance in Missouri. Can you tell me a little bit about the importance of States maintaining lists that are up to date?

Mr. HOVLAND. Absolutely. Thank you for the question, sir. So, the National Voter Registration Act, or NVRA, sets out a process for voter list maintenance, and that ensures that individuals are able to get registered, but when someone is no longer in a jurisdiction, it gives them the proper way to clean those rolls. Frankly, having clean rolls allows jurisdictions to save money and ensures that the right people are where they need to be.

Mr. BIGGS. My time has expired.

Chairman NADLER. The gentleman yields back. The gentlelady from Texas is recognized.

Ms. JACKSON LEE. I thank Chairman and Ranking Member for this hearing, and I thank all the witnesses for your service to the Nation. Let me ask the question for each of you, please. How confident are you that we will have an impeccable, safe, and secure election in 2020 from the work that you have now done on the Federal level? Mr. Masterson? Without intrusion from foreign operatives. Mr. Masterson?

Mr. MASTERSON. Thank you for the question, ma'am. Anyone that has run an election could tell you there is no such thing as an impeccable election, right? The goal is absolutely to build resilience, and I am confident that the 2018 election was more secure and resilient than 2016, and 2020 will certainly be more secure and

resilient thanks to the hard work of the State and local election officials, the private sector that is working with them, and our work with them.

Ms. JACKSON LEE. The rest of you, yes or no, and one sentence. Ms. Floris? Thank you.

Ms. FLORIS. I am confident that we are throwing every tool we have against the threat to our election security.

Mr. HICKEY. Agree.

Mr. HOVLAND. I would echo Mr. Masterson's sentiment and say that traveling around the country, it is amazing to see the hard work that State and local election officials are doing to address this issue.

Ms. JACKSON LEE. None of you have said, even though I appreciate Mr. Masterson's comment about we cannot have an impeccable election. I think the American people are owed an impeccable election, to be very honest with you. So, I will follow up my line of questioning about how secure are we and proceed to raise the question with Mr. Hickey. In light of the fact that there seems to be some loophole in how secure it is going to be, what is the approach of the DOJ in prosecuting and being proactive for what intrusions may occur in the 2020 election?

Mr. HICKEY. We will be very proactive, ma'am. I think one of the most important lessons coming out of 2016 and to the present is how we handle information that a State or a campaign may be targeted and getting what we will call victim notifications to the right people and following up. I think we are in a better position now than we were in 2016, both as a matter of policy and our sensitivity to the importance of that.

Ms. JACKSON LEE. Do you have a sufficient number of lawyers, DOJ prosecutors, and resources to be ready for the massiveness of the 2020 presidential election and other Federal elections?

Mr. HICKEY. I think we are well positioned. I also think the budget for 2020 includes additional resources for the sections I supervise that will improve our standing in that regard.

Ms. JACKSON LEE. I want to congratulate Congresswoman Lofgren for the work of her Committee on the question of shielding us from this kind of intrusion and congratulate her for including my legislation that Mr. Johnson and I introduced in April this year, H.R. 2353. The language in particular says if a candidate or any individual affiliated with a campaign of a candidate knowingly receives an offer for assistance with the campaign from a source the candidate or individual knows is a foreign power or an agent of a foreign power, the candidate or individual shall refuse the offer for such assistance and notify the Federal Bureau of Investigation of the offer not later than 72 hours after receiving the offer. Ms. Floris, if this legislation passed, but really its intent, should be acted upon by the FBI. What infrastructure do you have to ensure a response to any reporting of this kind of activity?

Ms. FLORIS. Thank you, ma'am, for the question. The FBI becomes interested in foreign influence activity, again, when it hits those four categories I spoke about in the beginning: The subversive nature of it, the undeclared nature of it, the coercive and criminal nature of it. The FBI will respond as we do in any investigation with the full might of not only the Foreign Influence Task

Force, but the, you know, hundreds of agents and analysts out in all our 56 field offices who are working the foreign influence threat day in and day out. We will use all the tools we have in our toolbox as we do—

Ms. JACKSON LEE. Do you have on enough staff? Have you ramped up your staff for the 2020 election? Do you have enough funding for staff to deal with the potential of this reporting?

Ms. FLORIS. Ma'am, we can always use more resources, but rest assured we are putting everything we can against this threat and facing it with absolute determination.

Ms. JACKSON LEE. Mr. Masterson, I sit on the Homeland Security Committee, so we appreciate the deep dive that you all have taken. So, give me an understanding of how you have as a priority efficiently sharing actionable intelligence in identifying threats. How have you ramped up that very important part of your work?

Mr. MASTERSON. Yeah, absolutely. I would highlight two areas, ma'am. The first is the buildout of the election Infrastructure Information Sharing and Analysis Center. This is the hub of information sharing that we use to reach State and local officials. We have all 50 States and the territories as Members of the IISAC as well as over 2,100 local election officials. So, this ensures that actionable, timely information is reaching the field so that they can take the steps they need to manage risk to their systems.

The second is our continued push with the intelligence community to provide clearances and classified briefings, whether through secure video teleconferences or in person, as well as working with private sector threat intelligence authorities. So, we have worked with private sector companies to provide briefings to State and local election officials about what they are seeing out internationally to help them manage risk to the system. So, we are exploring all avenues trying to find efficient ways to get this information to the election officials.

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

Chairman NADLER. The gentlelady yields back. The gentlelady from Arizona.

Mrs. LESKO. Thank you, Mr. Chairman. My first question is for Ms. Floris. Does anyone at the Foreign Influence Task Force draft FISA affidavits or applications?

Ms. FLORIS. No, ma'am.

Mrs. LESKO. Looking back at the FBI's activities investigating the 2016 election, it has been reported that FBI never obtained the original servers from the Democratic National Committee that had allegedly been hacked by Russia, instead relying on imaged copies. First, is that correct?

Ms. FLORIS. Ma'am, I can't speak to that. I am sorry.

Mrs. LESKO. Can someone else on the panel speak to that?

Mr. HICKEY. Yes, ma'am. We got the information that we required for our investigation, and it is pretty common for us to work with a security vendor in connection with an investigation of a computer intrusion.

Mrs. LESKO. So, can either one of you answer, does the DNC's cybersecurity consultant, CrowdStrike, still have possession of the Clinton servers?

Mr. HICKEY. I don't know what they have possession of now.

Mrs. LESKO. Does anyone on the panel know?

[No response.]

Mrs. LESKO. All right. My next question is for Mr. Hickey, and I know that Mr. Chabot asked you what other countries have shown an interest in disrupting the 2020 election, but what other countries had shown an interest or tried to interfere in the 2016 election?

Mr. HICKEY. Based on what I have read, both from what the IC has put out and also investigations by Congress, what I have seen only refers to Russia that I am aware of.

Mrs. LESKO. Then earlier, there was a question by Chairman Nadler, and I want to clarify what you think, if you think it is appropriate for a President of the United States to ask a foreign government to investigate previous election interference, and I guess I would like all of you to answer that question.

Mr. MASTERSON. Can you repeat the question, ma'am? I am sorry.

Mrs. LESKO. Do you think it is appropriate for the President to ask a foreign government to investigate previous election interference if there was election interference going on? To ask if there is anything he thinks was unlawful going on in other countries, to ask the other country to help to determine if there was something unlawful happening?

Mr. MASTERSON. I think it is appropriate to understand any attempts at interference in our elections so that we can continue to work to build resilience in the process.

Ms. FLORIS. The FBI is interested in any criminal violation as relates to foreign influence, so long as there is that foreign angle to the foreign influence operations.

Mrs. LESKO. Thank you.

Mr. HICKEY. I will give the same answer I gave before, which is I don't opine on appropriateness, per se, but I am focused on enforcing the criminal law.

Mr. HOVLAND. I think it is important to understand what occurred with our election so that election officials have the information they need to prepare for future elections.

Mrs. LESKO. Thank you, and I yield back my time.

Chairman NADLER. The gentlelady yields back. The gentleman from Tennessee?

Mr. COHEN. Thank you, Mr. Chair.

This is a question to anybody on the panel that has an answer. In 2016, I understand there were reports that I think were sound that Russia tried to interfere with a lot of State election rolls, maybe all of them. Anybody here aware of those reports?

Mr. Masterson, you seem to be first to go to bat, sir.

Mr. MASTERSON. Probably foolishly, sir. Thank you.

Yes. The DHS, in coordination with the FBI, released an information product out to State and local election officials that stated that based on the information we have as far as the activity in 2016, that the pattern of behavior is likely that the Russian government—or Russian actors conducted at least research on election entities across all 50 States. That doesn't necessarily mean that they attempted to access the systems. It could be as simple as a Google search to understand who runs elections in that State.

Based on the information that we and the intelligence community have, that it is assumed that they were at least researching all 50 States' election systems.

Mr. COHEN. Why would they have done that?

Mr. MASTERSON. Presumably—I don't want to speculate, but presumably, just to understand how elections are run across the United States.

Mr. COHEN. Spring training?

Mr. MASTERSON. To gather information.

Mr. COHEN. Kind of spring training?

Mr. MASTERSON. Yes.

Mr. COHEN. Yes, something like that. Anybody else have knowledge of that, have any other thoughts about it? No?

[No response.]

Mr. COHEN. How about Florida? Was there not reports that two different jurisdictions' voting systems were contacted by the Russians? Mr. Hickey?

Mr. HICKEY. So, I think we have briefed Florida officials on activity targeting systems and leading successful intrusions in two counties. I think it is important to be clear we have also reached the conclusion that there was no material impact on registration or vote counting, based on the evidence that we have seen. So, I think it is clear—important to be clear about that.

Mr. COHEN. Based on what happened in 2016 and based on what Mr. Mueller told us that the Russians at the time he testified were looking into effect being involved in our 2020 elections, are you confident that giving our funds directly to States, that they will use them to work against Russian cyber interference and protect those State systems?

Mr. HOVLAND. I am happy to talk about that. So, at the EAC, we distributed the \$380 million from fiscal year 2018, and as I mentioned in my opening statement, it appears that the vast majority of that will be spent. We have seen over 90 percent of that going toward improving security, again whether that is replacing outdated equipment, hardening systems, implementing audits. The States have done a number of things, but because of the variations in how elections are administered State to State, there have been different priorities.

Mr. COHEN. Mr. Masterson?

Mr. MASTERSON. Sir, just briefly on that, we worked with our Government Coordinating Council, which has 24 State and local election officials as a member, to identify priorities for that funding. What we have seen is States have taken that information, which is databased on our work with the States on where risks lie and used it to apply. I will give you a very specific example.

Prior to the 2018 election, the State of Wisconsin deployed two-factor authentication out to all its local election officials for the statewide voter registration database, which may seem unremarkable until you realize they have 1,800 local election jurisdictions in the State of Wisconsin and almost 3,200 users of the statewide voter registration database. So that is a very focused, targeted step, base level, that they have taken and used the money.

Mr. COHEN. Let me ask you this, Mr. Masterson. Director Krebs has emphasized the importance of protecting the campaigns based

on what happened in 2016 with interference with the DNC, the Clinton campaign stolen emails, *et cetera*. He said shame on us if we are not ready this time around.

Have you consulted with the President, or anyone involved in his re-election campaign?

Mr. MASTERSON. Sir, we have contacted not just the Trump campaign, but campaigns across the Presidential election—presidential campaigns to make sure that they are aware of our services and information-sharing responsibility.

Mr. COHEN. So, Mr. Mulvaney did not contact you, as he did your superior, and say this is a very sensitive subject for the President, don't mention it, or dance around it, or whatever?

Mr. MASTERSON. No, sir.

Mr. COHEN. Okay. Ollie, Ollie, in free. That is great.

I want to thank the FBI and the Justice Department as well. You all are stalwarts in the American system of government and the Rule of law, and I would have to disagree with some previous statements made that some individuals within your organizations were responsible for hurting your organizations. I think that an individual who is the President of the United States was the one that caused it by questioning those people's actions and making statements that were adverse to both the FBI and the Justice Department, which we should uphold.

I yield back the balance of my time.

Chairman NADLER. The gentleman yields back. The gentleman from Florida?

Mr. GAETZ. Thank you, Mr. Chairman.

I wish this were truly were a sincere hearing on election security. If it were, we might be marking up some of the bipartisan legislation that Members of the Committee have worked on, including House Resolution 3529 by Congresswoman Murphy, Mr. Deutch, Ms. Mucarsel-Powell, myself, to have greater connectivity prior to any intrusion, or we might be marking up the legislation by Mr. Ratcliffe, Mr. Himes, joined by Mr. Collins and Mr. Khanna, 3238, that would create greater consequence for those who engage in election interference. That is not what this is about.

This is about smearing the President of the United States and validating the corrupt people who have been involved in delegitimizing his historic election. We know that because just moments ago, Chairman said that Peter Strzok was acting in the highest traditions of Government service.

Now, Ms. Floris, I believe you currently hold the job that Mr. Strzok once held. Is engaging in an extramarital affair in the FBI with a coworker acting in the highest traditions of Government service?

Ms. FLORIS. I am not going to comment on that, sir.

Mr. GAETZ. Well, are there any regulations in the FBI against it that you are aware of?

Ms. FLORIS. I am not going to comment on that, sir.

Mr. GAETZ. Well, you hold Mr. Strzok's job. Are you saying that you don't know whether or not it is against FBI policy to have an extramarital affair with a coworker?

Ms. FLORIS. Sir, I hold a slightly different job than Mr. Strzok held. I am the DAD over the Intelligence Branch. He was over our

Operational Branch, not that we are held to a different standard. I am just not going to comment on whether or not Peter Strzok's behavior was out of conduct.

Mr. GAETZ. Well, is it in the highest traditions of Government service at the FBI to engage in affairs with coworkers? You should know that if you work there.

Ms. FLORIS. Sir, I am not going to comment on that.

Mr. GAETZ. Wow. Well, maybe I will ask you another one. The Inspector General said in his report, "We do not have confidence that Strzok's decision to prioritize the Russian investigation over following up on the midyear-related investigation." So, if the Inspector General didn't have confidence in the way that someone prioritized something, would that be acting in the highest traditions of Government service?

Ms. FLORIS. Sir, I am not going to comment on that.

Mr. GAETZ. The Inspector General further said, "The OIG found it is not only indicative of a biased State of mind but, even more suspiciously, implies a willingness to take action to impact a presidential candidate's electoral process. This is antithetical to the core values of the FBI and the Department of Justice."

If someone, anyone, is engaging in behavior that is antithetical to the core values of the FBI and Department of Justice, is that person acting in the highest traditions of Government service?

Ms. FLORIS. Sir, we have an entire Inspection Division. We have the OIG. There are several measures in place that take into account those questions. I am not going to answer those questions from the position I am in.

Mr. GAETZ. It is just really striking that someone in the senior leadership at the FBI, like an unwillingness to be critical of conduct that was so detrimental to our country. And as people all over America are looking at the corruption that negatively impacted our President and the institution of the presidency, it doesn't really inspire confidence that current officials from the FBI say, hey, you know what? It is a bad idea to be having affairs with your colleagues and to be undermining the trust that people have and to be prioritizing investigations over politics. Nonetheless, here we sit.

In fact, here we do sit. It was more than a month ago, Mr. Chairman, that you announced an impeachment inquiry in this committee. I believed you that our Committee would be engaged in that process. As we sit here today, three other committees are in the basement of the Capitol conducting secret interviews, engaging in selective leaks.

We have got Chairman Schiff then coming out and having his theatrical reperformances of transcripts that didn't really occur, and you have got lies about contacts with whistleblowers.

Now regardless of how people feel about the President or this impeachment, one would at least think that if Chairman of the Judiciary Committee announces the launch of an impeachment investigation, that Members of the Judiciary Committee might be willing to—or able to participate in that investigation. When I have gone to participate, Mr. Biggs has gone to participate, and others have gone, we have been locked out.

So, it is my sincere hope, and I asked this the last time we gathered, that you would take up the cause not just of someone's par-

tisan ambition to impeach the President, but that you would take up the cause of our Committee and advocate for our ability to participate. Because one can only suspect that the reason that the House Judiciary Committee has been dealt out of the hand on impeachment is because Speaker Pelosi didn't like the outcomes that were going on in this Committee when the current chairman was running it.

I mean, it wasn't a surprise to the country when you brought in Mr. Lewandowski. House Democrats looked like a dog that caught a car and didn't know what to do with it. When House Democrats brought in Robert Mueller, there were promises that this was going to sway the public, this was going to create a flood of support for impeachment. That was obviously something that didn't hold to bear.

So please stand up for our Committee and let us stop with this busywork. If we want to markup bills, let us markup real bills.

I yield back.

Chairman NADLER. The gentleman yields back. The gentlelady from Washington?

Ms. JAYAPAL. Thank you, Mr. Chairman.

I thank our witnesses for being here today. I would hardly call this "busywork" to protect our elections. So, I wish our colleagues on the other side would be as concerned with election security.

Back in July, the Senate Select Committee on Intelligence released its bipartisan report on Russian interference in our 2016 elections. Senate Intel found that "Russian government-affiliated cyber actors conducted an unprecedented level of activity against State election infrastructure in the run-up to the 2016 U.S. elections."

They called for sweeping action to protect our 2020 elections. With Election Day just 378 days away, it is crucial that we move quickly.

So, my questions. All of you are responsible for various aspects of protecting our elections, and you are no doubt aware that a significant concern of securing our elections is that foreign actors will attack election reporting or the results of elections. Take the following hypothetical.

Florida reports that candidate X won after counting the votes. The next morning, Florida election officials report that the results were tampered with, and, in fact, candidate Y won.

What is being done at the Federal level to, first, prevent attacks on our election results, and second, if such an attack occurs, to ensure public confidence in the reporting of our elections?

Mr. Masterson, let us start with you and then move to Floris, Hickey, and Hovland, please.

Mr. MASTERSON. Yes, thank you, ma'am.

Certainly, election night reporting systems, which are the ones you are referencing, are an area that we have worked with State and local election officials to secure, to understand risk to. The first and most important thing to understand that all the folks on the Committee here understand is that election night results are, in fact, unofficial results, that there is a canvas process that goes on after Election Day. So, ensuring that voters have that information, understand the unofficial nature of results, and that there is an en-

tire reconciliation process that election officials undergo following election night to ensure the correctness.

The second is a top priority for us, and that is working with election officials to have auditability of the results and to ensure efficient and effective auditing of those results. That is absolutely critical to ensure not just the loser that they won or lost, but also to reassure the public that their vote was counted as cast.

So that is two areas of high priority for us working with State and local election officials to empower them to talk to their voters about the steps they are taking both to protect those systems, but to really offer reassurance and transparency on the back end. I know election officials take that very seriously.

Ms. JAYAPAL. Does anybody want to add anything?

Mr. HICKEY. I would just add that in the circumstance where we know or have indications that a State is being targeted, it is really important that we get to State officials at the right level and with a sense of urgency so they can do whatever they can to mitigate on their systems.

Ms. JAYAPAL. Mr. Hovland?

Mr. HOVLAND. I would echo what Mr. Masterson said and add that at the Election Assistance Commission, part of the work that we have done is host IT trainings for election officials, which is relevant to this topic, work with them on improving audit processes, and certainly think that the issue you raise is one of real concern.

There are a number of responsibilities that election officials have, and I believe that the Election Assistance Commission should be more empowered to work on those, but the reality, as I mentioned in my opening statement, is that we are a \$7.95 million agency. We have one lawyer. We have one financial person.

Since its inception, the Election Assistance Commission has been kicked around like a political football, and we have never been empowered or funded in a way to actually help election officials in the way we can. I think that right now in this time, we see the need for the Federal clearinghouse that the EAC was created to be, and I would just ask you all to help make that possible.

Thank you.

Ms. JAYAPAL. Thank you.

Mr. Masterson, as a senior cybersecurity adviser, how have you engaged with local, State, and national media outlets to ensure that unofficial vote reporting is protected from malicious interference? What media networks specifically have you met with, and have any refused to meet with you? What new measures are you taking in 2020 that weren't applied in 2016 and 2018?

Mr. MASTERSON. Yes, thank you, ma'am, for the question.

The first is that the Associated Press, the team that handles the election night results for the AP on election night, is a member of our Sector Coordinating Council, which is the private sector council that we work with on providing support and services, information sharing. So, AP has been an active participant in that coordinating council to understand threat and risk, steps that they could take to secure their results reporting, and I know is taking that very seriously.

Secondly is we held a tabletop exercise with Members in the national media prior to the 2018 election to talk about what are sce-

narios that could play out, how is information being exchanged not just with State and local officials, but social media companies, the political parties, and others to ensure that media have access to the information they need before they report on results or other items.

Heading into 2020, we anticipate engaging media outlets individually and then having the tabletop exercise again heading into the 2020 election to work through those scenarios and ensure they have the information they need.

Ms. JAYAPAL. Thank you very much. Yield back.

Chairman NADLER. The gentlelady yields back. The gentleman from Virginia?

Mr. CLINE. Thank you, Mr. Chairman.

I want to thank the witnesses for being here. I, too, am concerned about foreign interference in our elections and have cosponsored the Ranking Member's bill, H.R. 3442, which would amend the Immigration Act to provide the aliens who have engaged in improper interference in a U.S. elections are inadmissible to and deportable from the U.S., and I also cosponsored 3238, Mr. Ratcliffe's bill, which would prohibit interference with voting systems in the Computer Fraud and Abuse Act.

I want to go ahead and ask Ms. Floris, in your testimony, you say that we do know that our adversaries are actively trying to influence public opinion and electoral processes in advance of the 2020 election. You have mentioned in your testimony influencing public opinion through various social media activity. What electoral processes, what efforts to interfere with electoral processes are you aware of at this time?

Ms. FLORIS. So, sir, thank you for the question.

As we roll into 2020, the one thing I want to highlight is that countries like Russia and China, they pose a pervasive and persistent threat. It is not just based on the electoral cycle. Their foreign influence operations are essentially always present.

When it comes to the electoral process, you could look at something as voter suppression. The whole concept of pushing out false information, of highlighting places to vote that are actually not true, this whole concept of disinformation that we have really seen the Russians focus on, that, in and of itself, can interfere with the electoral process.

Mr. CLINE. Okay. Nothing to the extent of actively trying to hack into or interfere with the electoral system?

Ms. FLORIS. To date, sir, we have not seen anything specific regarding hacking into the electoral systems of the 2020 election.

Mr. CLINE. All right. Thank you. I am going to yield the remainder of my time to Mr. Gaetz.

Mr. GAETZ. I thank the gentleman for yielding.

Mr. Chairman, I have a series of unanimous consent requests that set up my question. The first is a request that it be entered into the record an email from Nellie Ohr to Bruce Ohr on the 30th of May, entitled "Reported Trove of Documents on Ukrainian Party of Regions' Black Cash Box."

Chairman NADLER. Without objection.

[The information follows:]

MR. GAETZ FOR THE OFFICIAL RECORD

Nellie Ohr's 'Hi Honey' emails to DOJ about Russia collusion should alarm us all

 thehill.com/opinion/white-house/441580-nellie-ohrs-hi-honey-emails-to-doj-about-russia-collusion-should-alarm-us

John Solomon, opinion contributor

May 1, 2019

First came the text messages between FBI lovebirds Peter Strzok and Lisa Page, which gave us a painful glimpse at potential political bias inside America's most famous crime-fighting bureau.

Now, a series of "Hi Honey" emails from Nellie Ohr to her high-ranking federal prosecutor husband and his colleagues raise the prospect that Hillary Clinton-funded opposition research was being funneled into the Justice Department during the 2016 election through a back-door marital channel. It's a tale that raises questions of both conflict of interest and possible false testimony.

Ohr has admitted to Congress that, during the 2016 presidential election, she worked for Fusion GPS — the firm hired by Democratic nominee Clinton and the Democratic National Committee to perform political opposition research — on a project specifically trying to connect Donald Trump and his campaign chairman, Paul Manafort, to Russian organized crime.

Now, 339 pages of emails from her private account to Department of Justice (DOJ) email accounts, have been released under a Freedom of Information Act request by the conservative legal group Judicial Watch. And they are raising concerns among Republicans in Congress, who filed a criminal referral with the Justice Department on Wednesday night.

They clearly show that Ohr sent reams of open-source intelligence to her husband, Associate Deputy Attorney General Bruce Ohr, and on some occasions to at least three DOJ prosecutors: Lisa Holtyn, Ivana Nizich and Joseph Wheatley.

The contents tracked corruption developments in Russia and Ukraine, including intelligence affecting Russian figures she told Congress she had tried to connect to Trump or Manafort.

"Hi Honey, if you ever get a moment you might find the penultimate article interesting — especially the summary in the final paragraph," Nellie Ohr emailed her husband on July 6, 2016, in one typical communication. The article and paragraph she flagged suggested that Trump was a Putin stooge: "If Putin wanted to concoct the ideal candidate to service his purposes, his laboratory creation would look like Donald Trump." Nellie Ohr bolded that key sentence for apparent emphasis.

Such overt political content flowing into the email accounts of a DOJ charged with the nonpartisan mission of prosecuting crimes is jarring enough. It raises additional questions about potential conflicts of interest when it is being injected by a spouse working as a

Democratic contractor trying to defeat Trump, and she is forwarding her own research to her husband's department and co-workers.

For instance, the same July 6, 2016, email that forwarded the anti-Trump screed also included research on an oligarch named Rinat Akhmetov, a Ukrainian that Nellie Ohr told Congress she was researching for Fusion for possible ties to Trump.

“Rinat Akhmetov is someone who also was associated with Manafort. Now, he’s Ukrainian, and right now, I can’t remember whether people explicitly, you know, pointed to particular organized crime activity that he’s suspected of,” she testified.

Other emails that Nellie Ohr forwarded to her husband and the other DOJ officials contained links to open-source information, such as news articles and academic research, that would later surface as evidence of alleged collusion between Trump and Russia. They included that:

- then-Russian ambassador to Washington Sergey Kislyak attended an April 2016 foreign policy speech by Trump. Former Attorney General Jeff Session eventually was forced to recuse himself from the Russia investigation as attorney general in part because he met Kislyak at that speech;
- then-Trump campaign adviser Carter Page gave a July 2016 speech in Moscow. Nellie Ohr bolded a passage in the article noting Page’s company “continues to work with Russian investments” and included someone tied to the Russian energy giant GazProm.

House GOP investigators who reviewed Nellie Ohr’s emails believe that their timing may be essential to understanding how the false Russian narrative — special counsel Robert Mueller’s report did not establish there was Trump-Putin collusion — may have gotten such credence inside DOJ and intelligence circles despite its overtly political origins.

For instance, just 24 days after the anti-Trump screed was emailed, both Ohrs met in Washington with British intelligence operative Christopher Steele. Nellie Ohr testified that she had known Steele from past encounters and learned at that July 31, 2016, meeting at the Mayflower Hotel that Steele, like herself, was working for Fusion GPS on Trump-Russia research. She said she learned that Steele had concerns that he hoped the DOJ or FBI would investigate, with help from her husband.

The next day, Bruce Ohr used his official DOJ position to go to then-Deputy FBI Director Andrew McCabe with Steele’s allegations (later to become known as the Steele dossier), and the bureau opened its first investigation into Russia collusion.

When asked by House lawyers during her deposition last year, Nellie Ohr testified that she did not discuss her Fusion GPS research before fall 2016 with anyone except possibly her husband (which she refused to answer, citing marital privilege) and Steele at the hotel meeting.

Bruce Ohr testified that his wife gave him a thumb drive of research to provide to the FBI during the 2016 election.

“At any point prior to fall of 2016, did you discuss your research on organized crime and Donald Trump with individuals outside of Fusion GPS, outside of this Mayflower breakfast meeting?” Nellie Ohr was asked during her congressional testimony last fall. “No,” she testified.

But the DOJ emails show that Nellie Ohr frequently forwarded open-source research on Russian organized crime figures, Trump, Manafort and developments in Ukraine with implications for the Trump campaign.

For instance, she directly alerted her husband and two DOJ prosecutors specializing in international crime on May 30, 2016, to the discovery of “black ledger” documents in Ukraine. “Reported Trove of documents on Ukrainian Party of Regions’ Black Cashbox,” Nellie Ohr wrote her husband, Holtyn and Wheatley, attaching [a news article](#) on the announcement of the Ukrainian release of the documents.

Those documents eventually led Manafort to resign from the Trump campaign and face criminal prosecution by Mueller’s team for improper foreign lobbying.

Two months earlier, in March 2016, Holtyn asked Bruce Ohr for permission for Wheatley and another DOJ prosecutor to speak to Nellie Ohr. “Do you think she would be comfortable with talking to them, and would it present any conflict of interest issues for her or for you?” Holtyn wrote.

Bruce Ohr forwarded the request to his wife: “Hi honey! I trust you are okay with this? Love, B.” She wrote back two consecutive emails with the words “Sure!” and “Cool.”

There is no indication in the emails about what the three discussed. But Holtyn and Wheatley were among those who received some of Nellie Ohr’s Russia/Ukraine research. Holtyn sent a second email suggesting Nellie Ohr had “impressive knowledge” on a topic that was redacted from the released email chain and could be “of assistance” to the DOJ. Officials told me they believe the topic was Russian oligarchs, a subject her husband was working on in his official role.

“Thanks so much Nellie. I’m back in country and will touch base soon on the email you sent us yesterday,” Wheatley wrote on May 4, 2016, after Nellie Ohr forwarded information on a Spanish arrest warrant against Russian crime figures.

On more than one occasion, Nellie Ohr forwarded articles about [Oleg Deripaska](#), the Russian aluminum magnate and former Manafort business partner. She testified that Deripaska was one of the focal points of her research.

As it turns out, the Russian also was being targeted by her husband and Steele. Emails, text messages and handwritten notes show that, during the 2016 campaign, they repeatedly discussed approaching Deripaska about delivering dirt on Manafort. The FBI eventually did so in fall 2016.

Rep. Mark Meadows (R-N.C.), one of those who questioned Nellie Ohr last fall, said he is reviewing the accuracy of her testimony given the recent emergence of the emails.

“If Ms. Ohr used her time at the opposition research firm to place information directly in the hands of investigators, it would be a severe conflict of interest,” Meadows told me. “Contrary to Ms. Ohr’s congressional testimony, it appears that she funneled research gathered during her time at Fusion GPS directly to the DOJ. A draft of a criminal referral for giving false testimony to Congress is currently being reviewed.”

Joshua Berman, a lawyer for Nellie Ohr, did not immediately respond to email and phone requests for comment.

Tom Fitton, head of Judicial Watch, said the memos raise serious questions of a conflict of interest hidden behind a marriage: “The documents show that Nellie Ohr had extraordinary access to the Justice Department. Nellie Ohr may as well as have had a desk at DOJ.”

Whatever transpires, it is clear Nellie Ohr was no ordinary spouse during the 2016 election. She was a robust source of Russia information for her husband and his colleagues inside the DOJ, at the same time her employer was trying to smear Trump.

And that should concern us all.

John Solomon is an award-winning investigative journalist whose work over the years has exposed U.S. and FBI intelligence failures before the Sept. 11 attacks, federal scientists’ misuse of foster children and veterans in drug experiments, and numerous cases of political corruption. He serves as an investigative columnist and executive vice president for video at The Hill. Follow him on Twitter [@jsolomonReports](#).

Mr. GAETZ. I also seek unanimous consent to enter into the record a New York Times article, December 12, 2018, "Ukrainian Court Rules Manafort Disclosure Caused 'Meddling' in U.S. Election."

Chairman NADLER. Without objection.
[The information follows:]

MR. GAETZ FOR THE OFFICIAL RECORD

Ukraine Court Rules Manafort Disclosure Caused 'Meddling' in U.S. Election

By [Andrew E. Kramer](#) Dec. 12, 2018



Paul Manafort, center, arriving for his arraignment hearing at the federal courthouse in Alexandria, Va., in March. Al Drago for The New York Times

MOSCOW — A court in Ukraine has ruled that officials in the country violated the law by revealing, during the 2016 presidential election in the United States, details of suspected illegal payments to Paul Manafort.

In 2016, while Mr. Manafort was chairman of the Trump campaign, anti-corruption prosecutors in Ukraine disclosed that a pro-Russian political party had earmarked payments for Mr. Manafort from an illegal slush fund.

Mr. Manafort resigned from the campaign a week later.

The court's ruling that what the prosecutors did was illegal comes as the Ukrainian government, which is deeply reliant on the United States for financial and military aid, has sought to distance itself from matters related to the special counsel's investigation of Russia's interference in the 2016 presidential race.

Some of the investigation by the special counsel, Robert S. Mueller III, has dealt with Mr. Manafort's decade of work in Ukraine advising the country's Russia-aligned former president, Viktor F. Yanukovich, his party and the oligarchs behind it.

Sign up for The Interpreter

Subscribe for original insights, commentary and discussions on the major news stories of the week, from columnists Max Fisher and Amanda Taub.

After President Trump's victory, some politicians in Ukraine criticized the public release by prosecutors of the slush fund records, saying the move would complicate Ukraine's relations with the Trump administration.

In Ukraine, investigations into the payments marked for Mr. Manafort [were halted](#) for a time and never led to indictments. Mr. Manafort's conviction in the United States on [financial fraud charges](#) related to his work in Ukraine was not based on any known legal assistance from Ukraine.

Two Ukrainian members of Parliament had pressed for investigations into whether the prosecutors' revelation of the payment records, which were [first published in The New York Times](#), had violated Ukrainian laws that, in some cases, prohibit prosecutors from revealing evidence before a trial.

Both lawmakers asserted that if the release of the slush fund information broke the law, then it should be viewed as an illegal effort to influence the

United States presidential election in favor of Hillary Clinton by damaging the Trump campaign.



Artem Sytnik, the head of the National Anti-Corruption Bureau of Ukraine, said he had revealed the information about Paul Manafort "in accordance with the law in effect at the time." Oleksandr Stashevskiy/Associated Press

The Kiev District Administrative Court, in a [statement](#) issued Wednesday, said that Artem Sytnik, the head of the National Anti-Corruption Bureau of Ukraine, the agency that had released information about the payments, had violated the law. The court's statement said this violation "resulted in meddling in the electoral process of the United States in 2016 and damaged the national interests of Ukraine."

A spokeswoman for the anti-corruption bureau said she could not comment before the court released a full text of the ruling. In an interview last June, Mr. Sytnik said he had revealed the information "in accordance with the law in effect at the time."

The court also faulted a member of Ukraine's Parliament, Serhiy A. Leshchenko, who had commented on Mr. Manafort's case and publicized at a [news conference](#) materials that the anti-corruption bureau had already posted on its website.

Mr. Leshchenko said he would appeal the ruling, and that the court was not independent and was doing the bidding of the Ukrainian government as it sought to curry favor with the Trump administration.

"This decision of the court is for Poroshenko to find a way to Trump's heart," he said, referring to President Petro O. Poroshenko. "At the next meeting with Trump, he will say, 'You know, an independent Ukrainian court decided investigators made an inappropriate move.' He will find the loyalty of the Trump administration."

Mr. Leshchenko said the prosecutors' revelations about Mr. Manafort were legal because they were "public interest information," even if they were also potential evidence in a criminal investigation.

Mr. Manafort has not been charged with a crime in Ukraine, and earlier this year, Ukrainian officials froze several investigations into Mr. Manafort's payments at a time when the government was negotiating with the Trump administration to purchase sophisticated anti-tank missiles, called Javelins.

Ukraine's prosecutor general said the delay on Mr. Manafort's cases was unrelated to the missile negotiations. In total, the United States provides about \$600 million in bilateral aid to Ukraine annually.

Earlier this month, the special counsel accused Mr. Manafort of violating a cooperation agreement by lying. [Two of the five alleged lies](#), according to the filing, related to meetings or conversations with [Konstantin V. Kilimnik](#), Mr. Manafort's former office manager in Kiev, whom the special counsel's office has identified as tied to Russian intelligence and as a key figure in the investigation into possible coordination between the Trump campaign and

Russia.

Ukrainian law enforcement officials last year allowed Mr. Kilimnik to leave for Russia, putting him out of reach for questioning.

Mr. GAETZ. Finally, also from December 12, 2018, from the Kiev Post, "Update: Publication of Manafort Payments Violated Law, Interfered in U.S. Election, Kiev Court Rules."

Chairman NADLER. Without objection.

[The information follows:]

MR. GAETZ FOR THE OFFICIAL RECORD

UPDATE: Publication of Manafort payments violated law, interfered in US election, Kyiv court rules

Published Dec. 12, 2018. Updated Dec. 12 2018 at 2:45 pm



Editor's Note: This story has been updated to include a statement by MP Serhiy Leshchenko.

Two Ukrainian officials violated the law by revealing information about

millions of dollars of alleged illegal cash payments to lobbyist and former chair of U.S. President Donald Trump's election campaign Paul Manafort, a Kyiv district court said on Dec. 12.

In reviewing an administrative case filed by lawmaker Boryslav Rozenblat, the court concluded that Artem Sytnyk, director of the National Anti-Corruption Bureau of Ukraine, and parliamentarian Serhiy Leshchenko acted illegally when they revealed that Manafort's surname and signature were found in the so-called "black ledger" of ousted President Viktor Yanukovych's Party of Regions.

The "black ledger" is alleged to be a secret accounting book showing suspicious payments by the party to a range of individuals and officials. It became a key document implicating Manafort in corruption in Ukraine, and helped to end his tenure as Trump's campaign chair.

In a [statement on its website](#), the court also appeared to describe the two men's actions as constituting interference in the 2016 United States presidential election.

The release of information about the "black ledger," which was part of a pre-trial investigation, "led to interference in the electoral processes of the United States in 2016 and harmed the interests of Ukraine as a state," the court's press service wrote.

The court also declared that Leshchenko acted illegally and termed his actions "interference in the external politics of Ukraine by spreading the above-mentioned information about Paul Manafort."

In October 2017, the court launched judicial proceedings in Rozenblat's suit against Sytnyk and Leshchenko. In the suit, the lawmaker called on the court to recognize the two men's actions as illegal.

In its Dec. 11 ruling, the court partially satisfied the demands of the plaintiff because Sytnyk and Leshchenko, as “subjects of state authority,” could not prove that they spread the information about Manafort without violating the law, the court’s press-service wrote.

In response to the ruling, Leshchenko [published a post on Facebook](#) suggesting that the decision was aimed at helping President Petro Poroshenko remove Sytnyk from office. By finding the National Anti-Corruption Bureau chief in violation of the law, the government will attempt to deflect criticism from among Western diplomats in Kyiv if he is removed, Leshchenko claimed.

“In response to criticisms about how (firing Sytnyk) is unacceptable, the scammers in the president’s circle will say: we’re firing him for illegally influencing the elections in the U.S.,” Leshchenko wrote.

In 2005, Manafort went to work for the Party of Regions in Ukraine after mass protests prevented its leader, then Prime Minister Yanukovich, from assuming the presidency after the falsified 2004 election. That event, known as the Orange Revolution, became the impetus for a large and extremely expensive campaign to burnish Yanukovich’s reputation in Western capitals.

Manafort’s consulting would eventually help Yanukovich win the presidency in 2011. After a tenure marred by excessive corruption, Yanukovich would subsequently be forced from power by the EuroMaidan Revolution in 2014 and flee to Russia.

In May 2016, Leshchenko published information from the Party of Region’s “black ledger” showing that the party spent large sums of money on paid advertising and the services of top state officials.

In August 2016, the National Anti-Corruption Bureau of Ukraine published a report indicating that Manafort's name was found in the ledger alongside a list of payments. It [concluded](#) that Manafort could have received more than \$12 million from the Party of Regions since 2007.

That revelation helped force Manafort to abandon his role as Trump campaign chair. However, it also proved controversial in Ukraine.

After Trump's November 2016 election, Nazar Kholodnytsky, head of the Special Anti-Corruption Prosecutor's office, said his agency could not prove the authenticity of Manafort's supposed signature in the ledger. It also saw no grounds to press charges against Manafort.

In January 2017, the news site Politico published an article suggesting that Ukrainian government officials attempted to use the "black ledger" to interfere in the U.S. presidential election in favor of Trump's rival for the presidency, Secretary of State Hillary Clinton.

In June 2017, Yaroslav Hordiyevych, spokesperson for the Special Anti-Corruption Prosecutor's office, [told the Kyiv Post](#) that his agency did not support Leshchenko and the National Anti-Corruption Bureau's decision to release the information.

Claims that Ukraine attempted to interfere in the U.S. presidential election have even reached Trump himself. In July 2017, the U.S. president [wrote in a tweet](#): "Ukrainian efforts to sabotage Trump campaign – 'quietly working to boost Clinton.'"

In his Facebook post, Leshchenko suggested this was another reason for the court ruling.

"With this decision, Poroshenko will try to earn additional loyalty from the

Trump Administration, so it will close its eyes to any violations during the (March 2019 Ukrainian presidential) elections and the use of administrative resources, so that the ruling corrupt officials remain in power," he wrote.

Mr. GAETZ. Thank you, Mr. Chairman.

So, what is happening is that DNC pays a law firm to hire Fusian GPS, which hires Nellie Ohr. Nellie Ohr then sends an email to her husband about issues with Manafort and the Ukraine. That then works its way into the U.S. election dynamic, and a court in Kiev ruled that the activities to disclose the Manafort activities in the United States proximate to the 2016 election constituted election interference and was illegal under Ukrainian law.

Is there anyone on the panel who has a reason to disagree with the conclusion of the Ukrainian court that that constituted election meddling?

[No response.]

Mr. GAETZ. Okay. So, no one has reacted, any basis to disagree with the Ukrainian court, and the record can reflect that.

So, my question to Ms. Floris is what are we doing as a government to prevent future election meddling like that which Ukraine engaged in, where information was disclosed in the United States unlawfully in the foreign jurisdiction and then entered into the bloodstream of our politics?

Ms. FLORIS. Thank you, sir, for the question.

So, I will harken back to what I said previously. So, the FBI certainly is not in a position to police content on the Internet. That being said, if the FBI can identify a foreign actor, regardless of country, who is trying to push out disinformation with the end goal of sowing discord, disrupting our electoral process, and it is done in some sort of a subversive or undeclared or criminal manner, that is where it becomes an investigative interest to the FBI.

The trick, sir, is identifying that known foreign actor. Again, we can't work back from content. We cannot police content on the Internet. So, if we find that foreign actor behaving in foreign influence operations and part of that operation entails disinformation, the FBI will work with the social media providers to provide as much actual intelligence as we possibly can.

Mr. GAETZ. So, in this case, it looks like we must know the actor because a court ruled that the disclosure of the information was illegal. So, is there anything that the FBI is doing now to follow up on the decision by a Ukrainian court that there was illegal election meddling in the United States that emanated from the Ukraine?

Ms. FLORIS. Sir, I can't address anything related to the possibility or existence or non-existence of an FBI investigation.

Mr. GAETZ. It would seem, I think that my colleague from Washington, Ms. Jayapal, said with so few days between now and the upcoming election, it is just—I know you can't comment maybe on this setting, but I hope sincerely that this Ukrainian election meddling is being identified and being pursued by our government.

I yield back.

Chairman NADLER. The gentleman yields back. The gentleman from Florida, Mr. Deutch?

Mr. DEUTCH. Thank you, Mr. Chairman. Thanks for holding today's hearing. Thanks to the witnesses for being here.

We know that Russians interfered in our 2016 election. We know that national security experts have warned that they will do it again in 2020. The 2020 primaries are fast approaching. So, we are running short on time to ensure that every State is taking the nec-

essary action to harden our election defenses, guard against disinformation, and improve election Administration generally.

Florida was one of fewer than 20 States that still had elections with electronic machines without a paper trail to verify the ballots in 2016. Thankfully, our State is moving in the right direction. Between 2016 and 2018, the number of counties who had paperless elections dropped from 24 to 4, with efforts to move completely to paper-verified systems underway.

Now after learning that some of our systems were hacked in 2016, Floridians expect a strong response to bolster election security, and we expect that whatever is done will improve coordination with State and counties targeted by foreign governments and other bad actors.

According to the Mueller report, the Russian military intelligence agency was able to gain access to the network of at least one Florida county government. Subsequently, Members of our congressional delegation requested a briefing from law enforcement agencies and were informed that the networks of at least two Florida counties have been compromised.

Most recently, a report by the Republican-led Senate Intelligence Committee suggests that as many as four Florida counties may have been successfully attacked. Apparently, no tabulation systems were accessed, only registration rolls. Whatever the number of counties impacted, we have got to learn the lessons of 2016 and guard against these vulnerabilities before next year's elections. Florida clearly has work that it needs to do, from hardening election systems to improving auditing procedures, but we can't do it alone.

Mr. Masterson, certain breaches in 2016 were not immediately detected. What signs should election officials look for? What should they be trained to look for on Election Day to ensure that there are no undetected attacks, and how are you working with State officials to train them to detect such signs?

Mr. MASTERSON. Yes, thank you for the question, sir.

It starts long before Election Day so that you may be looking for those signs on Election Day, and I will talk about our activity there, but there are indicators that election officials are aware of and can be attuned to. For instance, in the States that offer early voting, you may begin to see signs of provisional ballots or registration roll activity that is anomalous. The ability to detect that and investigate the registration rolls to see if there is any kind of anomalies there is important.

So, there are early indicators that can be gained through something like early voting. In addition, and your home State of Florida is a perfect example, the deployment of our Albert intrusion detection sensors across all 50 States' election infrastructure allows for real-time alerting to not just the election official, but to our Elections Information Sharing and Analysis Center regarding possible malicious activity targeting election infrastructure.

I would note in the State of Florida, Florida was the first State to deploy those Albert sensors across all county governments, and so Florida is uniquely positioned for that kind of intrusion detection and alerting.

In addition, having that auditability in place that you mentioned, those auditable records. I think in Florida, there was less than 100 ballots cast in 2018 on auditable systems, and a drive towards complete auditability by 2020 is really critically important so that we can detect and recover from this.

Mr. DEUTCH. Thank you. Thank you very much, Mr. Masterson.

In our hearing on election security last month, the witnesses stressed the importance of treating elections as “interconnected systems.” We heard that any digital device that touches election processes must be safeguarded. Device security management should be centralized and streamlined.

So, I would like to hear from each of the witnesses what your organization is doing to help centralize and streamline the election security process. Mr. Hovland, we will start with you.

Mr. HOVLAND. Yes. So, essentially, at the Election Assistance Commission, we are participating in the Government Coordinating Council. We consistently work to put out best practices. Again, our capacity beyond our statutory requirements is very limited.

As we have the World Series coming to Washington, I would note that if we were a Major League Baseball player, we would be the 173rd highest-played player. We would be a middle reliever. We have no lack of ambition to take on these challenges and help, but we need the resources to do it.

Mr. DEUTCH. Appreciate the World Series reference. Mr. Hickey?

Mr. HICKEY. Sir, I am going to answer a bit by analogy. We have a number of department components that touch election security. We have got FBI agents in the field and at headquarters. We have got prosecutors in the field. We have got public corruption prosecutors. We have got national security prosecutors. We have got computer crime prosecutors.

All of them potentially touch this issue, and so it is on us to train them, so they are aware of each other and coordinated, and that is what we are doing this week. At the end of the week—rather, on the end of the month, the FBI is pulling together an all hands meeting with agents from around the country to train them, including on how to react and relate to State officials when it comes to victim notification.

Mr. DEUTCH. Ms. Floris?

Ms. FLORIS. Sir, thank you for your question.

I would just stress again the creation of the Foreign Influence Task Force, whose purpose was to do just what you asked, sir, to coordinate the efforts across the enterprise as it relates to election security. We have got elections crimes coordinators across all 56 of our field offices whose primary goal is to interact with State and local election officials, leading up to the day of the election.

We have got our cyber task forces across all 56 of our field offices, and we are working to increase our CI task forces as well. Again, the Foreign Influence Task Force really is that hub that brings all that effort together, again leading up to, during, and after the election.

Mr. DEUTCH. Thanks. Mr. Chairman, can Mr. Masterson just quickly answer that question?

Chairman NADLER. The gentleman may answer the question.

Mr. MASTERSON. Yes, thank you for the question, sir.

Across CISA, the Cybersecurity and Infrastructure Security Agency, over a third of our employees in 2018 engaged in election security work across the United States. We have field representatives, protective security advisers, cybersecurity advisers engaging directly with State and local election officials. Then my team, the Election Security Initiative, is the hub of that information.

So, as we get reporting, as we get requests for services, we are able to quickly and efficiently serve the needs of the community in order to make sure they have the information or services to help to manage risk to their systems.

Mr. DEUTCH. Okay. Thanks for what you all do. Mr. Hovland, I hope we have a chance to talk about what additional resources would mean in this effort.

Thank you, Mr. Chairman.

Chairman NADLER. The gentleman yields back. The gentleman from Texas?

Mr. GOHMERT. Thank you, Mr. Chairman, and appreciate the witnesses being here today.

Ms. Floris, so did you replace Peter Strzok as Deputy Assistant Director of Counterintelligence Division?

Ms. FLORIS. Sir, there are three Deputy Assistant Directors in the Counterintelligence Division. My particular role is over the Intelligence Branch. Mr. Strzok was not over the Intelligence Branch. He was over one of our two operational branches within the division.

Mr. GOHMERT. He was the one that was briefed by the intel community IG about Hillary Clinton's private server potentially being hacked. Do you know why you were not included in that briefing?

Ms. FLORIS. Yes, sir. I did not enter this position until the fall of 2018. During the 2016 timeframe, I was in the Counterterrorism Division.

Mr. GOHMERT. Okay. So, you came into your current position after Peter Strzok left?

Ms. FLORIS. Yes, sir.

Mr. GOHMERT. Well, since the Foreign Influence Task Force is a headquarters component, I am concerned that Peter Strzok ran two of the biggest cases in FBI history as headquarters special cases rather than the traditional way of running cases through field offices. Is the Foreign Influence Task Force running election cases from headquarters now?

Ms. FLORIS. No, sir.

Mr. GOHMERT. Then can you tell us the reason they were doing so when Peter Strzok was there?

Ms. FLORIS. Sir, I cannot speak to why things were done or not done during Peter Strzok's time. I can just speak to currently what we are doing in the Foreign Influence Task Force, which is essentially program managing the cases across our 56 field offices.

Mr. GOHMERT. Well, I would think that since there is such a big deal about influence peddling in 2016, even though you came in after that, that you would be a little bit concerned about the influence peddling when Peter Strzok was there. Are you not? Have you not looked into that at all in your current position?

Ms. FLORIS. Sir, my focus is on the 2020 elections and moving forward. The creation of the Foreign Influence Task Force hap-

pened in the fall of 2017. We are laser focused on the elections moving forward.

Mr. GOHMERT. So, you don't think there is anything to be learned from looking at what occurred in the 2016 election to help you prepare for what is going on and could go on in the 2020 election? Really, you don't think there is anything to learn from history?

Ms. FLORIS. Sir, there are always lessons to be learned from history. What we have learned in 2016—and I can speak strategically, not just what was happening in the FBI—was really a lack of coordination on the foreign influence threat across the entire U.S. intelligence community. We are now better engaged. We collaborate far more on a daily basis. We are working with our social media companies. All of this, lessons learned from 2016, lessons learned from 2018, and we are going to continue to put best practices forward as we move into 2020.

Mr. GOHMERT. Well, since you are concerned about 2020, have you—were you aware of President Petro Poroshenko dispatching Olga Bielkova or any other Ukrainian officials to the U.S. to influence our election in 2016?

Ms. FLORIS. Sir, I am not familiar with that.

Mr. GOHMERT. Are you aware—do you know who Olga Bielkova is?

Ms. FLORIS. Sir, again, I am not going to confirm or deny the existence or non-existence of FBI investigations or persons of interest to the FBI in this setting.

Mr. GOHMERT. That was not my question. I didn't ask you that. I asked you, do you know who that is?

Ms. FLORIS. Sir, I am not going to answer that question in this setting. I am happy to come back in a closed setting and go into detail about current investigations that we have related to foreign influence.

Mr. GOHMERT. So, you can't even say if you know a person?

Ms. FLORIS. No, sir.

Mr. GOHMERT. Do you realize you are supposed to be telling us about 2020, and you can't even tell us about whether you know anything about people involved in 2016? It really hurts the credibility when you can't do that.

Let me ask you, will the FITF run informants against political campaigns?

Ms. FLORIS. Sir, much in the same vein that the FITF does not run cases, we do not run sources either. We program manage the sources that our 56 field offices run as it relates to foreign influence.

Mr. GOHMERT. Well, I have a real concern about the credibility of what is happening for 2020 if you can't even tell us that you even know people from the Ukraine. So, I am very disturbed and concerned.

Chairman NADLER. The gentleman yields back. The gentleman from California, Mr. Correa?

Mr. CORREA. Thank you, Mr. Chairman.

First, I want to say to our panelists today thanks for being here today and thank you for service to our country.

As you know, trust in our election system is the foundation of our democracy, and when it comes to cyberattacks, time is of the

essence. When financial institutions are attacked or our military, the response is within seconds. It is usually coordinated throughout the industry—not institutions, not individually, but the industry, if not worldwide.

So given the importance of America's democracy, I presume that we are now and, Ms. Floris, you were talking about lack of coordination, I believe you said, in 2016 among Government agencies as being one of the lessons learned. I presume we have a system in place now to coordinate that kind of information when there is a cyberattack throughout Federal Government? Yes/no question to all of you.

Ms. FLORIS. Sir, thank you for the question, and you are absolutely correct. As it relates to cyber incidents, we do have an extremely strategic plan in how we notify our victims. So, simply put, and I will certainly yield to my colleague from DHS to add on here, the FBI and DHS respond to incidents jointly. You can almost look at it as the FBI lead in essentially the threat response. If a crime has been committed, the FBI will open an investigation.

DHS is the lead for protecting and mitigating whatever vulnerability existed that led to the cyber intrusion in and of itself.

Mr. CORREA. So let me interrupt you. So, you open up an investigation, but a cyberattack happens within seconds. So how quickly—who is the lead or if you don't have a lead, how do you get that information out to all of your investigative agencies, your defense task force, instantaneously? Do you have that system in place?

Mr. Masterson?

Mr. MASTERSON. Yes, sure. Thank you for the question.

Following 2016–2017, one of our top priorities was to work with State and local election officials to establish communications protocols for exactly this reason. As you may be aware, in 2016, DHS, being new to the election space, didn't even know who to call in the States if need be. We now have points of contact in all the States. We have information sharing going to all 50 States.

Mr. CORREA. So, you do have points of contacts with each and every State?

Mr. MASTERSON. Yes. More importantly, they know how to share information with us because the most likely people to report a cyber incident are the owners and operators—

Mr. CORREA. So, you do have a specific individual at each State that you talk to?

Mr. MASTERSON. Yes.

Mr. CORREA. Is the information—are we talking silos here, or is the information a two-way street, so to speak? Do you have folks at the State level who you trust, who you can work with to make sure you are all sharing the information on a real-time basis?

Mr. MASTERSON. Absolutely, sir. Thank you for that question.

We have points of contact and trusted relationships across all 50 States so that they feel comfortable sharing that information. Then we are able to take and not just respond to that individual incident, but take the technical information in that response and distribute it broadly across the entire election community so they can take defensive actions or look for possible compromises across the entire election infrastructure.

That is the biggest area of improvement since 2016 is the amount of information we are receiving from the State and local election officials on a regular basis, whether it is reporting or those Albert intrusion detection sensors.

Mr. CORREA. So, if Secretary of State Alex Padilla from the State of California calls one of you, and it is the wrong telephone, do you return his call immediately, or how that phone call get channeled into the system to get a quick response?

Mr. MASTERSON. Yes—

Mr. CORREA. Or is it even a phone call? Do you have a digital system where somebody puts in a—types in an alert saying something is going on over here, a certain virus is being detected, so the rest of the country can essentially get on their toes?

Mr. MASTERSON. Yes. So, first, Secretary Padilla has my number and calls me regularly and is an incredibly active, engaged partner with us. You have described it exactly correctly. A report to one is a report to across the Federal Government. Within CISA's operation center, we have Members of the FBI, we have Members of the intelligence community, we have Members of our Elections Information Sharing and Analysis Center sitting on our operations floor such that as reporting comes in, we are able to take that information, analyze it, support the victim, but then begin the process of sharing information broadly across the sector.

Mr. CORREA. Let me shift very quickly. It was mentioned earlier the elections are not just about Election Day, but that election period. In California, that is about 3 weeks, as well as other States.

How do you assure that whatever you begin to detect 3 weeks out is something that you follow up on and is coordinated?

Mr. MASTERSON. Yes, again, working through our Information Sharing and Analysis Center, as we get reporting, if there are additional facts, additional jurisdictions, we are able to coordinate that across the whole of Government and look for those trends, look for that information that would connect incidents.

Mr. CORREA. Final question for you. I am out of time, but I have been through a number of elections. I detected irregularities. I try to call my local D.A. So, in 2020, I am out there, walking door-to-door. I see something weird happening. Who do I call? Or do I Google your telephone number?

Mr. MASTERSON. So, depending on the activity—

Mr. CORREA. We talked about coordination of private and public sector individuals out there.

Mr. MASTERSON. Yes. So, from our perspective at CISA, one is you should report any anomalous activity to the local election official, the local election administrator, who can understand the activity you are seeing and remediate it. In addition, we worked with voter protection groups in 2018 and will again in 2020 to have points of contact on Election Day so that if there is reporting that indicates trends, we are able to respond, reach out to the election officials in coordination and understand what is going on.

Mr. CORREA. Mr. Chair, I yield.

Chairman NADLER. The gentleman yields back. I now recognize the distinguished vice chair of the Committee and thank her once again for beginning the hearing in my absence, the gentlelady from Pennsylvania.

Ms. SCANLON. Thank you, Chairman.

Ms. Floris, on October 3rd, the FBI, along with DHS, issued an advisory to State election officials that the Russian government would be using voter suppression tactics to interfere in the 2020 elections, and obviously, we are extremely concerned about that.

Can you give us any idea about when the FBI learned about these Russian tactics and any gap in time between when the threat was identified and when the States were notified?

Ms. FLORIS. Thank you for the question, ma'am.

I cannot speak in specifics about the reporting. I am happy to take that back for an after action. I will say as we roll into 2020, as we did as we were rolling into 2018, it is our goal—and not just the FBI's goal, but across the U.S. intelligence community—to report threat information as quickly as possible to the audience who needs to hear it, taking into account certainly the sensitivity of the sources and methods of how that intelligence was collected.

Ms. SCANLON. Okay. You have talked a little bit about the Foreign Influence Task Force that was formed in 2017, and I think you described how it was expanded after the 2018 election, and you described a growing list of foreign adversaries that you are looking at. Can you tell us what resources—can you describe the number of people who make up that task force and whether that has grown from 2017 to the present and if you need additional people or resources to do that job?

Ms. FLORIS. Thank you, ma'am, for the question.

I am not going to get into specifics about the actual number of individuals on the task force. What I will say is we certainly surged resources as we rolled into 2018. Our intention is that we again are going to surge resources as we roll into 2020.

One thing I will note that individuals on the FITF are not the only individuals in the FBI who are working the foreign influence threat. Just given the nebulous nature of it, it is wedded in so much of what we do in the investigative side of the house, from criminal to cyber to counterterrorism as well. So, there are agents and analysts and professional staff across all 56 of our field offices who work foreign influence and investigations tied to foreign influence.

Regarding your question about resources, as I stated earlier, we are always happy to have more resources and can use more resources. But the FBI is using everything we can right now to mitigate this very serious threat.

Ms. SCANLON. Okay. Is the reason you can't give us numbers, relative numbers between 2017 and the present, because you don't have them, or is there some security reason?

Ms. FLORIS. There is no security reason. It is just it is hard to compare since in 2017, we were focused only on Russia. With the expansion to include all global actors who are participating in foreign influence operations, it is not necessarily a good one-to-one comparison of where we have come.

Ms. SCANLON. Okay. Mr. Hickey, you mentioned that one aspect of the DOJ's efforts to disrupt malign foreign influence operatives is stepped-up enforcement of FARA, the Foreign Agents Registration Act, which requires people who Act as agents of foreign principals to register with our government.

So, I guess we know some of those enforcement acts that would include the guilty plea by Michael Flynn, who was Trump's first National Security Adviser; the convictions of the Trump campaign manager, Paul Manafort and Richard Gates; the possible involvement of Mr. Giuliani and his associates who were arrested last week for possible FARA violations. Are those all the kind of things you are talking about?

Mr. HICKEY. With respect to that last case, at the moment, those are campaign finance violations. I think the charges allege a connection to a foreign—foreign location, so the kind of activity we want to be alert to.

Ms. SCANLON. Is included there?

Mr. HICKEY. So, at the moment, the charges are campaign finance allegations. I don't think FARA is pled there. Stepping back from that specific case, if there are indications of a foreign principal covertly trying to influence our politics, whether through campaign finance or political activities under FARA, that is something that we would be involved in.

Ms. SCANLON. Okay. The one I am really concerned about, which is listed on DOJ's FARA enforcement actions, is the one involving the 13 Russian nationals who worked on behalf of the Russian government to interfere in the 2016 election by manipulating social media to advocate for the Trump campaign and against the Clinton campaign because that included organizing political rallies in States like Pennsylvania, which I represent. They literally took pictures of Pennsylvania coal miners and slapped them on these rally things and tried to stir up sentiment in a particular direction.

Does DOJ have the resources it needs to identify and prosecute malign actors such as those I mentioned as we approach the 2020 election?

Mr. HICKEY. Well, indeed, we do because we have used those resources to bring that case. Fortunately, I think the 2020 budget includes additional funding for the sections I supervise, including the Counterintelligence Section, which is devoted to foreign influence, countering malign foreign influence, in addition to cyberthreats and other counterintelligence activities.

Ms. SCANLON. How about moving proactively before the 2020 election because, unfortunately, those convictions came 2 years after the influence in 2018?

Mr. HICKEY. Yes. As I said in my opening statement, my testimony, preventing a crime or disrupting it is more rewarding and more important than convicting someone after the fact, and we have put a lot of thought into how we will disrupt that and whether we will provide notifications to Congress, to the public, based on various factors, including wanting to make sure that the public is as educated as we can make them.

Ms. SCANLON. Thank you to all the witnesses. I see my time has expired.

Chairman NADLER. The gentlelady yields back. The gentlelady from Texas?

Ms. GARCIA. Thank you, Mr. Chairman.

As my colleague Ms. Jayapal noted earlier, the Senate Intelligence Committee report on Russian interference in 2016 election states that many—disinformation campaigns and cyberthreats do

not just manipulate just one platform. The information moves across various platforms where a cyberattack threatens multiple companies' network security and data integrity. There must be greater cooperation with the tech sector and between the tech sector and the Government to address these issues.

In fact, we saw today that Facebook removed a network of Russian-backed accounts that posted as locals commenting on political issues in swing States praising President Trump and attacking former Vice President Joe Biden. This is a familiar threat that we saw in 2016 and appears to be repeating as we approach 2020.

The report we referenced represents formalized mechanisms for collaborations that facilitate content sharing among social media platforms to defend against foreign disinformation. This occurred with violent extremist content.

My question is to Mr. Masterson and Ms. Floris, and this is simply a yes or no. Have your organizations created a task force to coordinate cooperation between Government and the tech sector as they did with violent extremist content?

Mr. MASTERSON. So, I will defer to my colleague at the FBI as well, but yes, we are working within my team at the Election Security Initiative. We have a team working on countering foreign influence that works regularly with the social media and tech sector on these issues.

Ms. GARCIA. Will be ready for 2020?

Mr. MASTERSON. Absolutely, yes.

Ms. GARCIA. Okay. Ms. Floris?

Ms. FLORIS. Thank you, ma'am, for the question.

So, within the Foreign Influence Task Force is a significant effort to increase engagement with both the tech sector and the social media companies. Folks from the FITF meet almost monthly with those companies. What we have tried to do is create a bidirectional relationship wherein we share with them actionable intelligence and threat indicators. They, in turn, share with us information related to individuals who have violated their terms of service. So, it is certainly one of our primary strategies as we roll into 2020.

Ms. GARCIA. Do you have a specific task force that helps coordinate all of that, or are you just leaving it up to each group to cooperate with each other?

Ms. FLORIS. It is actually within the Foreign Influence Task Force. That is one of our goals is to coordinate that engagement with social media companies as it relates to foreign influence.

Ms. GARCIA. All right. So, DHS' May 2019 report detailed the disinformation model, including false information operations, deep fake technology, and digital message creation attacks. Can you please describe the impact of these type of threats to our elections and what DHS is doing to combat them, particularly regarding misinformation about voter registration? Mr. Masterson?

Mr. MASTERSON. Yes, thank you, ma'am.

My team within the Election Security Initiative, starting in 2018, began working with State and local election officials to talk to them about ways to engage voters about disinformation around the election process. Election officials see this regularly, whether through social media or other activity. It is not new to election Administration.

So, we wanted to work with them on a variety of products to help them engage the electorate on what to look for, but more importantly, how to empower themselves as voters. To check their voter registration status to make sure it is up to date, to make sure they understand when and where to vote, what is on their ballot, how the election process works, and most importantly, to understand who the trusted voices in their communities are. Those local election officials and State election officials that have the information they need, so that they can head to the polls with confidence.

Building on that effort, heading into 2020, our team is focused on expanding that engagement, working with trusted voices across communities—whether that is mayors, governors, or others—to engage the American people about how to identify disinformation and how to build resilience so they are not responsive—

Ms. GARCIA. I heard your testimony on that, but I note your written testimony, you also said that you wanted to raise public awareness. With 8,800 jurisdictions—one of you all testified to that. I forget which one of you. I mean, how are you really getting the work out with 8,800 jurisdictions that have to be on the lookout for this. I mean, you are talking across the country.

When I saw, again in all testimony, I think you were focused on like a handful of States that you have done some of these tabletop exercises. So, what are you really doing to make sure that all 8,800 election jurisdictions know how to detect, report, and work with you on these issues?

Mr. MASTERSON. Yes, absolutely. Thank you for the question.

So, it is twofold. One is by building those relationships with the State election officials, they reach the counties, too. So, I mentioned in my testimony the Last Mile Initiative. That is an initiative geared towards county election officials specific to their jurisdictions about how to manage risk and threat, including how to talk to voters about the process and manage voters' expectations.

The second is, and you mentioned the tabletops, it is not just the individual tabletops with States. We conduct national-level tabletop exercises where thousands of local election officials, in coordination with their State election officials—so their chief State election official—participated over 3 days this year.

Then next year, we anticipate a high level of participation to talk through exactly what you said. How does information get shared? How do we push it down to the locals? Then how do they get it back up to us so that we have full awareness and can push broadly to the elections community to understand what is the threat of risk, and how do they protect the systems?

Ms. GARCIA. Thank you, Mr. Chairman. I yield back.

Chairman NADLER. The gentlelady yields back. The gentleman from Colorado?

Mr. NEGUSE. Thank you, Mr. Chair, for holding this incredibly important and timely hearing.

I also want to thank each of the witnesses for their testimony and also for your service to our country. I must confess I am disappointed by some, not all, but some of my colleagues on the other side of the aisle who chose to use their time impugning the integrity of former Government officials instead of talking today with these distinguished witnesses about the subject matter at hand,

which is protecting our republic and ensuring the integrity of our elections. I realize that each of you, in your respective departments, work with a wide range of colleagues on precisely that, and I thank you for it.

I reviewed the written testimony of each of the witnesses. Ms. Floris, in your testimony, you noted on page 3—and I believe you alluded to this in your verbal testimony—that in the run-up to the 2018 midterm elections, social media companies deactivated more than 1,000 inauthentic social media accounts linked to malign foreign influence actors. The companies made these decisions informed by dialogue and information exchanges with the FBI and other Government agencies.

So, I take from that that you have a robust relationship with the social media companies, both the FBI, the task force, and obviously other apparatuses of DOJ. I take that to be true. Is that a fair estimate?

Ms. FLORIS. Yes, sir.

Mr. NEGUSE. Okay. I very much appreciate the work that the task force and that the FBI and the other entities within our law enforcement community are taking, the steps that they are taking to protect the integrity of our elections. Part of what is the most disturbing for me and gives me the most pause, and I suspect some of my colleagues, is what you mentioned earlier, Ms. Floris, which is that it is happening in real time.

Foreign actors, by virtue of the disinformation and misinformation campaigns that they are engaged in, utilizing the ubiquitous social media engines that we all now use in our daily lives, they are changing the way Americans think and Americans interact with each other, the way in which we view public policy issues.

I am sure you are familiar—there was a report recently—it was covered by CNN—from Graphika, the IRACopyPasta campaign issued on October 21, 2019. Russian accounts posing as Americans on Instagram targeted both sides of polarizing issues ahead of the 2020 election. Are you familiar with this report?

Ms. FLORIS. In title only, sir.

Mr. NEGUSE. In title only? Okay.

Ms. FLORIS. Yes, sir.

Mr. NEGUSE. Mr. Hickey, are you familiar with the report?

Mr. HICKEY. Same answer.

Mr. NEGUSE. All right. So just for the benefit, with unanimous consent, would ask that this report be submitted to the record, Mr. Chair.

Chairman NADLER. Without objection.

[The information follows:]

MR. NEGUSE FOR THE OFFICIAL RECORD

Graphika

The IRACopyPasta Campaign

Russian accounts posing
as Americans on
Instagram targeted both
sides of polarizing issues
ahead of the 2020 election

10.2019

By Camille François, Ben Nimmo,
C. Shawn Eib



Executive Summary

On October 21, 2019, Facebook announced the takedown of 50 Instagram accounts posting about US social and political issues and the 2020 election. Facebook concluded that the operation "originated from Russia" and "showed some links to the Internet Research Agency (IRA)", the Russian "troll farm" that previously targeted US audiences and the United States presidential election in 2016.¹

These accounts, all linked to the same operation, claimed to represent multiple politically active US communities: black activist groups, advocates speaking out against police violence, police supporters, LGBTQ groups, Christian conservatives, Muslims, environmentalists, gun-rights activists, southern Confederates, and supporters of Senator Bernie Sanders and President Donald Trump. A minority of posts focused directly on the 2020 election. Multiple accounts praised Bernie Sanders or Donald Trump. Accounts from both sides of the political spectrum attacked Joe Biden; some also attacked Kamala Harris and Elizabeth Warren. Almost half the accounts claimed to be based in "swing states," especially Florida.

This choice of targets and content echo the campaigns previously deployed by the IRA. Additionally, a few of the posts in this set reused or recreated IRA memes: this is why we named this campaign "IRACopyPasta". That these accounts reused and recreated IRA content is insufficient grounds on its own to provide a firm attribution, but it aligns with Facebook's own analysis that the operation showed some links to the IRA.

The operators went to great lengths to hide their origins, prioritizing operational security (OPSEC) over audience growth. Many of their posts consisted only of memes, without accompanying text. Posts that included text were usually sourced from viral posts made by American accounts. Facebook noted of this operation that it "had the hallmarks of a well-resourced operation that took consistent operational security steps to conceal their identity and location."

Most of these accounts had low numbers of followers: over half had fewer than 5,000 followers, and only one, focused on environmental issues, had over 20,000. The total number of posts for this operation was just under 75,000. The campaign appeared to be a recent creation, using purpose-made accounts rather than accounts compromised from real users. Some posts gained hundreds of likes but typically obtained orders of magnitude fewer than the American personalities they copied. The operation appears to have been active almost exclusively on

¹ See Indictment 1:18-cr-00032-DLF, "United States of America v. Internet Research Agency," U.S. Department of Justice, February 16, 2018, <https://www.justice.gov/file/1035477/download>

Instagram. Nevertheless, it made heavy use of Twitter by posting screenshots of tweets from genuine American users to Instagram.

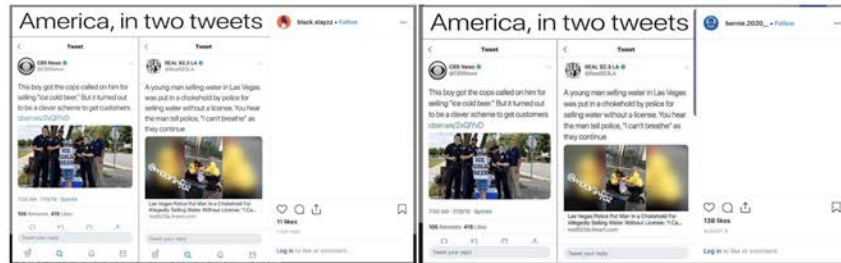
IRACopyPasta Assets: Posing as Americans, Posting on Divisive Issues

These accounts posed as supporters of specific US social or political groups:

- 11 Conservative accounts focused on praising President Donald Trump
- 9 “black activism” accounts, with a focus on police violence
- 4 liberal accounts, with a focus on praising Senator Bernie Sanders
- 3 Conservative accounts focused on gun rights
- 3 LGBTQ+ accounts
- 3 “feminist” accounts
- 2 “thin blue line” pro-police accounts
- 2 “Confederate” accounts
- 1 environmentalist account²
- 1 “Muslim” account
- 1 “Christian” account

The majority of posts by each account was not directly election related but focused on general news and political commentary. These posts were most likely used for persona development and branding. Multiple accounts in each subgroup repeatedly shared the same content over the space of a few hours or days, reinforcing the impression that they were part of a network.

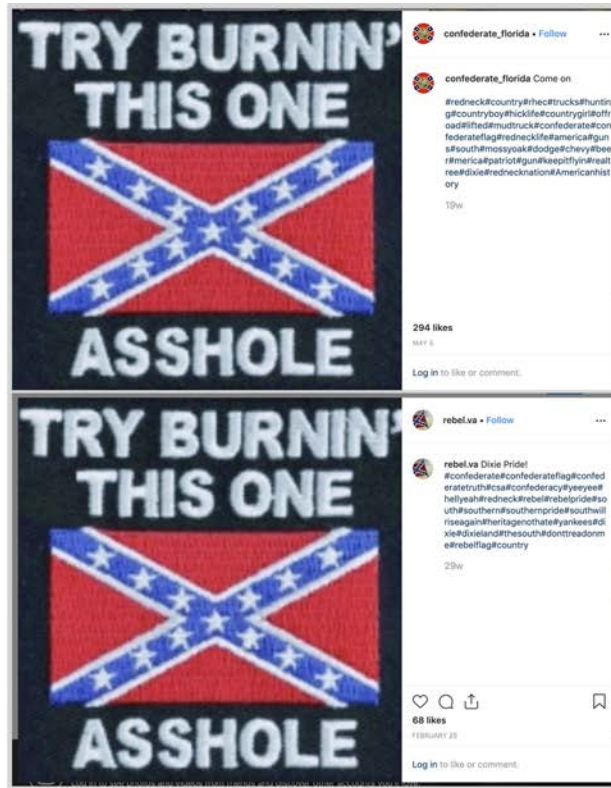
² The environmental focus here appears somewhat new, but reminiscent of a previous Russian operation uncovered on Instagram and Facebook and targeting French audiences. See: Ben Nimmo and Camille Francois, “#TrollTracker: Glimpse Into a French Operation” DFRLab, November 28, 2018, <https://medium.com/dfrlab/trolltracker-glimpse-into-a-french-operation-f78dcae78924>.



Posts by black.slayzz and bernie.2020_. Neither account posted text alongside the memes. All screenshots were taken in September 2019 unless indicated otherwise. Graphika has blanked the reactions of users not associated with the operation on all screenshots.



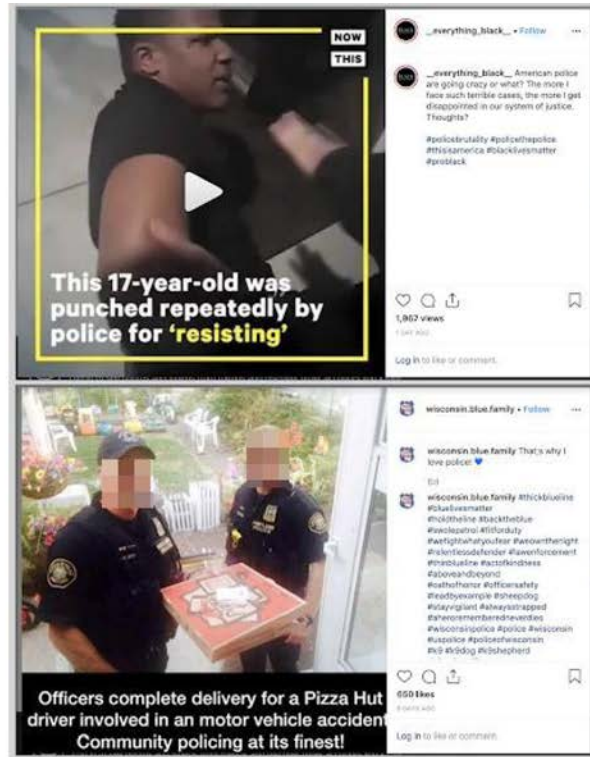
Posts by _everything_black_ and blacks_only_



Posts by *confederate_florida* and *rebel.va*, several weeks apart. Note the minimal use of language alongside the memes, other than hashtags.

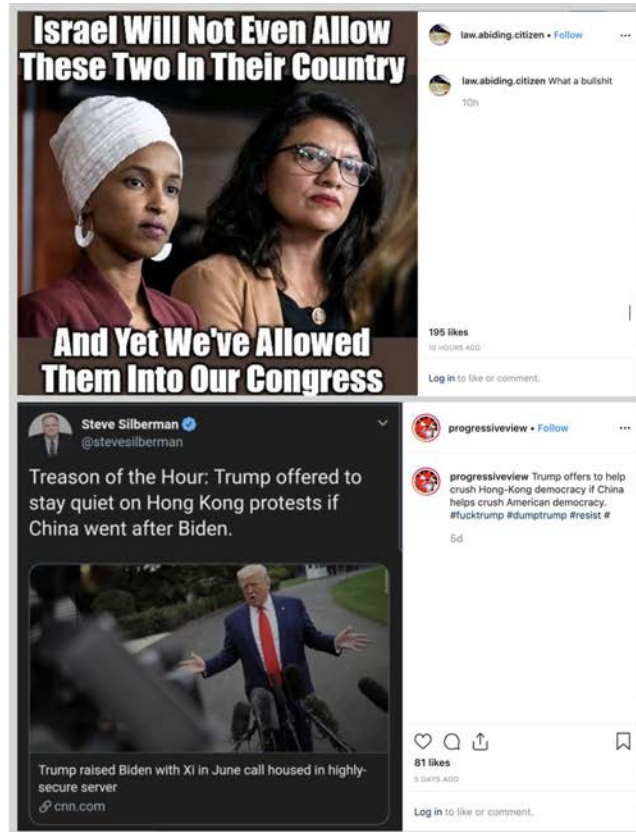
Divisive Content

Much of the content posted by these accounts was divisive and served to reinforce each target group's hostility toward other groups or individuals. Often, the sets of accounts posted on both sides of divisive issues. For instance, police violence was a topic addressed by accounts in the set, some of them posting with hashtags such as *#policebrutality* and *#blacklivesmatter* and others with *#bluelivesmatter* and *#backtheblue*.



Posts by *_everything_black_* and *wisconsin.blue.line* on the police.

Accounts across the “progressive” spectrum attacked President Donald Trump; accounts across the “conservative” spectrum attacked Democratic congresswomen Alexandria Ocasio Cortez (“AOC”) and Ihan Omar.



Posts by *law.abiding.citizen* (top) and *progressiveview* (bottom) on contemporary politics.

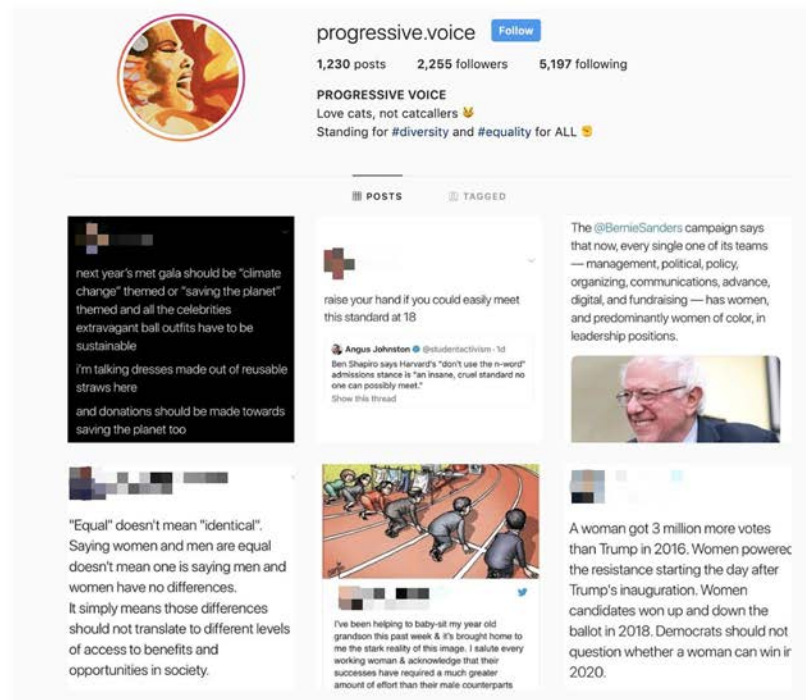
This practice of targeting both sides on divisive issues is characteristic of the campaigns initially conducted by the [IRA](#) to [target](#) American audiences in 2014-2018.³

³ See the US indictment of the IRA: Indictment 1:18-cr-00032-DLF, "United States vs. Internet Research Agency et al," US Department of Justice, February 16, 2018, <https://www.justice.gov/file/1035477/download>. See also Philip Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François. *The IRA, social media and political polarization in the United States, 2012-2018*. University of Oxford, 2018.

Leveraging Authentic Content from American Users

These accounts primarily reposted political content produced by American users on social media rather than creating their own. This is likely to have served two ends: it allowed the accounts to embed more firmly into their target audiences by sharing in-group content, and it reduced the amount of language they would have to produce, thereby reducing the scope for telltale language errors like the one shown in the screenshot above.

A high proportion of the content posted by these accounts were screenshots of tweets. These often featured an aspect ratio inappropriate for Instagram, reducing their visual impact. Despite a heavy use of Twitter content, the Instagram accounts in this operation did not have equivalent accounts on Twitter.



Profile page of *progressive.voice* shortly before the takedown: note how all its most recent posts were screenshots of tweets. The image also shows the followers to following ratio: the account had 2,255 followers but followed 5,197, suggesting an ongoing audience-building effort.

The “conservative” accounts in the set had a particular fondness for the conservative partisan group Turning Point USA, often sharing its memes and comments (a trait also observed in previous campaigns run by the Internet Research Agency). “Progressive” accounts in the set drew from a wider range of sources.



Meme watermarked "Turning Point USA" posted by ad0rable_depl0rable

Again, the selection of content appears to have been designed to push both sides of divisive issues and to inflame supporters and detractors of American political figures.



Posts attacking and defending AOC (or "OAC"). Top, *free.dom.choice*; bottom, *progressive.voice*. Note the numbers of likes. The original posts performed far better than these reproductions, perhaps because the operators looked for viral posts to copy from.

Election Messaging

Interspersed with these general audience-building and divisive posts, the accounts posted memes and comments about the 2020 elections. The overall alignment of these posts paralleled

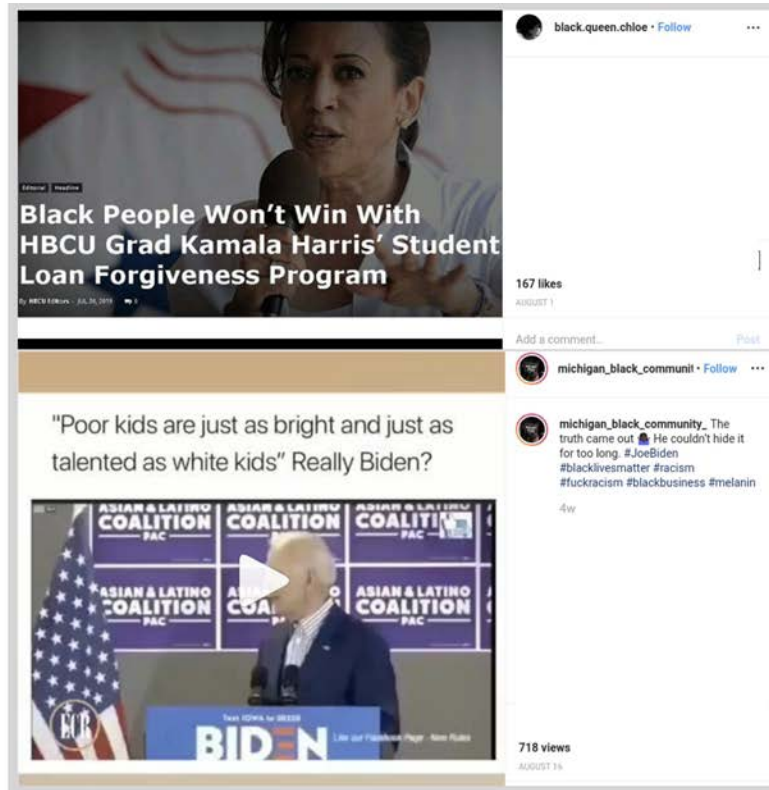
the IRA's [strategic messaging](#) in 2016,⁴ especially by expressing support for Donald Trump and Bernie Sanders, while attacking other presidential candidates.

Among the accounts focused on black activism, there was strong support for Bernie Sanders along with a moderate amount of content opposing Kamala Harris. Education reform and student debt relief were two of the most commonly mentioned reasons for supporting Sanders, while Harris's record as a California DA was mentioned as a reason to oppose her candidacy. Mixed in with these was a small amount of content attacking Joe Biden, primarily due to gaffes related to his previous handling of racial issues.



Post by support_black_fl on Bernie Sanders

⁴ Indictment 1:18-cr-00032-DLF, "United States vs. Internet Research Agency et al," US Department of Justice, February 16, 2018, para 43, <https://www.justice.gov/file/1035477/download>. See also Philip Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François. *The IRA, social media and political polarization in the United States, 2012-2018*. University of Oxford, 2018.



Posts by *black.queen.chloe* and *michigan_black_community_* on Harris and Biden. The Biden quote referenced a [remark](#) he made on August 9, 2019, a week before the post was published.⁵ The Harris comment referenced her [education](#) at the historically black HBCU.⁶

On the progressive side of the spectrum, considerably more accounts attacked Joe Biden. This contrasted starkly with IRACopyPasta's support for Sanders and is reminiscent of the original IRA's [strategy](#) of attacking Clinton while they supported Sanders.⁷ On the other side of the political

⁵ Stevens, Matt, "Joe Biden says 'poor kids' are just as bright as 'white kids'," New York Times, August 9, 2019, <https://www.nytimes.com/2019/08/09/us/politics/joe-biden-poor-kids.html>.

⁶ Ramirez, Stephanie, and Mitchell, Lacrai, "How Kamala Harris' education at a black college shaped her," CBS News, September 12, 2019, <https://www.cbsnews.com/news/how-kamala-harris-education-at-a-black-college-shaped-her/>.

⁷ Indictment 1:18-cr-00032-DLF, "United States vs. Internet Research Agency et al," US Department of Justice, February 16, 2018, para 43, <https://www.justice.gov/file/1035477/download>.

spectrum, the “conservative” accounts routinely praised and supported Trump and his family. They, too, focused their attacks on Biden.



Post explicitly contrasting Biden and Sanders, by bernie.2020_



Anti-Biden posts by law.abiding.citizen and free.dom.choice

Overall, election-related content made up a minority of IRACopyPasta's posts, but the accounts' geographical targeting also suggest a focus on electoral dynamics. Of the 40 accounts that Graphika reviewed, 19 gave a location in a state: Arizona (1), Colorado (2), Florida (5), Iowa (1), Michigan (3), Nevada (1), Ohio (3), Pennsylvania (1), Virginia (1), and Wisconsin (1). It is noteworthy that all of these have been reported online as "swing states" that will be critical in the 2020 presidential election. The focus on "purple" states, specifically Colorado, Florida, and Virginia, is also consistent with the instructions received by the IRA in July 2016 and their subsequent election targeting in the 2016 election, per the [Mueller IRA indictment](#).⁸

Recreating Content

The parallels between the IRACopyPasta campaign and previous campaigns attributed to the Internet Research Agency go beyond a similarity of targeted communities, tactics, and issues.

Memes originally posted by accounts attributed to the IRA's previous campaigns are reused (or recreated) throughout this set.⁹ The examples below illustrate this, with the IRACopyPasta account "wisconsin.blue.family" posting a meme watermarked to the original IRA account "Veterans US" and with the IRACopyPasta "rebel.va" account posting a meme watermarked to the original IRA account "South United."

⁸ Indictment 1:18-cr-00032-DLF, "United States vs. Internet Research Agency et al", U.S. Department of Justice, February 16, 2018, para 31, <https://www.justice.gov/file/1035477/download>

⁹ For more data points, see www.io-archive. The Information Operation Archive hosts publicly available and rigorously attributed data points from known Information Operations on social media platforms.



IRA watermarked meme posted by wisconsin.blue.family. Posts by "Veterans US" can be seen in the "UsHadrons" [archive](#).¹⁰

¹⁰

<https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-account-veterans-us-8c1beb0aa607>



Left, post by known IRA account "South United", from the [UsHadrons archive](#);¹¹ right, post by IRACopyPasta account *confederate_florida*

Sharing original IRA memes is a weak signal on its own: a number of spam operations are known to have done the same, since IRA memes have been preserved online in various archives.¹² On a handful of occasions, however, these assets went further: two ostensibly "Confederate" accounts, *rebel.va* and *confederate_florida*, posted memes that were almost identical to memes shared by known IRA account *South United*, but *recreated* them rather than simply *copying* them, taking steps to delete the original watermark.

Such memes featured the same background image and wording as the earlier IRA posts, but with a different font or layout, and without the *South United* watermark originally present when used by the IRA in previous campaigns. To make them, the operators must have found the original source photo and rebuilt the meme on it, a more labor-intensive process than a simple "copy-paste."

¹¹

<https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-south-united-35bcdca6f29>

¹² See for instance that of researcher "@USHadrons" on Twitter, available at <https://medium.com/@ushadrons>



Left, post by South United, watermarked, from the [US Hadrons archive](#).¹³ Right, post by confederate_florida without the watermark and in a different font, March 2019.

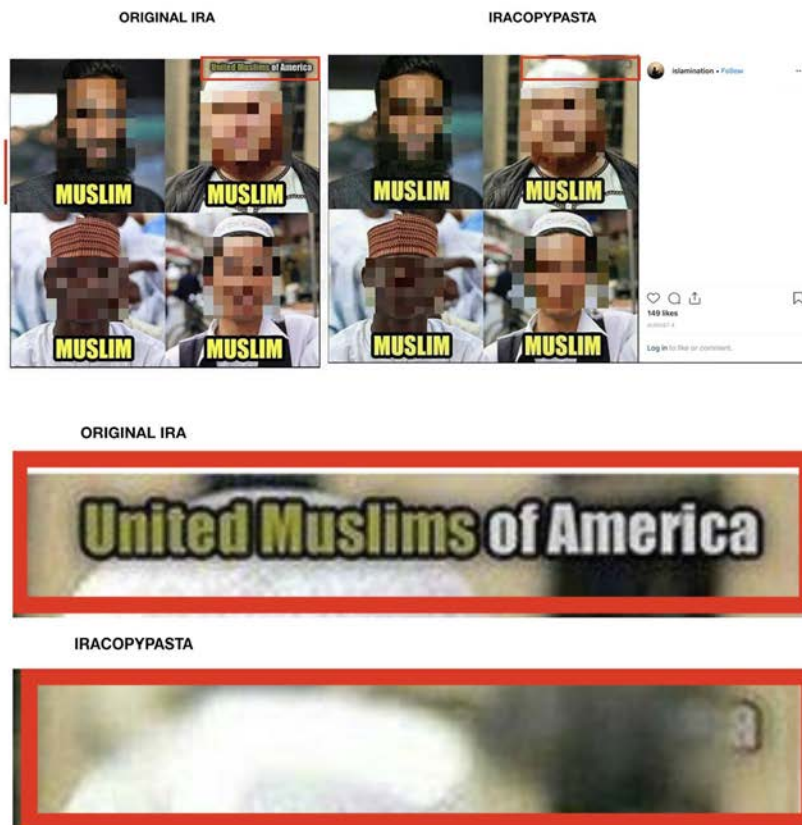


Left, post by South United, watermarked, from the [US Hadrons archive](#).¹⁴ Right, post by rebel.va without the watermark, September 2019. Graphika has blurred the faces of the individuals in the picture.

¹³ Ibid.

¹⁴ Ibid.

Yet another account, @islamination, posted a meme arguing that there is no racism in Islam. This was an IRA-watermarked meme from an account called [United Muslims of America](#),¹⁵ but the @islamination post blurred out the lettering almost completely, leaving the final -a in place.



Posts by "United Muslims of America" (top left) and @islamination (top right), together with detail boxes showing the placement of the original watermark and the blurred area with final -a in the recreated meme. Graphika has blurred the faces of the individuals in the picture.

¹⁵

<https://medium.com/@ushadrons/this-space-is-a-repository-for-ads-from-the-russian-social-media-group-united-muslims-of-america-b4d9b88dda65>.

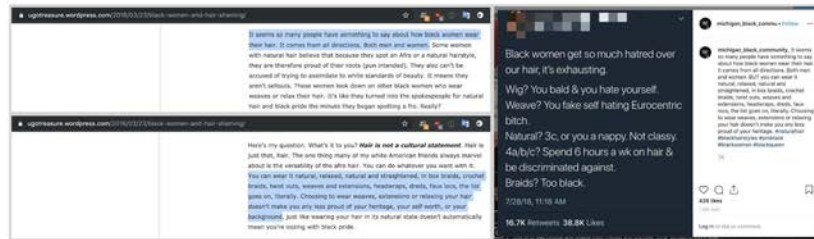
Throughout this investigation we identified almost 20 instances in which different accounts in the target set shared images and memes that had also been posted and watermarked by the IRA, but without the watermark. This represents only a tiny proportion of the total volume of content posted, but it nonetheless provides a clear indication that the operation was trying to repeat the IRA's performance, without looking like it was doing so.

Copy-Paste-Hide

The operation went to remarkable lengths to hide its presence and reduce its online footprint, perhaps at the expense of efforts that would have yielded higher engagement with the content posted.

The accounts posted very little in the way of linguistic content. Many posts consisted of nothing but a meme; others included a meme and a string of hashtags. Some had one or two sentences of colloquial text. Very few included more substantial passages. This may have been an attempt to reduce the volume of original language posted and therefore to reduce the risk of grammatical English errors betraying the operation's Russian origin.

A few accounts did post longer texts, but these were usually copy-pasted from other online sources. The copy-pasting was done with some care: often, posts would select paragraphs from separate sections of their sources and rearrange their order or omit large sections, rather than copying the entire text.



Left, blog post from 2016 on black hairstyles; right, post by michigan_black_community_



Mark II [edit]

The Mark II was the most common variant, with two million units produced. It was a much rougher weapon than the Mk I. The flash eliminator and the folding handle (the grip) of the Mk I were omitted. A removable barrel was now provided which projected 3 inches (76 mm) beyond the barrel sleeve. Also, a special catch allowed the magazine to be slid partly out of the magazine housing and the housing rotated 90 degrees counter-clockwise (from the operator's perspective), together covering the ejection opening and allowing the weapon and magazine both to lie flat on its side.

The barrel sleeve was shorter and rather than having small holes on the top, it had three sets of three holes equally spaced on the shroud. To allow a soldier to hold a Sten by the hot barrel sleeve with the supporting hand, an insulating lace-on leather sleeve guard was sometimes issued.^[16] Sten Mk II's in German possession were designated MP 749(s), the "s" signifying "singlisch". Some Mk IIs were fitted with a wooden stock as this part was desirable and interchangeable with the Mk V. Also, the Spz-kr assault rifle uses the receiver and components from the Sten Mk II.

Regular Mark II:

- Overall length: 762 mm (30.0 in)
- Barrel length: 197 mm (7.8 in)
- Weight: 3.2 kg (7.1 lb)

Mark II (Canadian) [edit]

During World War II a version of the Sten gun was produced at the Long Branch Arsenal in Long Branch, Ontario now part of Toronto, Ontario. This was very similar to the regular Mark II, with a different stock (skeleton type instead of strut type) and improved quality of manufacture. It was first used in



Top, post by gun.toting.tom on the STEN gun. Bottom, *the original* on Wikipedia.¹⁶ The Instagram post copied passages from the Wikipedia article verbatim, but in abridged form.

¹⁶ "STEN", Wikipedia, <https://en.wikipedia.org/wiki/Sten>.



Left, Facebook post on a genuine page. Right, the identical wording posted by IRACopyPasta asset gun.toting.tom. The text originally appeared in *"The Atlantic"* in 2018, written by David French.¹⁷ The woman in the photo was featured on a separate Facebook page belonging to a gun instructor in January 2019.

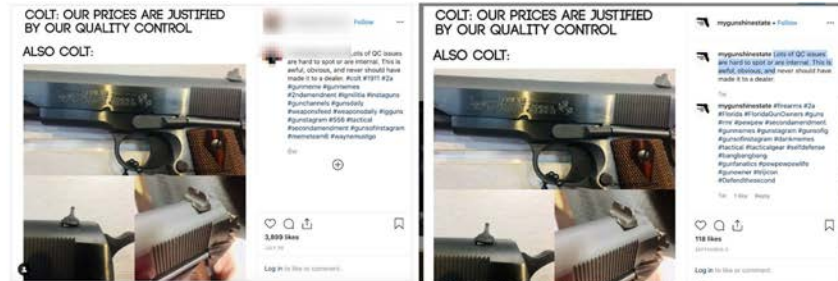
This plagiarism extended to political campaigns, especially that of Bernie Sanders. On a number of occasions, "progressive" accounts in the cluster copy-pasted both memes and comments originating directly from Sanders' own Instagram account.



Left, post by Bernie Sanders.¹⁸ Right, the same post by IRACopyPasta asset bernie.2020_. Note that the IRACopyPasta account gathered 105 likes, while Sanders' posts gathered over 65,000 likes.

¹⁷ French, David, "What critics don't understand about gun culture," *The Atlantic*, February 27, 2018, <https://www.theatlantic.com/politics/archive/2018/02/gun-culture/554351/>.

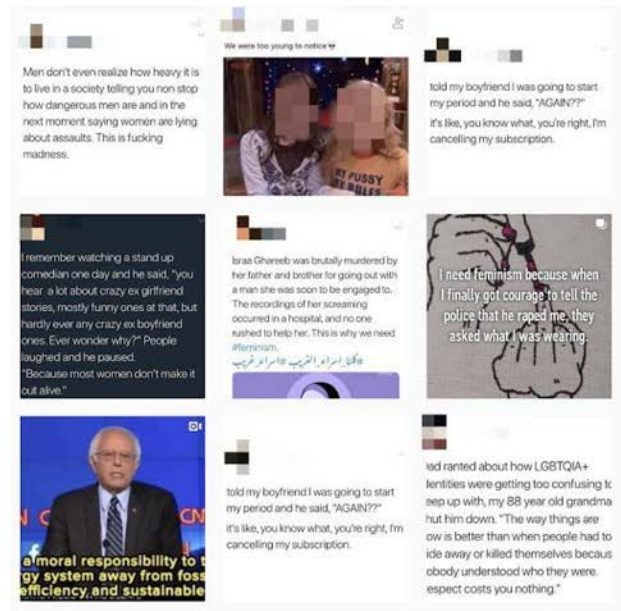
¹⁸ Post by Bernie Sanders' verified account, Instagram, August 25, 2019, <https://www.instagram.com/p/B1me35yhez4/>.



Left, post by a genuine guns-focused account¹⁹; right, the identical post from Florida-focused IRACopyPasta account mygunshinestate.

As noted earlier, the accounts also posted a high proportion of screenshot tweets, significantly more than in any other operation we previously analyzed.

¹⁹ Post by fromtheguncounter, Instagram, July 29, 2019, <https://www.instagram.com/p/B0ghqVJg0PA/>.



Posts by feminismdomination, from the account's profile page. Note that seven of the nine posts are screenshots of tweets.

This technique blurred the operation's fingerprint by reducing the scope for linguistic errors and maintaining a high stock of genuine American content appropriate to the political groups it targeted. However, it also gave each asset less of a discernible personality and therefore may have reduced the IRACopyPasta asset's ability to build audiences. It is not the first time that the platforms and researchers have exposed information operations that prioritized operational security over audience. The "Secondary Infektion"²⁰ operation that emanated from Russia went to extreme lengths to hide its traces, but as a result, almost none of its stories gained traction.

²⁰ DFRLab team, "Top Takes: Suspected Russian Intelligence Operation," DFRLab, June 22, 2019, <https://medium.com/dfrlab/top-takes-suspected-russian-intelligence-operation-39212367d2f0>.

Linguistic and Cultural Clues

Despite the lengths the operators went to to obscure their linguistic footprint, both texts and memes posted by the operation employed grammatical constructions and idioms uncharacteristic of speakers whose native language is American English.



"Do you also do same?" The correct idiom would end "do the same." Post by IRACopyPasta asset "myblackohioblog."



"What a bullshit": the idiom would be "what bullshit!" Post by IRACopyPasta asset *law.abiding.citizen*.



"What the future for their children will be?" Note the inaccurate word order. Post by IRACopyPasta asset *rebel.va*.



"What a poor logic that he has." Post by IRACopyPasta asset free.dom.choice.

In addition to odd linguistic constructions, this operation also echoed specific cultural references favored by the IRA in previous campaigns to target Southern Pride/pro-Confederate audiences. For instance, an abundance of content referenced the early-80's TV show "Dukes of Hazzard" (also previously frequently shared by the formerly active IRA account [South United](#)²¹) and showed an over-reliance on content borrowed from accounts and websites operated by the Redneck Nation network.

²¹

<https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-south-united-35bcdcaa6f29>.



"Dukes of Hazzard" Content from rebel.va (left) and confederate_florida (right);
Note the language on the left: more idiomatic would be, "don't you?"

The IRA Connection

Facebook attributed IRACopyPasta to operators "originating from Russia" who showed "some links" to the IRA.

Previous analyses of the IRA's campaigns targeting American audiences between 2014 and 2018 pointed to a set of issues and communities similar to those targeted by the IRACopyPasta campaign. "Socially divisive issues, such as race, immigration, and Second Amendment rights,"²² which were the focus of the IRA's previous campaigns, appear clearly throughout this set. The targeting, the language and content clues, and the recreation of original IRA content, all underscore the resemblance between the original IRA and IRACopyPasta.

If IRACopyPasta was, indeed, the work of the IRA or an affiliated group, they have continued evolving, placing an ever greater emphasis on remaining undetected. The high level of operational security throughout this campaign stands in sharp contrast to the various non-Russian clickbait and spam operators who have recycled known IRA content since 2017, blatantly, in high volume, and with no attempt at disguise.²³ The operation tried hard to hide, even at the expense of building its audience, and took the trouble to rebuild some of its earlier memes, rather than simply reusing them. Facebook concluded that the operation "had the hallmarks of a well-resourced operation that took consistent operational security steps to conceal their identity and location". The open-source evidence supports that conclusion.

²² "Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election," Vol. 2, available at: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

²³ See for instance the recently discussed and Ukraine-based "I Love America" Facebook page.

Appendix: List of Assets

Assets in this set are listed below. If you have been in touch with one of the accounts in this set, or have additional context to share, feel free to reach out at info@graphika.com

Username	Target Community Theme
__everything_black__	Black Activism
michigan_black_community_	Black Activism
support_black_fl	Black Activism
myblackohioblog	Black Activism
black.queen.chloe	Black Activism
blacks_only_	Black Activism
black.slayzz	Black Activism
alpha.union	Black Activism
blackenterprisemi	Black Activism
rebel.va	Confederate Southern heritage
confederate.florida	Confederate Southern heritage
protect.environment	Environmentalism
power_to_women_	Feminist
feminist_agenda_	Feminist
feminismdomination	Feminist
islamination	Muslim Islamic unity
lgbt_foxes	LGBTQ+
lgbt.florida	LGBTQ+
equality.state_	LGBTQ+
progressive.voice	Liberal
stop.trump2020	Liberal Anti-Trump
bernie.2020__	Liberal Pro-Bernie
progressiveview	Liberal Pro-Bernie
jesus.by.my.side	Religious Inspirational
gun.toting.tom	Conservative Gun rights
iowa.patriot	Conservative Gun rights
mygunshinestate	Conservative Gun rights

rightwing__memes	Conservative Pro-Trump
_conservative.minds	Conservative Pro-Trump
nofreeload	Conservative Pro-Trump
right_fl	Conservative Pro-Trump
law.abiding.citizen	Conservative Pro-Trump
ad0rable_depl0rable	Conservative Pro-Trump
freedom_first_1776	Conservative Pro-Trump
arizonan_american	Conservative Pro-Trump
ohio_conservative_	Conservative Pro-Trump
free.dom.choice	Conservative Pro-Trump
conservative.pa	Conservative Pro-Trump
nevada_blue_line	Thin blue line
wisconsin.blue.family	Thin blue line

Mr. NEGUSE. So, I would just quote from this, and then we will get to my question. On October 21, 2019, Facebook announced the takedown of 50 Instagram accounts posting about U.S. social and political issues in the 2020 election. Facebook concluded that the operation originated from Russia and showed “some links” to the Internet Research Agency, IRA, and the Russian troll farm that previously targeted U.S. audiences in the United States presidential election in 2016.

These accounts are attacking Kamala Harris, Elizabeth Warren. Almost half of the accounts claim to be based in swing States, especially Florida. What they are doing is not all that dissimilar from what they did before, focusing on divisive content.

Much of the content “posted by these accounts was divisive and served to reinforce each target group’s hostility toward other groups or individuals.” Often the sets of accounts posted on both sides of divisive issues. For instance, police violence was a topic addressed by accounts in the set, some of them posing with hashtags such as “police brutality” and “black lives matter” and other with, quote—or *#bluelivesmatter* and *#backtheblue*.

I know you are familiar with these accounts—I suspect, these kind of postings from before. Correct? Ms. Floris?

Ms. FLORIS. Yes, sir.

Mr. NEGUSE. All right. Mr. Hickey?

Mr. HICKEY. Yes, sir.

Mr. NEGUSE. So, the question I have. Clearly, our law enforcement agencies are working very hard to try to combat this disinformation, but it strikes me that the root cause, or at least one of the root causes, of the disinformation is the reality of anonymous accounts in these social media engines. There has been a lot of discussion as to whether or not universal verification, as opposed to having to constantly be reactive working with these social media companies like Facebook is the prime example, that instead, we could get at the root cause. It would eliminate so much of this disinformation and misinformation that is being perpetrated at the American public.

So, I would like to kind of get your sense, Ms. Floris and Mr. Hickey, as to whether or not that is something that your agencies, respectfully, have discussed internally and whether or not it is something you might recommend we take up as a matter of discussion on a policy basis.

Mr. HICKEY. So, sir, I will agree with you that the anonymity of the Internet generally poses a broad cybersecurity challenge. I don’t know I would say it is the number-one reason why we have so many challenges of security on the Internet with respect to foreign influence and others, but it is a leading one. How you address that, I think, is very tricky. How you have verification or authenticity in a way that you know who is emailing—is sending you a message is actually the person they claim to be.

At the moment, we are—I am not in a position to comment on legislation or propose it. What we are trying to do is where we see indications that someone isn’t who they claim to be, along the lines of what DAD Floris said, we will try to—and they tie to individuals that we are investigating, we will try to tip the providers to it so they can pierce behind that anonymization.

We are also currently prosecuting entities that we allege are tying to the Internet Research Agency in district court right now, which limits my ability to comment on it. But certainly, we are hoping to impose consequences for activity related to 2016.

Chairman NADLER. The gentleman's time has expired. The gentlelady from Georgia?

Mrs. MCBATH. Thank you, Mr. Chairman. Thank you so much for convening this hearing today.

Thank you, each and every one of you, for being here. Voting, I think all of us would agree, is just basically the foundation of our democracy, and protecting our ability to be able to vote and protecting our voting infrastructure from foreign interference is paramount.

In Georgia, where I represent, we have learned that before the 2016 election, a Russian agent visited the websites of Cobb and Fulton counties, counties that I represent, looking for vulnerabilities. While it appears that the agent didn't gain access to our election system in 2016, we continue to face attacks to this very day. Just last month, it was reported that two computers were stolen from both—stolen from Fulton County, there again, in my district. These computers contained very sensitive information that relates to every single voter in Georgia.

So, as we take on these threats I want to make sure that we are working to build a collaboration and transparency across the Federal Government, States, and for the American people.

I want to ask each of you about how we can increase this transparency while also improving election security. Mr. Hickey, I will start with you. I am curious about your thoughts on whether States should be treated differently than other victims that DOJ prosecutes, in terms of sharing victims' identities. For example, it was reported that the election systems in two Florida counties were breached, but the government has not identified which Florida counties were breached. On one hand, we want to encourage states to represent and to talk about these vulnerabilities, to report them, and sharing State-specific information publicly could discourage such reporting. On the other hand, we want the public to have confidence in our election system, and we want them to have confidence in the transparency of our election process.

So, indeed, you testified—and I am sorry that I was not here this morning, but I have your testimony—you testified, and I quote, "Exposure of foreign influence operations ultimately may be one of the best ways to counter them," end quote. So, can you speak how you think the Federal Government should navigate disclosing such victim information in the election security context?

Mr. HICKEY. Thank you, ma'am. I appreciate your nuanced treatment of that issue, because it does implicate a number of competing values. We do, as the vice chair of the Committee said, when she gave her opening statement, we want to encourage and guard the trust of the States so that they are willing to call the FBI and not worry that we are going to release their identities or the problem publicly.

Two, I think, core principles. One, we think it is a matter for State officials to decide when they disclose to their publics what the threats to their particular infrastructure have been. So, we will

leave it to Florida officials to communicate with the voters in that State, or any other State, hey, we worked with the FBI, we have remediated, we have done X, Y, and Z. We are going to leave it to that sovereign State.

The second key principle, I think, is that it is ultimately State-level officials who are politically accountable for certifying the results of an election. So, we are currently—the FBI is currently reviewing guidance on how to handle victim notification in the context of elections. It is not out yet, it is not finalized yet, but I anticipate that we will continue to notify system owners and operators, which may be local officials, but also providing a heads-up to the politically accountable chief State election official or board, so that they are aware of what the FBI is doing at a more local level.

Mrs. MCBATH. Thank you. Mr. Masterson and Ms. Floris, I would like to hear from each of you very briefly on your agency's transparency policies and whether more transparency is actually needed.

Mr. MASTERSON. So, I will speak to that very briefly. So, as I mentioned prior in the hearing, we have established communications protocols with the State and local election officials on how information will be reported, to empower them to speak to either activity targeting their systems or possible incidents. Then, most importantly, being transparent in sharing technical indicators broadly in an unclassified environment to the entire elections community about what threats are targeting election systems, so that they can not only take defensive measures but talk to their voters about the threat being real and the steps that they are taking to secure the process so that voters know that they are taking it seriously and responding.

I think this is where running elections at the State and local level really is critical. Voters have the ability to engage directly with those who run elections and have their questions answered. They can be poll workers. They can watch pre-election testing of the system. In many States they can watch post-election auditing. So, how can we empower those election officials with that information, whether about threat or activity, to talk directly to the voters and respond.

Ms. FLORIS. Thank you, ma'am, for your question. Just one thing I can add in addition to my colleagues on the panel. As I mentioned in the opening statement, when it comes to being transparent, one of the prongs of our strategy within FITF is to share intelligence and information as quickly as possible and to whoever needs to receive that information. Certainly, that is not a decision the FBI can make unilaterally. It involves all Members who are dabbling in the election security space, including individuals outside just the four Members on this panel. Rest assured, it is certainly one of our strategies to be as forward-leaning as we can in sharing actionable intelligence to the people who need to receive it.

Mrs. MCBATH. Thank you.

Chairman NADLER. The time of the gentlelady has expired. The gentlelady from Pennsylvania?

Ms. DEAN. Thank you, Mr. Chairman, and I want to sincerely thank all of you for being here and representing to us the important work you are doing to protect our elections. We take this very,

very seriously, and I can see that you do too. So, for the viewing public, we have the Department of Homeland Security. We have the FBI. We have the Department of Justice. We have U.S. Election Assistance Commission. You are so important on the front line, and we are here to partner with you.

I will start this question kind of quickly to Ms. Floris. On October 8th, just this month, 2019, the Senate Intelligence Committee published its second volume of its investigation on Russia's interference in the 2016 elections and the U.S. Government's response to that attack. The report concluded that in October of 2017, a counterintelligence division at FBI tasked an outside contractor to identify Russian influence activity on Twitter. As the report explains, that suggests, quote, "FBI either lacked resources or viewed the work in this vein as not warranting more institutionalized consideration."

Ms. Floris, the Senate committee's report is concerning. Do you believe you have enough resources at FBI to investigate and protect our elections?

Ms. FLORIS. Thank you, ma'am, for that question. As I have said, we can always use more resources, but that being said, we are throwing everything we have against the foreign influence threat. We have shifted resources to the Counterintelligence Division for that very purpose. We continue to engage with all 56 of our field offices to ensure that they are tracking the threat as closely as we are within the FITF.

Ms. DEAN. So, are you using—how often are you using outside contractors, or are you moving away from that, particularly in the issue of election security?

Ms. FLORIS. Ma'am, I can't speak specifically on the use of outside contractors within our workforce. We do have contractors throughout many parts of the FBI. I can't specifically as to how many are working on the foreign influence threat. I can certainly take that back.

Ms. DEAN. Yeah, we would love that information if you could share it with us. Can you tell us whether we have ever, or would ever use an outside contractor from, say, Russia, Iran, China, North Korea? Do you know?

Ms. FLORIS. Ma'am, I would defer that question to our Human Resources Division and our Security Division.

Ms. DEAN. Okay. We will follow up.

I would like to ask each of you the same thing. Do you have adequate resources at each of your departments and do you use outside contractors? I will start with Mr. Masterson.

Mr. MASTERSON. Thank you, ma'am. We have the resources we need to build on the success that we had in 2018 and continue to support State and local election officials. Certainly, with more resources comes greater capacity and responsiveness, the ability to increase support from the EI-ISAC or build on something like remote penetration testing. But we certainly have what we need to build on the success, and I defer you also to Human Resources and Security.

Ms. DEAN. Mr. Hovland?

Mr. HOVLAND. I would say that the Election Assistance Commission absolutely does not have the resources that we need. I would

also echo that the fiscal year 2018 \$380 million that went to the States, while that was a great first step it did not provide the States with the funding levels to solve all the challenges that they face. As I mentioned earlier, we have seen people prioritizing from a menu of options, but there are a number of things that State and local election officials could do, and additional funding is crucial to help them do that.

Ms. DEAN. We would love that information. Thank you for sharing that with us.

Mr. Hickey?

Mr. HICKEY. Ma'am, briefly, the 2020 budget would increase funding for the Counterintelligence Section, which I supervise, which would help our efforts to confront maligned foreign influence and national state-sponsored hacking.

I don't think we employ contractors specifically for this area of work, though, of course, we do have contractors working in the Justice Department, and they are vetted, and I will defer to others to explain how they are vetted.

I will say choosing contractors sometimes reflects our judgment. There are folks with particular technical expertise that we can bring on and use them in our, you know, foreign investment security reviews. We have contractors on board and use them because they have particular experience that we, as lawyers, do not have.

Ms. DEAN. Do you use any foreign contractors from, say, Russia, China, Iran?

Mr. HICKEY. What I do know is that we vet contractors, and they have to be screened for a security clearance. So, I can't speak to their nationalities but I know they would be vetted.

Ms. DEAN. Okay. What is concerning to us, or to me, is that the President's fiscal year 2020 budget proposal would cut funding to CISA, especially troubling since 2020 is the Presidential election year. Each of you, Robert Mueller, and many others have said the threat is persistent, pervasive, sweeping, systematic.

Maybe I will end on this question, real quickly. I wanted to follow up, Ms. Floris, that you talked about the disinformation. Could you be specific as to the disinformation that you were able—give us a concrete example of what it looked like? How were we disinformed? How were voters disinformed? Thank you, Mr. Chairman.

Ms. FLORIS. Ma'am, are you talking about leading into the 2016 election—

Ms. DEAN. Yes.

Ms. FLORIS. —or 2018 election? I can't speak in specifics about that right now, but I can certainly take that question back.

Ms. DEAN. Okay. Thank you very much. Thank you.

Chairman NADLER. The gentlelady yields back. The gentlelady from Texas.

Ms. ESCOBAR. Thank you, Mr. Chairman, and many thanks to our witnesses. I really appreciate your presence here today and your work.

I am still very concerned, and I think the American public should still be very concerned about our elections approaching in 2020. We know that three years ago Russia was wildly successful in attacking our democracy by attacking our elections, and despite the infor-

mation that we have and despite the unified voice from our intelligence community, we have a President who is cutting resources to our election security. It is stunning to me that the President of the United States would be willing to erode our election security instead of fighting to keep it safe.

Our voting machines are still outdated. Many of the vulnerabilities remain today. So, we should all be very concerned, and I hope that you all will continue your work to confront the obstacles ahead of you and to inform the American public.

With that said, we know that Special Counsel Mueller's indictment against several Russian entities noted that one of the ways that they interfered with our 2016 election was by encouraging minority voters not to participate in elections. In fact, the Pew Research Center found that in 2016, African American turnout dropped by 20 percent, despite the fact that we had record turnout in the country. The report detailed the complex strategies Russia used to target the African American community and to discourage African Americans from voting.

Starting with Mr. Masterson, for each one of you, please, what steps specifically are you taking to combat interference efforts to discourage minority groups from voting, and are those steps sufficient?

Mr. MASTERSON. Thank you for your question, ma'am. Our focus, in coordination with the FBI's Foreign Influence Task Force, is really on building resilience in the American people, talking to them about how they are being targeted with disinformation, where the source of information, the trusted source of information regarding the election process or otherwise would be.

So, we have created a variety of products and then are working with various communities and groups, so reaching out to groups like the NAACP, AARP, or others, to provide those resources to them, recognizing they are the trusted voice in that community that can talk to their Members about how they may be targeted with disinformation and how to respond.

Ms. FLORIS. Thank you, ma'am, for your question. I will just piggyback on that response, with this whole concept of media literacy with the American public. We cannot stress enough to every American city to understand when, how, where to vote. Your vote matters and it is up to you to have that media literacy to understand essentially truth in where you are obtaining your information.

On the more practice side of the house, again, I will hit on our engagement with social media companies and our willingness to engage with them to share threat indicators as it relates to disinformation, when we know that a foreign actor is trying to propagate disinformation using their platforms and continuing that dialogue and engagement with the social media companies as we roll into 2020.

Mr. HICKEY. DAD Floris referred to nefarious actors. Part of what the Justice Department does is help the FBI investigate those actors. So, we are often there to obtain legal process of various forms, to investigate what foreign actors are doing, and that information can be part of the information that ultimately is shared with the providers, to confront the disinformation you are suggesting.

Mr. HOVLAND. When the disinformation crosses over to talk about the election process or election Administration issues, like when you vote or how to register or how to participate, that would certainly be where it would fall into our interest area. In doing that we are really working with State and locals to encourage their voters or their citizens to participate, to be able to identify trusted sources of information, be able to check their voter registration to make sure it is updated and accurate, and those are—that is where our focus has been.

Ms. ESCOBAR. Ms. Floris, I have two follow-up questions for you.

Number one, you mentioned working with social media outlets on preventing the spread of disinformation. We sometimes have American candidates repeating disinformation provided by Russia, for example. Do you alert social media about that kind of disinformation that is coming from American candidates? That is number one.

Number two, what specific steps did you take, if any, to identify whether there were foreign efforts, similar to those used in 2016, to discourage minority voters, whether they were used again in 2018?

Ms. FLORIS. Thank you, ma'am, for your question. I will address your first question. The FBI cannot be the truth police. It is not our job to police content as to whether true or false information is being propagated. Again, we start with the foreign actors, that foreign aspect of what we do that is of investigative interest to the FBI. That is the information that we then provide to the social media providers, and it is really up to those providers to determine whether or not that content violates their own terms of service.

Regarding what steps we saw in 2018, if we saw the same activity that we saw in 2016, certainly not at the same level, and I really tout that to the success of the interagency collaboration, and again, our work with the social media companies.

Ms. ESCOBAR. Thank you. I yield back, Mr. Chairman.

Chairman NADLER. The gentlelady yields back. The gentleman from Georgia?

Mr. JOHNSON of Georgia. Thank you, Mr. Chairman, and thank you all for being here today.

In February of 2019, DOJ and DHS issued a joint statement concluding that there was, quote, “no evidence to date that any identified activities of a foreign government or agency had a material impact,” end quote, on the 2018 election. Now, Mr. Hickey and Mr. Masterson, your agencies reached this conclusion because the intelligence community didn’t detect a threat. Correct?

Mr. HICKEY. I think that is more or less right. The EO, which is what the report was issued under, sets forth a two-step process—the IC, including the FBI, gather reports, and then we evaluate the materiality of any impact.

Mr. JOHNSON of Georgia. I understand, but the intelligence community did not detect a threat, and that is why you issued your proclamation that no evidence to date was that any identified activities of a foreign government had a material impact on the election.

State and local officials also did not detect a threat. Isn’t that correct?

Mr. HICKEY. Well, so I think the IC did gather a report of actions that had the intent and purpose of interfering. So, when you say threat, threat means, to us, intent and purpose. State election officials—

Mr. JOHNSON of Georgia. They didn't detect a successful threat.

Mr. HICKEY. That is my understanding.

Mr. JOHNSON of Georgia. Okay. All right. Thank you.

Now you concluded also that Albert sensors did not detect a threat. Correct?

Mr. MASTERSON. So, Albert sensors regularly, across the country, regularly detect possible malicious activity against election infrastructure.

Mr. JOHNSON of Georgia. None was detected for 2018.

Mr. MASTERSON. I am not aware of any foreign adversary interfering or gaining access to election infrastructure in 2018.

Mr. JOHNSON of Georgia. Now isn't it possible that an attacker could have accessed and changed voter databases without being detected in 2018? Isn't it possible? Yes or no.

Mr. MASTERSON. So, we have no information to suggest that occurred.

Mr. JOHNSON of Georgia. All right. Fair enough. Now Mr. Hovland, your testimony was that 8,000 local jurisdictions conduct elections. Many of those local jurisdictions used direct recording electronic voting machines, also known as touch-screen electronic voting machines, in the 2016 presidential elections and in the 2018 presidential elections. In investigating election interference after the 2016 presidential election, how many of the tens of thousands of direct recording electronic voting machines used in that election were subjected to a forensic audit by any Federal agency?

Mr. HOVLAND. I am not aware of forensic audits that were performed.

Mr. JOHNSON of Georgia. What about any other type of testing or analysis on any direct recording electronic voting machines used in the 2018 elections?

Mr. HOVLAND. I would say that as far as the Election Assistance Commission goes, that—

Mr. JOHNSON of Georgia. Are you aware of any Federal agencies that have conducted any analysis of direct recording electronic voting machines used in the 2018 or 2016 elections?

Mr. HICKEY. So, we haven't been asked, and I don't think it is our role to audit election systems. The States certify the accuracy of the votes.

Mr. JOHNSON of Georgia. I understand. My question is just simply having the Federal Government use its resources to look at or conduct a forensic audit of any voting machines, any direct recording voting machines, either in 2016 or 2018. It appears that the answer is no. Would anybody disagree with that?

Mr. HICKEY. To the best of my knowledge that is correct. We have not been asked to second-guess the State certification of accuracy.

Mr. JOHNSON of Georgia. Okay. I am concerned about the 2020 election, especially considering the insecurity of our voting machines that has come to light in the past three years, and I would like to hear from the representative agencies the response plan

should our elections be successfully hacked in 2020. What would be the Federal response to a successful hacking in 2020?

Chairman NADLER. The gentleman's time has expired. The witnesses may answer the question.

Mr. MASTERSON. Thank you, sir. I will keep it short. DHS stands prepared to offer a number of incident response services, including deployment of teams to the locality or State, depending on the impacted infrastructure, in order to conduct analysis and work to mitigate the impacts of a possible cyber intrusion on election infrastructure. In addition, we have numerous analysis capabilities remotely that we can provide to help determine if there is, in fact, an intrusion, and the best way to mitigate it.

Ms. FLORIS. Sir, the FBI would work certainly in concert with CISA if there were an intrusion detected. We would use all our investigative might to ensure that we can determine attribution and potentially bring about criminal charges, if need be.

Mr. HICKEY. Obviously we try to prevent it. If we got indications that a State were being targeted, we would try to help them batten down the hatches before an intrusion was successful.

Mr. HOVLAND. I would say, on a positive note, that both with the fiscal year 2018 \$380 million and other resources that the number of paperless machines that are left out there has decreased substantially, and over 90 percent of Americans will be voting with some type of paper audit trail.

Mr. JOHNSON of Georgia. Thank you.

Chairman NADLER. The gentleman's time has expired. The gentlelady from Florida.

Ms. MUCARSEL-POWELL. Thank you, Mr. Chairman. Thank you for coming here this morning to such an important hearing.

It has been confirmed, and we have talked about this several times today, that all the main intelligence agencies confirmed that Russia interfered in the 2016 elections in a sweeping and systematic fashion, and it wasn't just a single attempt. We have heard from several witnesses in prior hearings that they are actually engaging in interference currently, as we speak.

So, I want to ask this, and I think Chairman may have asked this previously, but I want to get an answer from each and every one of you. Do you think it is appropriate for a sitting President, or any elected official, for that matter, to ask a foreign government to interfere in our elections?

Mr. HOVLAND. No.

Mr. HICKEY. I don't like the word "appropriate," ma'am, but I will say that we would urge anyone who has indications of such interference to come to the FBI and work with us so we can investigate criminal violations.

Ms. FLORIS. I would echo what my DOJ colleague said. We are certainly interested in any criminal activity as it relates to foreign influence.

Mr. MASTERSON. No.

Ms. MUCARSEL-POWELL. Thank you. During the 2016 hacking, Florida, my home state, was hacked and singled out by the Russian government. They targeted voter registration systems and they were able to successfully hack into at least the systems of two dif-

ferent counties. We actually got a security briefing from the FBI and others on that issue.

So, one of the things that I asked during that briefing is if they could say with certainty that hackers didn't manipulate the data, and I was told that they actually could not, that you could not say with certainty that these hackers did not manipulate the data. Can you confirm that again with me today, please?

Mr. HICKEY. I wasn't at the closed briefing, and I don't know what touches on classified or unclassified information. What I do know is we have said we have no indication to believe that there was any material impact on the ability to vote or the counting or tabulation of votes. I believe to be correct.

Ms. MUCARSEL-POWELL. I asked specifically about the data. That is why I think that they answered that. Ms. Floris?

Ms. FLORIS. I would just echo what my DOJ colleague said, ma'am. I certainly was not at the closed hearing, but I have no reason to doubt what was briefed to you during that time.

Ms. MUCARSEL-POWELL. Thank you. I know that there is a group now in DHS working with Federal, State, and local officials to secure our elections. It is called the Election Infrastructure Subsector Government Coordinating Council. The council is working to improve security protocols and works with local and State election officials so they can respond to threats quickly.

So, Mr. Masterson and Mr. Hovland, is Florida part of that council?

Mr. MASTERSON. Yes. Florida actually has two local representative that are on the Government Coordinating Council, and work with us.

Ms. MUCARSEL-POWELL. Can you just very briefly describe the progress of that group?

Mr. MASTERSON. Absolutely. The growth and engagement of the Government Coordinating Council since its establishment in 2018 has been great. We have 24 State and local Members that represent a vast array of the community. So, they represent secretaries of state, State election directors, local election officials from across the country. The purpose of that group is to inform CISA's approach to helping them secure elections. So, what is their view of risk, what services support and information sharing would be help them manage that risk, and how do we grow that trusted relationship so that they feel comfortable sharing back with us.

Ms. MUCARSEL-POWELL. Thank you. I am going to move on now to a different topic here. Mr. Masterson, on May 1st, 2019, Director Krebs testified that the President still had not received a briefing on Russia interference in the 2020 elections. Yes or no? Are you aware of DHS briefing the President on Russian interference in the 2020 elections?

Mr. MASTERSON. I am not aware but that doesn't mean it didn't happen. I am operational so that is above my level. I will say we engage regularly in coordination with the NSC across the whole of government on this election security work.

Ms. MUCARSEL-POWELL. Do you know if your agency has tried to meet with the President on election security?

Mr. MASTERSON. I don't know but that doesn't mean it hasn't happened.

Ms. MUCARSEL-POWELL. Do you think it would be important for the President to understand the threat picture facing the 2020 elections before he allocates resources to agencies on election security?

Mr. MASTERSON. I think the work we have done across the NSC has provided the information and work that we have done to coordinate that, and so I assume that is part of the NSC's coordination with us.

Ms. MUCARSEL-POWELL. Okay. Thank you. The same question, Ms. Floris and Mr. Hickey. How many times has your agency met with the President to discuss election security?

Ms. FLORIS. Thank you for the question, ma'am. I can't answer that specifically. Again, that doesn't mean that it has not happened. I just don't know personally.

Mr. HICKEY. Same answer, ma'am.

Ms. MUCARSEL-POWELL. Okay. Do you think it would be important, though, for your agencies to discuss election security with the President?

Mr. HICKEY. I think it is important for the President to understand the national security threats facing the country, yes.

Ms. MUCARSEL-POWELL. Ms. Floris?

Ms. FLORIS. I think it is important for everyone to understand the national security threats facing the country, especially as it relates to election security.

Ms. MUCARSEL-POWELL. Thank you so much.

Chairman NADLER. The gentlelady yields back.

This concludes today's hearing. We thank all our witnesses for participating. Without objection, all Members will have five legislative days to submit additional written questions for the witnesses or additional materials for the record.

Again, we thank everyone. Without objection, the hearing is adjourned.

[Whereupon, at 12:39 p.m., the Committee was adjourned.]

APPENDIX

QUESTIONS FOR THE RECORD - DHS
 SECURING AMERICA'S ELECTIONS PART II:
 OVERSIGHT OF GOVERNMENT AGENCIES
 HEARING DATE: OCTOBER 22, 2019

I. Chairman Jerrold Nadler

1. During the hearing, Congresswoman Mucarsel-Powell asked whether each agency had briefed the President on Russian interference in the 2020 elections. As of May 1st, 2019, Director Krebs testified that the President still had not received a briefing on Russia interference in the 2020 elections. Each agency testified that they were “not aware” of such a briefing.

- **Question for FBI, DOJ, DHS and EAC:** *Can each of you confirm whether your Department has met with the President on election security and if so, how many times in the last year and if no, whether your Department has tried to schedule a meeting and been turned down?*

2. An October 2018 report provided to the Senate Intelligence Committee by social media analytics firm Graphika indicates that Russian disinformation efforts may be focused on gathering information and data points in support of an active measures campaign targeted at the 2020 U.S. presidential election.

- **Question for DHS:** *What specifically is DHS doing to alert campaigns of these issues and to prevent attacks?*

3. Mr. Masterson, you have extensive experience in election and cyber security. Yet, you testified last June that election infrastructure still sees quote: “the same vulnerabilities you see across the IT sector, managing software updates as well as general upgrades that need to take place to help with resiliency.”

- **Question for DHS:** *What is preventing you from enacting these changes? What is DHS doing to work to ensure that these software updates are occurring in each state system?*

4. As you all are aware, 97% of states and territories use vendors in some capacity. Three vendors control over 90% of this process; of those three, over 60 percent of American voters cast ballots on systems owned and operated by a single vendor. Despite the impact of vendors, there is no real regulation over vendors to ensure election security. As a result, we’ve seen serious issues with vendor security. H.R. 1 includes regulations on vendors, such that DHS and EAC could be able to complete supply chain security and other qualification mandates on vendors.

- **Question for FBI, DOJ, DHS and EAC:** *Do you think such regulation over vendors would be helpful? Given that H.R. 1 has not passed, what else is each of your agencies doing to ensure that vendors are not undermining election security?*
5. In June 2017, Jeanette Manfra testified that DHS was engaging with quote “many vendors of [voting machine] systems to look into conducting some joint forensics.”
- **Question for DHS:** *Which vendors you have worked with since June 2017 to conduct those forensics on machines and what specific tests have been conducted?*
6. The intelligence community has been universal in confirming the gravity of the threat to our elections. Indeed, Director of National Intelligence Daniel R. Coats testified last summer, along with the heads of the CIA, FBI, NSA, and DIA, that the United States is quote, “under attack.” FBI Director Christopher Wray elaborated, “make no mistake: the threat just keeps escalating and we’re going to have to up our game to stay ahead of it.”
- **Question for FBI, DOJ, DHS and EAC:** *I’d like to hear from each witness: do you agree that there are serious threats facing our 2020 elections, yes or no?*
 - **Question for FBI, DOJ, DHS and EAC:** *If you received additional resources for your respective organizations to secure our elections, what would be the most pressing need for the additional funds?*
7. In 2018, the White House eliminated the cybersecurity coordinator position on the National Security Council.
- **Question for DHS:** *How has the absence of a cybersecurity coordinator at the National Security Council affected the Department’s ability to coordinate its election security activity strategically and effectively across the interagency?*
8. Director Krebs of DHS’s Cybersecurity and Infrastructure Security Agency, testified in May that he does **not** have 100% confidence that hacking will not take place in our electronic voting systems and, accordingly, that “auditability is a key tenet of cybersecurity.” He also testified that DHS is “working with [the Election Assistance Commission] to incentivize auditability.”
- **Question for DHS:** *As of today, do all states have a system in place to ensure auditability of their elections? If no, how many do not and can you provide a list of the states that do not?*

9. According to a recent report by the Brennan Center, an estimated 27.5 million voters cast ballots on paperless machines in 2016. As states take step to improve election auditability, this number is estimated to decrease to 16 million in 2020. But this is still a very high number – keep in mind that the margin of victory in presidential elections has ranged from about 3-9 million since 1988, so 16 million votes without an auditable paper trail is a huge deal.

- **Question for DHS:** *If DHS believes audits are so essential, what specifically is DHS doing to ensure such end-to-end verifiability or post-election audits? What needs to happen to make sure every vote can be audited?*

10. In response to QFRs for your testimony last year, Mr. Masterson testified that in February of last year, DHS, DNI, and the FBI gathered all state chief election officials at an intelligence community facility and provided one-time read-ins in a classified threat briefing.

- **Question for DHS:** *Is there a plan to hold similar briefings leading up the 2020 elections and why or why not?*

11. The Senate Intelligence Committee's report published October 8 concludes, and I'm quoting: Increased transparency is another critical priority if the United States is to defend itself against foreign influence campaigns. A dear lesson from 2016 is that the U.S. public needs information about influence campaigns prior to the election itself. That includes information about U.S. adversaries' attempts to undermine some candidates while assisting others. In 2016, the specific intent of the Russians was not made public during the election. . . . Between now and the 2020 election, the Intelligence Community must find ways to keep the U.S. public informed not only of individual influence operations, but the Community's assessment of the goals and intent of Russia and other foreign adversaries."

- **Question for FBI, DOJ, DHS and EAC:** *Can each of you describe your protocols for sharing threat information with the public on election day or leading up to the elections?*
- **Question for FBI, DOJ, DHS and EAC:** *Canada created the "Critical Election Incident Public Protocol," a series of steps to notify political parties and the wider public about foreign interference in elections in real time. Can each of you describe your thoughts on this process and whether the U.S. should adopt a comparable one?*

12. There were concerns in 2016 that North Carolina voter equipment was purchased by a firm targeted by Russian hackers. During the election, electronic poll books in Durham

County – which allow poll workers to check in registered voters – mistakenly showed many voters as having already voted, ultimately resulting in an emergency move to paper pollbooks and long lines. There has since been concerns about whether malfunction was in some way connected to a Russian attack.

- **Question for DHS:** *CNN reported that on June 5, 2019 DHS was planning to audit election equipment. Why did this investigation take so long and what is your organization doing to ensure that any future concerns are immediately investigated?*

13. Director Krebs recently pointed out the increase in ransomware attacks on small municipalities around the country, with 10 in Texas alone in the last few months.

- **Question for FBI, DOJ and DHS:** *What are your agencies doing to preemptively deter and respond to these attacks? Are the actors being prosecuted?*

14. Six months after the 2016 attacks on our elections, the states wrote a letter to DHS stating that quote “nearly six months after the [critical infrastructure] designation and in spite of comments by DHS that they are rushing to establish election protections, no secretary of state is currently authorized to receive classified threat information that would help them to protect their election systems.”

- **Questions for DHS:** *How many Secretaries of State are authorized to receive classified threat information to protect their election systems? Mr. Masterson testified last year before the senate that DHS is sponsoring up to three election officials in each state for security clearances. How many states you have already cleared three officials?*

15. The Defending Digital Democracy Report wrote that, on pages 8-9: “disparities in cybersecurity resources and experience across jurisdictions creates vulnerabilities. Smaller jurisdictions with fewer resources may be seen as more vulnerable targets by adversaries. Our nationwide security survey of states and territories reinforced this, with the most frequent concern noted by election officials being insufficient resources to secure the process, especially in smaller counties.”

- **Question for FBI, DOJ, DHS and EAC:** *Are your organizations prioritizing protecting more vulnerable counties with less resources? What is the protocol for ensuring protection of these communities?*

16. During the hearing, Congresswoman Scanlon asked the FBI about an October 3, 2019 advisory the FBI, along with DHS, issued an advisory to State election officials that the Russian government would be using voter suppression tactics to interfere in the 2020

elections, and obviously, we are extremely concerned about that. Ms. Floris could not speak to the specifics of (1) when the FBI learned about these Russian tactics and (2) how long after the FBI learned of this threat states and local officials were notified.

- **Question for FBI and DHS:** *When did you learn of the threat issued in his advisory; when were states notified; and if there was a delay between, please state the basis for delaying reporting this information to the states.*

17. In 2018, your department's "Cybersecurity and Infrastructure Security Agency" or CISA set up a war room and invited state and local officials and private sector technology providers to participate and share information, which was a strong step forward.

- **Question for DHS:** *What is your organization doing to improve the real-time sharing of threat information in 2020?*

18. Intelligence communities have reported that "deep fake" technologies are a major threat going into 2020.

- **Question for FBI, DOJ and DHS:** *Are your organizations actively looking into preemptively identifying and holding accountable individuals who attempt to use deep fake technologies / create false videos? How specifically are you doing this?*
- **Question for FBI, DOJ and DHS:** *How are you working with news organizations to work against these threats?*

19. On November 18, 2018, Business News reported that China granted trademarks for Ivanka Trump to make voting machines.

- **Question for FBI, DOJ, DHS and EAC:** *Are these trademarks for machines in China or here? Do we accept voting machines in this country from foreign countries, particularly countries trying to attack us?*

20. The attack on our 2016 elections, including stealing thousands of documents from the DNC, DCCC, and the Clinton Campaign, underscore the importance of protecting our campaigns from attacks. Director Krebs has since emphasized the importance of protecting these campaigns, saying: "Shame on us if we're not ready this time around." During our hearing, you testified that you have "made contact with the Trump campaign."

- **Question for DHS:** *Can you please explain how many times you've met with them, what recommendations you provided, and whether they adopted those recommendations?*

II. Congresswoman Madeleine Dean

1. In March of 2018, Ms. Manfra testified that *many* vendors submit equipment through a voluntary compliance process run by DHS.
 - **Question for DHS:** *How many vendors exactly have submitted to this process and what percentage of their equipment has gone through that process? Have you reached out to vendors who have not voluntarily submitted to compliance tests to coordinate security? Why or why not?*
2. Like all technology in use, voting machines sold by vendors will require periodic updates and software patches.
 - **Question for DHS:** *What are the guidelines for updating these machines, are they manually updated to maintain an airgap, or are vendors given remote online access?*

III. Congressman Greg Stanton

1. There have been cuts to DHS funding. The White House has also disbanded the Commission on Election Integrity and the Cyber Coordinator—the roles of those groups are now within DHS. Yet, in February, the Daily Beast reported that according to three current and former DHS officials, quote: “two teams of federal officials assembled to fight foreign election interference are being dramatically downsized.” More specifically, one task force assembled to help defend our elections is now quote: “half the size it was two months ago” according to two DHS officials familiar with the task forces.
 - **Question for DHS:** *I understand that your director has confirmed that election security remains a priority for the Cyber Security and Infrastructure Security Agency (CISA). But I want you to answer very specifically: have teams dedicated to election security been cut, reduced or reorganized by this administration in the last year?*
 - **Question for DHS:** *DHS requested 20 new advisors to help in advance of the 2020 election cycle. Yes or no, do you feel you have the resources you need in the President’s new budget—which again cuts CISA’s budget—to protect our elections?*
2. The Senate Select Committee’s Intelligence Report concluded that the intelligence community is dependent on the states’ doing their own investigation in order to collect information on potential breaches.

- **Question for FBI, DOJ, DHS and EAC:** *What are your agencies doing to ensure that you can preemptively detect breaches, and ensure adequate investigation of breaches following any issues on election day?*

IV. Congresswoman Lucy McBath

1. Multiple witnesses testified that their agencies rely on information-sharing between local, state, and federal entities to effectively address threats.
 - **Question for FBI, DOJ, DHS and EAC:** *What are each of your agencies doing to ensure sufficient information-sharing from local and state jurisdictions to your agencies?*
 - **Question for FBI, DOJ, DHS and EAC:** *What obstacles, if any, have your agencies encountered in making sure that local and state entities are willing to quickly share threat information with your agencies?*

RESPONSES OF
ADAM S. HICKEY
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

TO QUESTIONS FOR THE RECORD
ARISING FROM A HEARING
BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

ENTITLED
“SECURING AMERICA’S ELECTIONS PART II:
OVERSIGHT OF GOVERNMENT AGENCIES”

OCTOBER 22, 2019

Questions Submitted by Chairman Nadler:

1. During the hearing, Congresswoman Mucarsel-Powell asked whether each agency had briefed the President on Russian interference in the 2020 elections. As of May 1st, 2019, Director Krebs testified that the President still had not received a briefing on Russia interference in the 2020 elections. Each agency testified that they were “not aware” of such a briefing.

Question for FBI, DOJ, DHS and EAC: *Can each of you confirm whether your Department has met with the President on election security and if so, how many times in the last year and if no, whether your Department has tried to schedule a meeting and been turned down?*

Response: Pursuant to longstanding Department and Executive Branch policies and practices, I am unable to comment on any White House communications.

2. As you all are aware, 97% of states and territories use vendors in some capacity. Three vendors control over 90% of this process; of those three, over 60 percent of American voters cast ballots on systems owned and operated by a single vendor. Despite the impact of vendors, there is no real regulation over vendors to ensure election security. As a result, we’ve seen serious issues with vendor security. H.R. 1 includes regulations on vendors, such that DHS and EAC could be able to complete supply chain security and other qualification mandates on vendors.

A - 1

SENSITIVE BUT UNCLASSIFIED

Question for FBI, DOJ, DHS and EAC: *Do you think such regulation over vendors would be helpful? Given that H.R. 1 has not passed, what else is each of your agencies doing to ensure that vendors are not undermining election security?*

Response: The Department supports efforts to enhance cybersecurity and supply chain security for election infrastructure. To that end, through the Federal Bureau of Investigation, we share indicators, warnings, and best practices with vendors and States alike, to assist them in protecting their networks and products. We also welcome any opportunity to work with Congress in exploring measures that would enhance election security, consistent with the appropriate role of the federal government.

3. **The intelligence community has been universal in confirming the gravity of the threat to our elections. Indeed, Director of National Intelligence Daniel R. Coats testified last summer, along with the heads of the CIA, FBI, NSA, and DIA, that the United States is quote, "under attack." FBI Director Christopher Wray elaborated, "make no mistake: the threat just keeps escalating and we're going to have to up our game to stay ahead of it."**

Question for FBI, DOJ, DHS and EAC: *I'd like to hear from each witness: do you agree that there are serious threats facing our 2020 elections, yes or no?*

Response: Yes. The Department agrees that there are serious threats facing our 2020 elections. Protecting our Nation's democratic processes, including our elections, is among the Department's top priorities, and malign foreign influence operations targeting those processes are among the most pressing threats our Nation faces.

Question for FBI, DOJ, DHS and EAC: *If you received additional resources for your respective organizations to secure our elections, what would be the most pressing need for the additional funds?*

Response: In recent years, the Department has sought (and Congress has appropriated) additional funds for positions in the National Security Division's Counterintelligence and Export Control Section ("CES"), which houses the attorneys who investigate foreign, state-sponsored computer intrusions and attacks (including those affecting election infrastructure) and malign foreign influence. We have requested those resources because of the growing threats in cyberspace as well as our increased efforts to enforce the Foreign Agents Registration Act ("FARA"), which helps protect the integrity of American democracy by combating covert foreign government influence in our political process.

The Department's commitment to transparency and enforcement of FARA has borne fruit:

- In 2018 alone, more than 20 individuals and entities were criminally charged with violations involving FARA. That is more than the total number of individuals and entities charged in the prior 50 years.
- Last year, the Division used its civil enforcement authority for the first time since 1991 to obtain a court order requiring RM Broadcasting to register as the agent of a Russian state-owned media enterprise.
- In 2019, the Department doubled the number of new registrants and new foreign principals registering annually as of 2016. Moreover, almost twice the number of individuals who work for registrants (known as “short-form registrants”) have registered, increasing transparency concerning the individuals (and not just the entities) engaged in foreign influence activities.
- The FARA Unit has increased the number of inspections of FARA registrants, to audit compliance with their record-keeping and reporting obligations, by over 30 percent, from an average of about 14 a year (from 2010 to 2018) to 20.

Similarly, the Department’s commitment to investigating and holding accountable foreign, state-sponsored hackers and those who engage in illegal, covert influence operations, has led to criminal charges exposing those operations and holding those individuals and entities accountable:

- In February and July 2018, the Department announced criminal charges related to Russian interference in the 2016 election. First, in *United States v. Internet Research Agency LLC et al.*, the Department charged 13 Russian nationals and three Russian companies for committing federal crimes while seeking to conduct “information warfare against the United States” by interfering in the United States political system. Second, in *United States v. Netyksho et al.*, the Department charged 12 Russian military intelligence officers for their role in a sustained effort to hack into the computer networks of the Democratic Congressional Campaign Committee, the Democratic National Committee, and the presidential campaign of Hillary Clinton, and to release that information on the internet under the names “DCLeaks” and “Guccifer 2.0” and through another entity.
- Also in July 2018, the Department arrested Russian national Maria Butina on charges of acting as an agent of the Russian Federation within the United States without prior notification to the Attorney General. From approximately 2015 to 2017, Butina acted as an agent of a Russian government official, under whose direction, she provided key information about Americans who were in a position to influence United States politics and took steps to establish an unofficial line of communication between Russia and these Americans. Butina later pleaded guilty, admitting that she took these actions for the benefit of the Russian Federation and without providing the required notifications to the Attorney General that she was in fact acting as an agent of the Russian Federation. She was sentenced to 18 months’ imprisonment and deported to Russia.
- In October 2018, the Department announced charges against seven Russian military intelligence officers in *United States v. Morenits et al.* for their role in an international hacking and related influence and disinformation operations targeted

U.S. and international audiences. Along with the criminal charges, the Department seized the websites that the conspiracy was using to publicize stolen data and related disinformation.

- In October 2018, the Department announced charges in *United States v. Khusyaynova* in relation to the Internet Research Agency's ("IRA") alleged conspiracy to interfere in the 2018 mid-term elections, which exposed the IRA's ongoing efforts to influence the U.S. electorate through social media.
- In September 2020, the Department announced charges in *United States v. Lifshits* against a Russian national who is alleged to have been a manager in the IRA-related Project Lakhta. Lifshits was charged for his alleged role in a conspiracy to use the stolen identities of real U.S. persons to open fraudulent accounts at banking and cryptocurrency exchanges, including to further the goal of disrupting the democratic process and spreading distrust towards candidates for political office and the political system in general.

In many of those cases, the actors were well-resourced and attempted to take advantage of the anonymity offered by the internet, including through fake accounts, proxy computers around the world, cryptocurrency networks, and other anonymizing efforts. Overcoming these investigative obstacles required significant expenditure of time and resources by trial attorneys of the Counterintelligence and Export Control Section ("CES") of the Department's National Security Division (at certain times requiring one hundred percent of CES's resources dedicated to cyber investigations).

4. **The Senate Intelligence Committee's report published October 8 concludes, and I'm quoting: Increased transparency is another critical priority if the United States is to defend itself against foreign influence campaigns. A dear lesson from 2016 is that the U.S. public needs information about influence campaigns prior to the election itself. That includes information about U.S. adversaries' attempts to undermine some candidates while assisting others. In 2016, the specific intent of the Russians was not made public during the election.... Between now and the 2020 election, the Intelligence Community must find ways to keep the U.S. public informed not only of individual influence operations, but the Community's assessment of the goals and intent of Russia and other foreign adversaries."**

Question for FBI, DOJ, DHS and EAC: *Can each of you describe your protocols for sharing threat information with the public on election day or leading up to the elections?*

Response: The Department has adopted a formal policy for evaluating whether to publicly disclose malign foreign influence activities, which is codified in the *Justice Manual*. See *Justice Manual* § 9-90.720 (Sept. 2018), available at <<https://www.justice.gov/jm/jm-9-90000-national-security#9-90.730>>. The policy recognizes that that in many circumstances, public exposure of foreign influence operations, and of foreign governments' goals and intent in conducting them, can be an

important means of countering the threat and rendering those operations less effective. It also recognizes, however, that in some circumstances (outside the contexts of criminal charges or notification to victims of computer intrusions), public exposure can be counterproductive or otherwise imprudent, for example, if such exposure may amplify an operation, re-victimize victims, or create undue public alarm, harm, or confusion. The policy provides relevant factors for consideration given the countervailing considerations, requires that partisan political considerations must play no role in efforts to disclose malign foreign influence activities, and also requires that such disclosures must not be made for the purpose of conferring any advantage or disadvantage on any political or social group. Under the policy, where a Department component is considering whether to alert the general public to a specific foreign influence operation, consultation with the National Security Division is required.

In addition, the Federal Government adopted an Executive Branch-wide framework to ensure that threat information about foreign interference related to elections is shared with the public (or on a nonpublic basis with targets or other affected entities) where necessary to protect U.S. national security. This framework contains guiding principles and relevant factors that are consistent with the Department's policy. For example, the decision to notify must be in service of the national security interests of the United States and our responsibility to protect the American people, including to secure the integrity of our elections, and partisan politics must not play any role in the decision to provide notifications. Moreover, notification decisions must consider whether providing notification will help deter foreign influence and protect the public, and will avoid amplifying foreign interference activity or re-victimizing the targets of such activity.

Question for FBI, DOJ, DHS and EAC: *Canada created the "Critical Election Incident Public Protocol," a series of steps to notify political parties and the wider public about foreign interference in elections in real time. Can each of you describe your thoughts on this process and whether the U.S. should adopt a comparable one?*

Response: The Department agrees that it is important to share information and policies with our allies and other likeminded countries that are also confronting malign foreign influence so that we can learn from each other on best practices for addressing this threat. Without commenting on any specific Canadian policy or practice, the Department can share that Canada is an important partner for us in confronting malign foreign influence.

As noted above, the Federal Government adopted its own process for determining whether to notify political parties, other targets, or the wider public about foreign interference in elections in real time. The Executive Branch-wide framework contains the guiding principles and relevant factors for determining whether to make a notification about foreign interference related to elections. It also establishes processes for making nonpublic notifications, including to political parties or other targets, and for making public notifications.

5. **Director Krebs recently pointed out the increase in ransomware attacks on small municipalities around the country, with 10 in Texas alone in the last few months.**

Question for FBI, DOJ and DHS: *What are your agencies doing to preemptively deter and respond to these attacks? Are the actors being prosecuted?*

Response: One of the Department's highest priorities is to deter, disrupt, and respond to malicious cyber activities, including ransomware attacks. FBI Cyber Division recently hosted a ransomware summit to bring together the private sector and State, local, U.S. and U.K. government partners who specialize in ransomware. This allowed attendees to better understand all equities and enhance working relationships. Cyber criminals use ransomware and other malware to infect infrastructure connected to the Internet. While this activity can degrade individual components of infrastructure, including election systems, such infections are often opportunistic rather than focused efforts to compromise election integrity.

Part of the Department's deterrence strategy is to demonstrate to the malicious cyber actors that we are able to hold them accountable for their activities (including, but not limited to, ransomware). For example, in 2018 we charged one North Korean individual (who remains a fugitive) for his role in a DPRK-sponsored criminal conspiracy that unleashed the "WannaCry" ransomware attack in May 2017. We have also filed charges in other, more common cases where ransomware activities were carried out by actors motivated by personal profit. For example:

- In April 2017, an indictment was returned charging a Russian national with offenses stemming from his operation of the Kelihos botnet, which he used to facilitate malicious cyber activities, including installing ransomware. He was arrested by Spanish authorities and extradited to the United States. He pleaded guilty in September 2018, and is awaiting sentencing.
- In December 2017, the Department unsealed a criminal complaint charging two Romanian nationals with a conspiracy to illegally access approximately 123 computers associated with District of Columbia Metropolitan Police Department ("MPD") surveillance cameras and to use those computers in connection with a scheme to distribute ransomware in January 2017. One of the defendants pleaded guilty and agreed to testify against her co-defendant, who is facing extradition to the United States.
- In November 2018, the Department unsealed an indictment charging two Iranian nationals with deploying a sophisticated strain of ransomware known as "SamSam," which infected over 200 victims across the United States and Canada, causing over \$30 million in losses. This indictment was the first of its kind.
- In December 2018, an indictment was returned charging two Iranian men with committing a sophisticated ransomware attack on the City of Atlanta in March 2018.

The Department has also charged persons who facilitate ransomware attacks, such as by laundering money derived from ransomware attacks. For example, in July 2017, DOJ announced the indictment of a Russian national and an organization he allegedly operated, BTC-e, for facilitating transactions for international cybercriminals, and for receiving the criminal proceeds of numerous malicious cyber activities, including ransomware attacks. In parallel with the Department's actions, a regulatory agency assessed a \$110 million civil money penalty against the organization for willfully violating U.S. anti-money laundering laws. In June 2018, a Washington state resident pleaded guilty to conspiracy to commit money laundering in connection with the spread of a particular type of ransomware commonly referred to as Reveton. In August 2018, he was sentenced to 18 months in prison.

Moreover, in recent years, the Department has also relied on a variety of other legal authorities, such as civil forfeiture orders and seizure warrants, to disrupt cybercriminal groups by seizing valuable assets such as computer servers and domain names, as well as profits derived from illegal activity, and to help victim computers neutralize their malware. For example, in 2014, the Department deployed a combination of criminal and civil tools to disrupt a highly sophisticated ransomware scheme called Cryptolocker, which had encrypted computer files on more than 260,000 computers. Similarly, in 2017, DOJ obtained civil and criminal court orders that authorized measures to neutralize the Kelihos botnet, which had facilitated installing ransomware and other malicious software on tens of thousands of computers.

The Department has not limited such technical disruption efforts to criminal cyber threats. For example, in May 2018, the Department announced a court-authorized action to disrupt an Advanced Persistent Threat ("APT") 28 botnet of hundreds of thousands of infected routers and network storage devices, known publicly as "VPNFilter." Later, in January 2019, the Department announced a court-authorized effort to map and disrupt a botnet, known as "Joanap," which was used by North Korean hackers.

Finally, the Department, including the FBI, has supported deterrence-by-denial efforts against ransomware. For example, the Department has engaged in extensive public outreach to educate potential ransomware victims about the steps they can take to avoid infection in the first place, or recover from ransomware infection without having to pay ransom by restoring their systems from secure offline backups. The Department also provides guidance documents aimed at informing State and local governments, as well as the private sector, about how to protect their networks from ransomware.

6. **Microsoft's Digital Crimes Unit actively tracks threat actors and has successfully executed court orders to disrupt and transfer control of internet domains a dozen times in the last two years, shutting down over 80 "fake" websites.**

Question for DOJ: *Does DOJ track similar websites? If so, what is the success rate for taking down such websites and if not, why is DOJ not prosecuting these websites in court?*

Response: The Department supports Microsoft’s efforts (and frequently coordinates with Microsoft to ensure those efforts are as effective as possible and do not compromise a criminal investigation or prosecution). The Department cannot prosecute the websites themselves, of course, but we seek to identify and prosecute the actors who are responsible for establishing or otherwise using such domains for criminal purposes, and we use legal process (such as court orders) to disrupt their infrastructure. In the national security context, three examples include: (i) a May 2018 disruption of the GRU’s “VPNFilter” botnet through the Department’s seizure of one of its command and control domains; (ii) an October 2018 seizure of the fancybear.net website, which the GRU utilized to publicize the private health information of approximately 250 athletes from almost 30 countries as part of a Russian malign influence campaign; and (iii) in January 2019, the Department infiltrated and mapped a North Korean hacker-operated botnet, known as “Joanap,” and worked with the private sector and international partners to identify and remediate the victim computers. We also have disrupted and transferred controls of domains in the non-state-actor criminal context as well.

7. **The Defending Digital Democracy Report wrote that, on pages 8-9: “disparities in cybersecurity resources and experience across jurisdictions creates vulnerabilities. Smaller jurisdictions with fewer resources may be seen as more vulnerable targets by adversaries. Our nationwide security survey of states and territories reinforced this, with the most frequent concern noted by election officials being insufficient resources to secure the process, especially in smaller counties.”**

Question for FBI, DOJ, DHS and EAC: *Are your organizations prioritizing protecting more vulnerable counties with less resources? What is the protocol for ensuring protection of these communities?*

Response: The Department recognizes the importance of protecting all jurisdictions from cyber and other threats to elections, including smaller jurisdictions with fewer resources.

On the front lines of our efforts to protect jurisdictions from cyber and other threats to elections are our 94 U.S. Attorney’s Offices. Each U.S. Attorney’s Office—no matter how small—has designated one specially trained prosecutor to serve as a National Security Cyber Specialist and one specially trained prosecutor to serve as a District Election Officer. The National Security Cyber Specialists hold a security clearance and receive specialized training in combatting national security cyber threats from experts in the Department’s Criminal and National Security Divisions and the FBI. These prosecutors then serve as the lead national security cyber prosecutors for their districts as

well as the primary points of contact for the Department on national security cyber matters in their districts. Similarly, the District Election Officers receive specialized training in voter protection and election-related crimes from experts in the Department's Civil Rights, Criminal, and National Security Divisions and the FBI, and they then serve as the lead election crimes prosecutors and primary points of contact for the Department on election matters in their districts. By ensuring that U.S. Attorney's Office has a National Security Cyber Specialist and a District Election Officer, the Department ensures that we have a prosecutor on the ground who can assist State and local governments in protecting their communities from cyber and other threats to elections.

In addition, at Main Justice in Washington, the Criminal and National Security Divisions have expert attorneys who are equipped to work on cyber and election crimes cases. These attorneys are closely connected with the U.S. Attorney's Offices throughout the country for purposes of all cyber and election crimes matters. For example, attorneys from the Criminal Division's Public Integrity Section are notified and available to provide assistance in all federal criminal matters involving federal or State campaign finance laws, federal patronage crimes, and corruption of the election process. Similarly, attorneys from the National Security Division are notified and available to provide assistance in all federal criminal matters affecting, involving, or relating to national security, including malicious cyber and foreign influence activities perpetrated by foreign governments, their agents, or their proxies. These attorneys can provide further resources and assistance with efforts to help protect State and local governments from cyber and other election threats, including in jurisdictions with fewer resources.

8. Intelligence communities have reported that "deep fake" technologies are a major threat going into 2020.

Question for FBI, DOJ and DHS: *Are your organizations actively looking into preemptively identifying and holding accountable individuals who attempt to use deep fake technologies / create false videos? How specifically are you doing this?*

Response: The Department recognizes that "deep fake" technologies raise challenging problems. "Deep fake" videos do not violate federal criminal law merely because they contain or depict misrepresentations; however the Department will seek to hold individuals accountable when they use "deep fake" videos to violate criminal law. More generally, the Department has asked the private sector to coordinate with law enforcement agencies on emerging technology and security issues, and to work cooperatively to address them. We need technology companies and social media platforms to develop practices that account for the ways their products may be misused, including through "deep fake" technologies, and we need government agencies to have the means to develop and implement investigative capabilities that keep up with enforcement challenges.

Question for FBI, DOJ and DHS: *How are you working with news organizations to work against these threats?*

Response: Creating and posting “deep fake” videos is not a federal crime unless it is associated with criminal conduct such as fraud, extortion, or other federal crimes. However, the FBI engages with a variety of partners to share information on new and emerging threats, including the threat presented by malicious use of technology that can produce “deep fake” media (e.g., video, audio, images, text). Specifically, the FBI engages with technology companies and social media platforms to exchange information regarding the threat from malicious use of “deep fake” technologies, methods for detection, authentication, and attribution, and ways the U.S. Government and private sector can work in parallel, complementary ways to address this threat.

9. **Three days before the November 6, 2018 midterm elections, the Department of Justice provided a list of recent and ongoing action it was taking to ensure election security.**

Question for DOJ: *What actions will be taken to ensure free and fair elections in 2020, including efforts through the Civil Rights Division, Criminal Division, National Security Division and FBI to assist state and local jurisdictions?*

Response: The Department works year-round to ensure free and fair elections for all Americans, including through efforts by the Civil Rights Division, the Criminal Division, the National Security Division, and the FBI to assist State and local jurisdictions ensuring that all qualified voters have the opportunity to cast their ballots and have their votes counted free of discrimination, intimidation, fraud, or foreign interference in the election process.

As part of those ongoing efforts, prosecutors in the U.S. Attorney’s Offices, as well as in the Civil Rights, Criminal, and National Security Divisions, will continue to enforce federal criminal statutes that help to ensure free and fair elections. The Civil Rights Division is responsible for ensuring compliance with the civil provisions of federal statutes that protect the right to vote, and with the criminal provisions of federal statutes prohibiting discriminatory interference with that right. The Criminal Division oversees the enforcement of federal laws that criminalize certain forms of election fraud and protect the integrity of the federal election process. The National Security Division oversees federal criminal matters affecting, involving, or relating to national security, including malicious cyber and foreign influence activities perpetrated by foreign governments, their agents, or their proxies. Moreover, the FBI will continue to identify, investigate, and disrupt federal election crimes and other threats to free and fair elections, including by assisting State and local election officials in protecting themselves against such threats.

The Department will also continue several specific initiatives to enhance our election security efforts. On the front lines of the Department's efforts to protect elections are our 94 U.S. Attorney's Offices and our 56 FBI Field Offices. To ensure that every U.S. Attorney's Office and FBI Field Office can assist the Department's election security efforts, each U.S. Attorney's Office has designated a senior prosecutor to serve as a District Election Officer in the respective district, and each FBI Field Office has designated a senior special agent to serve as an Election Crimes Coordinator. District Election Officers and Election Crimes Coordinators are responsible for overseeing potential election-crime matters in their districts, for coordinating with the Department's election-crime experts at Main Justice and FBI headquarters in Washington, D.C., and for serving as a point of contact for State and local election officials. In February 2020, experts from the Criminal Division's Public Integrity Section, along with experts from the Civil Rights Division, National Security Division, and FBI, taught an in-person, three-day-long voter protection and election crimes course to the District Election Officers and Election Crimes Coordinators. This course ensures that each U.S. Attorney's Office and each FBI Field Office is prepared for the Department's role in the 2020 election season and will enhance the Department's law enforcement response to ballot fraud, campaign finance offenses, national security, cyber, and civil rights violations that take place in connection with the election process. The course included a detailed discussion of the criminal and civil laws, procedures, and remedies related to voting rights, campaign finance, combatting foreign interference, and election crimes. Similarly, in October 2019 the National Security Division hosted its annual three-day National Security Cyber Specialists Conference, which brings together experts from the Department, United States Attorney's Offices, and the FBI to collaborate and share lessons-learned in investigating and disrupting state-sponsored cyber threats. During that training, audience members received a training module on "Federal Election Security," which provided guidance on the role of Department prosecutors in protecting our elections, as well as several multi-hour case studies from colleagues who had investigated and charged criminal cases relating to the 2016 general and 2018 mid-term elections.

On Election Day, November 3, 2020, the Department implemented a number of additional security awareness and monitoring measures with our U.S. Government, State, and local partners to ensure the securest possible settings for the election process. For example, the District Election Officers in U.S. Attorney's Offices and FBI special agents serving as Election Crime Coordinators in the FBI Field Offices were on duty while polls were open in their jurisdictions, including to receive inquiries from State or local election officials and to receive complaints from the public. Moreover, in Washington, D.C., the Department hosted an all-day Election Day Watch at the FBI's Strategic Information and Operations Center ("SIOC") at FBI headquarters. Several FBI components were co-located at SIOC, along with attorneys from the Criminal Division's Public Integrity Section and the National Security Division. The Department attorneys and FBI personnel at SIOC coordinated communications with the District Election Officers and Election Crimes Coordinators, and were available to provide expert guidance to the field. In addition, they coordinated with other Federal agencies working on protecting our

elections, including the Department of Homeland Security and the Intelligence Community. Further, the Civil Rights Division conducted monitoring in the field at polling places around the country. Civil Rights Division attorneys in Washington, D.C., were ready to receive election-related complaints relating to any of the federal statutes and to take appropriate action.

As in 2018, we provided the public with a list of recent and ongoing action we were taking to ensure election security before Election Day 2020.

10. **On November 18, 2018, Business News reported that China granted trademarks for Ivanka Trump to make voting machines.**

Question for FBI, DOJ, DHS and EAC: *Are these trademarks for machines in China or here? Do we accept voting machines in this country from foreign countries, particularly countries trying to attack us?*

The Department has no comment on the Business News report. The Department defers to the Election Assistance Commission and State authorities to discuss the choice of voting machines used in this country.

Questions Submitted by Representative Stanton:

1. **President Trump's son-in-law Jared Kushner called the election interference investigation quote: "way more harmful" than any possible interference. Kushner went on to say the extent of 2016 foreign interference amounted to quote: "a couple of Facebook ads" and characterized election security investigations as quote: "nonsense, to be honest."**

Question for FBI and DOJ: *As members of the intelligence community, was Russia's attack just a "couple of Facebook ads"?*

Response: Russian influence in the 2016 election was a serious national security matter.

Question for FBI and DOJ: *Do you think election security investigations are nonsense?*

Response: I am unfamiliar with the quote cited, but election security is one of the Department's top priorities.

2. **Three days before the November 6, 2018 midterm elections, the Department of Justice provided a list of recent and ongoing action it was taking to ensure election security.**

Question for DOJ: *Can the DOJ tell the Committee what actions it will be taking to ensure free and fair elections in 2020, including efforts through the Civil Rights Division, Criminal Division, National Security Division and FBI to assist state and local jurisdictions?*

Response: Please see the Department's answer to Chairman Nadler's Question 9.

3. **The DOJ and FBI are working to investigate and disrupt threats to our elections systems and alert potential victims and targets. On October 3rd, the FBI, along with DHS, issued an advisory to state election officials that the Russian government would use voter suppression tactics to interfere in the 2020 U.S. elections.**

Question for FBI and DOJ: *What was the basis for this advisory? Who was told about the advisory besides state election officials?*

Response: The product, titled "Russia May Try to Discourage Voter Turnout and Suppress[] Votes in 2020 US Election," highlighted potential tools and tactics that Russia *could* adopt to discourage voter turnout and suppress voting in 2020; it was written to alert federal, State, and local officials of *possible* Russian approaches. The product was based upon previous reporting about the tools and tactics the Russian government or other Russian actors or proxies have used in prior elections; it was not based on any specific new intelligence information about the 2020 U.S. elections and did not conclude that the Russian government "would" use voter suppression tactics in 2020.

4. **The Senate Select Committee's Intelligence Report concluded that the intelligence community is dependent on the states' doing their own investigation in order to collect information on potential breaches.**

Question for FBI, DOJ, DHS and EAC: *What are your agencies doing to ensure that you can preemptively detect breaches, and ensure adequate investigation of breaches following any issues on election day?*

Response: The Department, including the FBI, works closely with other departments and agencies, including the Department of Homeland Security and Intelligence Community partners, to help State and local governments secure election infrastructure from cyber-enabled foreign interference or other cyber threats. This work preceded Election Day, was in a heightened posture on Election Day, and will continue after Election Day.

First, an important part of this effort is the Department's proactive investigation of actors who have in the past engaged in such activities, or who have indicated an intent and

capability to do. Through such investigations, our goal is to obtain and share indicators and warnings of malicious cyber-enabled threats with State and local officials and with other network defenders before a breach or other incident. Second, on Election Day itself, the Department activated an Election Day Cyber Incident Command Center, staffed by subject-matter experts from multiple threat units within the FBI. It maintained the ability to quickly and effectively review cyber-related threat reporting, including from the Intelligence Community; to communicate with other Department personnel and other federal agencies; and to coordinate response actions. Third, in many cases, the Department depends on States, local governments, and other affected entities who own or operate election infrastructure to report malicious cyber activities against their infrastructure. The Department encourages these infrastructure owners and operators to report any suspicious activities to the FBI.

Following any cyber incident targeting election infrastructure, the Department, including the FBI, will rely on the investigative resources of prosecutors and agents, both at headquarters and in the field, who have received specialized training in investigating election-related crimes or computer intrusions and attacks. These prosecutors and agents would work hand-in-hand with State or local officials following any incidents. The Department would encourage the State or local officials to cooperate with the Department's investigation and would not leave the State or local officials on their own.

Questions Submitted by Representative McBath:

1. **Multiple witnesses testified that their agencies rely on information-sharing between local, state, and federal entities to effectively address threats.**

Question for FBI, DOJ, DHS and EAC: *What are each of your agencies doing to ensure sufficient information-sharing from local and state jurisdictions to your agencies?*

Response: On the front lines of our election security efforts are our 94 U.S. Attorney's Offices. We have ensured that each U.S. Attorney's Office designates a specially trained prosecutor to serve as a District Election Officer who can serve as the primary point of contact on the ground for the Department on election-crimes matters in their districts. These prosecutors facilitate information-sharing from local and State jurisdictions to the Department. We have also sent information to local and State jurisdictions about the Department's election security efforts in which we requested that they direct election-crime complaints to their local U.S. Attorney's Office or the local FBI Field Office.

Question for FBI, DOJ, DHS and EAC: *What obstacles, if any, have your agencies encountered in making sure that local and state entities are willing to quickly share threat information with your agencies?*

Response: The FBI encourages State and local election partners to report any suspicious cyber incidents to the FBI and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA"). We consistently encourage FBI field offices to develop robust working relationships with the broad landscape of relevant State and local partners in order to ensure threat information is shared, and if appropriate, actioned, in a timely manner.

The FBI is focused on investigating malicious cyber activity against election infrastructure—as it is with all threats to critical infrastructure. The FBI engages regularly with State and local partners and provides election officials the technical information they need to protect their systems. State and local officials work with the FBI because they trust that the FBI will protect and handle their information appropriately. The majority of technical information the FBI has been able to provide election officials was a direct result of self-reporting and cooperation with the FBI from election officials and vendors. By partnering with the FBI, these officials helped the nation combat our adversaries' activities.

QUESTIONS FOR THE RECORD - EAC
SECURING AMERICA'S ELECTIONS PART II:
OVERSIGHT OF GOVERNMENT AGENCIES
HEARING DATE: OCTOBER 22, 2019

I. Chairman Jerrold Nadler

1. During the hearing, Congresswoman Mucarsel-Powell asked whether each agency had briefed the President on Russian interference in the 2020 elections. As of May 1st, 2019, Director Krebs testified that the President still had not received a briefing on Russia interference in the 2020 elections. Each agency testified that they were “not aware” of such a briefing.
 - **Question for FBI, DOJ, DHS and EAC:** *Can each of you confirm whether your Department has met with the President on election security and if so, how many times in the last year and if no, whether your Department has tried to schedule a meeting and been turned down?*
2. As you all are aware, 97% of states and territories use vendors in some capacity. Three vendors control over 90% of this process; of those three, over 60 percent of American voters cast ballots on systems owned and operated by a single vendor. Despite the impact of vendors, there is no real regulation over vendors to ensure election security. As a result, we've seen serious issues with vendor security. H.R. 1 includes regulations on vendors, such that DHS and EAC could be able to complete supply chain security and other qualification mandates on vendors.
 - **Question for FBI, DOJ, DHS and EAC:** *Do you think such regulation over vendors would be helpful? Given that H.R. 1 has not passed, what else is each of your agencies doing to ensure that vendors are not undermining election security?*
3. The intelligence community has been universal in confirming the gravity of the threat to our elections. Indeed, Director of National Intelligence Daniel R. Coats testified last summer, along with the heads of the CIA, FBI, NSA, and DIA, that the United States is quote, “under attack.” FBI Director Christopher Wray elaborated, “make no mistake: the threat just keeps escalating and we're going to have to up our game to stay ahead of it.”
 - **Question for FBI, DOJ, DHS and EAC:** *I'd like to hear from each witness: do you agree that there are serious threats facing our 2020 elections, yes or no?*

- **Question for FBI, DOJ, DHS and EAC:** *If you received additional resources for your respective organizations to secure our elections, what would be the most pressing need for the additional funds?*
4. The Senate Intelligence Committee's report published October 8 concludes, and I'm quoting: Increased transparency is another critical priority if the United States is to defend itself against foreign influence campaigns. A dear lesson from 2016 is that the U.S. public needs information about influence campaigns prior to the election itself. That includes information about U.S. adversaries' attempts to undermine some candidates while assisting others. In 2016, the specific intent of the Russians was not made public during the election. . . . Between now and the 2020 election, the Intelligence Community must find ways to keep the U.S. public informed not only of individual influence operations, but the Community's assessment of the goals and intent of Russia and other foreign adversaries."
- **Question for FBI, DOJ, DHS and EAC:** *Can each of you describe your protocols for sharing threat information with the public on election day or leading up to the elections?*
 - **Question for FBI, DOJ, DHS and EAC:** *Canada created the "Critical Election Incident Public Protocol," a series of steps to notify political parties and the wider public about foreign interference in elections in real time. Can each of you describe your thoughts on this process and whether the U.S. should adopt a comparable one?*
5. The Defending Digital Democracy Report wrote that, on pages 8-9: "disparities in cybersecurity resources and experience across jurisdictions creates vulnerabilities. Smaller jurisdictions with fewer resources may be seen as more vulnerable targets by adversaries. Our nationwide security survey of states and territories reinforced this, with the most frequent concern noted by election officials being insufficient resources to secure the process, especially in smaller counties."
- **Question for FBI, DOJ, DHS and EAC:** *Are your organizations prioritizing protecting more vulnerable counties with less resources? What is the protocol for ensuring protection of these communities?*
6. The proposed federal Voluntary Voting System Guidelines (VVSG) do not include a ban on internet connectivity and wireless modems, despite over 55k public comments that were sent in urging the inclusion of a ban. In fact, EAC Chair Christy McCormick testified at a Senate Rules Oversight Committee hearing in response to a direct question that the VVSG *did* ban internet connectivity, only to correct herself that they do not.

- **Question for EAC:** *Can you please clarify whether the VVSG will be amended to ban internet connectivity and wireless modems and, if not, why you are not doing this despite the public support for such a ban?*
7. On November 18, 2018, Business News reported that China granted trademarks for Ivanka Trump to make voting machines.
- **Question for FBI, DOJ, DHS and EAC:** *Are these trademarks for machines in China or here? Do we accept voting machines in this country from foreign countries, particularly countries trying to attack us?*

II. Congressman Greg Stanton

1. The Senate Select Committee's Intelligence Report concluded that the intelligence community is dependent on the states doing their own investigation in order to collect information on potential breaches.
 - **Question for FBI, DOJ, DHS and EAC:** *What are your agencies doing to ensure that you can preemptively detect breaches, and ensure adequate investigation of breaches following any issues on election day?*
2. The proposed federal Voluntary Voting System Guidelines (VVSG) do not include a ban on internet connectivity and wireless modems, despite over 55 thousand public comments that were sent in urging the inclusion of a ban. In fact, EAC Chair Christy McCormick testified at a Senate Rules Oversight Committee hearing in response to a direct question that the VVSG *did* ban internet connectivity, only to correct herself that they do not.
 - **Question for EAC:** *Can you please clarify whether the VVSG will be amended to ban internet connectivity and wireless modems and, if not, why you are not doing this despite the public support for such a ban?*
3. The current guidelines used by EAC were certified under standards that were set in 2005—nearly 15 years old. Moreover, my understanding from our witnesses last month is that there is not a single election system that's ever been certified under these guidelines. Secretary of State Boockvar testified last month that she had to create her own minimum standards because the EAC's and federal standards are old, so most states do this. The press releases on your website seem to have different dates for when these guidelines concluded public comment, when they were voted on by a quorum of commissioners, and when they will be finalized.

- **Question for EAC:** *Can you please explain why the process has taken over 15 years and what you are doing to expedite the process so that states have the minimum standard guidelines they need on a national level to protect their state systems?*
4. During our testimony last month Mr. Burt, a representative from Microsoft, said that, quote: “We need the EAC to adopt new guidelines for certification quickly” because the “current ones . . . don’t adequately address security and they take too long and they’re too burdensome.” He went on to say that “one of the really critical things for all state and local election officials is we need to make it very easy to apply security updates. . . . We need to apply security updates quickly, expeditiously, without so much bureaucracy so that we can respond.”
- **Question for EAC:** *Why is there not more urgency to impose minimum standards? What are you doing to make sure that certification for security updates is faster and more efficient, in light of the evolving threat picture?*
 - **Question for EAC:** *What do you need to finish the guidelines and implement them as quickly as possible?*
5. The National Association of State Secretaries has suggested that EAC should delegate authority without a quorum so that requirements can be updated and the certification process can be expedited.
- **Question for EAC:** *Do you agree with the NASS’s recommendation? Why or why not?*

III. Congresswoman Lucy McBath

1. Multiple witnesses testified that their agencies rely on information-sharing between local, state, and federal entities to effectively address threats.
- **Question for FBI, DOJ, DHS and EAC:** *What are each of your agencies doing to ensure sufficient information-sharing from local and state jurisdictions to your agencies?*
 - **Question for FBI, DOJ, DHS and EAC:** *What obstacles, if any, have your agencies encountered in making sure that local and state entities are willing to quickly share threat information with your agencies?*
2. The Election Assistance Commission’s (EAC) report to Congress, “Election Administration and Voting Survey: 2018 Comprehensive Report” reports the number of

poll workers per polling location. Georgia was one of only seven states that did not provide this data in responding to the survey.

- **Question for EAC:** *What efforts does EAC take to ensure it collects complete data from state and local jurisdictions?*
- **Question for EAC:** *Has Georgia provided this data on previous Election Administration and Voting Surveys (EAVS)? If so, please provide this data for the past four EAVS.*

QUESTIONS FOR THE RECORD - FBI
SECURING AMERICA'S ELECTIONS PART II:
OVERSIGHT OF GOVERNMENT AGENCIES
HEARING DATE: OCTOBER 22, 2019

I. Chairman Jerrold Nadler

1. During the hearing, Congresswoman Mucarsel-Powell asked whether each agency had briefed the President on Russian interference in the 2020 elections. As of May 1st, 2019, Director Krebs testified that the President still had not received a briefing on Russia interference in the 2020 elections. Each agency testified that they were “not aware” of such a briefing.

- **Question for FBI, DOJ, DHS and EAC:** *Can each of you confirm whether your Department has met with the President on election security and if so, how many times in the last year and if no, whether your Department has tried to schedule a meeting and been turned down?*

2. An October 2018 report provided to the Senate Intelligence Committee by social media analytics firm Graphika indicates that Russian disinformation efforts may be focused on gathering information and data points in support of an active measures campaign targeted at the 2020 U.S. presidential election.

- **Question for FBI:** *What specifically is the FBI doing to investigate these actor measures campaigns?*

3. As you all are aware, 97% of states and territories use vendors in some capacity. Three vendors control over 90% of this process; of those three, over 60 percent of American voters cast ballots on systems owned and operated by a single vendor. Despite the impact of vendors, there is no real regulation over vendors to ensure election security. As a result, we've seen serious issues with vendor security. H.R. 1 includes regulations on vendors, such that DHS and EAC could be able to complete supply chain security and other qualification mandates on vendors.

- **Question for FBI, DOJ, DHS and EAC:** *Do you think such regulation over vendors would be helpful? Given that H.R. 1 has not passed, what else is each of your agencies doing to ensure that vendors are not undermining election security?*

4. The intelligence community has been universal in confirming the gravity of the threat to our elections. Indeed, Director of National Intelligence Daniel R. Coats testified last

summer, along with the heads of the CIA, FBI, NSA, and DIA, that the United States is quote, “under attack.” FBI Director Christopher Wray elaborated, “make no mistake: the threat just keeps escalating and we’re going to have to up our game to stay ahead of it.”

- **Question for FBI, DOJ, DHS and EAC:** *I’d like to hear from each witness: do you agree that there are serious threats facing our 2020 elections, yes or no?*
 - **Question for FBI, DOJ, DHS and EAC:** *If you received additional resources for your respective organizations to secure our elections, what would be the most pressing need for the additional funds?*
5. The Senate Intelligence Committee’s report published October 8 concludes, and I’m quoting: Increased transparency is another critical priority if the United States is to defend itself against foreign influence campaigns. A dear lesson from 2016 is that the U.S. public needs information about influence campaigns prior to the election itself. That includes information about U.S. adversaries’ attempts to undermine some candidates while assisting others. In 2016, the specific intent of the Russians was not made public during the election. . . . Between now and the 2020 election, the Intelligence Community must find ways to keep the U.S. public informed not only of individual influence operations, but the Community’s assessment of the goals and intent of Russia and other foreign adversaries.”
- **Question for FBI, DOJ, DHS and EAC:** *Can each of you describe your protocols for sharing threat information with the public on election day or leading up to the elections?*
 - **Question for FBI, DOJ, DHS and EAC:** *Canada created the “Critical Election Incident Public Protocol,” a series of steps to notify political parties and the wider public about foreign interference in elections in real time. Can each of you describe your thoughts on this process and whether the U.S. should adopt a comparable one?*
6. Director Krebs recently pointed out the increase in ransomware attacks on small municipalities around the country, with 10 in Texas alone in the last few months.
- **Question for FBI, DOJ and DHS:** *What are your agencies doing to preemptively deter and respond to these attacks? Are the actors being prosecuted?*
7. Congresswoman Dean asked the FBI about their use of outside vendors in election security. On October 8th, just this month, 2019, the Senate Intelligence Committee published its second volume of its investigation on Russia’s interference in the 2016

elections and the U.S. Government's response to that attack. The report concluded that in October of 2017, a counterintelligence division at FBI tasked an outside contractor to identify Russian influence activity on Twitter. As the report explains, that suggests, quote, "FBI either lacked resources or viewed the work in this vein as not warranting more institutionalized consideration." Ms. Floris testified that she would get back to the Committee on how many vendors are working on foreign influence of elections.

- **Question for FBI:** *Please provide a list of outside vendors working on election security and the process used to vet those vendors? Please note if any vendors originate in Russia, Iran, North Korea, or China.*

8. The Defending Digital Democracy Report wrote that, on pages 8-9: "disparities in cybersecurity resources and experience across jurisdictions creates vulnerabilities. Smaller jurisdictions with fewer resources may be seen as more vulnerable targets by adversaries. Our nationwide security survey of states and territories reinforced this, with the most frequent concern noted by election officials being insufficient resources to secure the process, especially in smaller counties."

- **Question for FBI, DOJ, DHS and EAC:** *Are your organizations prioritizing protecting more vulnerable counties with less resources? What is the protocol for ensuring protection of these communities?*

9. During the hearing, Congresswoman Garcia asked whether the FBI has created a task force to coordinate government and technology sector cooperation on election security to coordinate government and technology sector cooperation, as it did with violent extremist content online. The FBI testified that the FITF works on a "monthly basis" with companies, but would not confirm whether there is a separate task force on election security.

- **Question for FBI:** *Can you compare the resources used in the violent extremist content task force, to those in FITF? What measures were taken with violent extremist content not currently undertaken in the election security context?*

10. During the hearing, Congresswoman Scanlon asked the FBI about an October 3, 2019 advisory the FBI, along with DHS, issued an advisory to State election officials that the Russian government would be using voter suppression tactics to interfere in the 2020 elections, and obviously, we are extremely concerned about that. Ms. Floris could not speak to the specifics of (1) when the FBI learned about these Russian tactics and (2) how long after the FBI learned of this threat states and local officials were notified.

- **Question for FBI and DHS:** *When did you learn of the threat issued in his advisory; when were states notified; and if there was a delay between, please state the basis for delaying reporting this information to the states.*

11. Intelligence communities have reported that “deep fake” technologies are a major threat going into 2020.

- **Question for FBI, DOJ and DHS:** *Are your organizations actively looking into preemptively identifying and holding accountable individuals who attempt to use deep fake technologies / create false videos? How specifically are you doing this?*
- **Question for FBI, DOJ and DHS:** *How are you working with news organizations to work against these threats?*

12. On November 18, 2018, Business News reported that China granted trademarks for Ivanka Trump to make voting machines.

- **Question for FBI, DOJ, DHS and EAC:** *Are these trademarks for machines in China or here? Do we accept voting machines in this country from foreign countries, particularly countries trying to attack us?*

II. Congressman Greg Stanton

1. President Trump’s son-in-law Jared Kushner called the election interference investigation quote: “way more harmful” than any possible interference. Kushner went on to say the extent of 2016 foreign interference amounted to quote: “a couple of Facebook ads” and characterized election security investigations as quote: “nonsense, to be honest.”

- **Question for FBI and DOJ:** *As members of the intelligence community, was Russia’s attack just a “couple of Facebook ads”?*
- **Question for FBI and DOJ:** *Do you think election security investigations are nonsense?*

2. The DOJ and FBI are working to investigate and disrupt threats to our elections systems and alert potential victims and targets. On October 3rd, the FBI, along with DHS, issued an advisory to state election officials that the Russian government would use voter suppression tactics to interfere in the 2020 U.S. elections.

- **Question for FBI and DOJ:** *What was the basis for this advisory? Who was told about the advisory besides state election officials?*

3. The Senate Select Committee's Intelligence Report concluded that the intelligence community is dependent on the states' doing their own investigation in order to collect information on potential breaches.

- **Question for FBI, DOJ, DHS and EAC:** *What are your agencies doing to ensure that you can preemptively detect breaches, and ensure adequate investigation of breaches following any issues on election day?*

III. Congresswoman Lucy McBath

1. Multiple witnesses testified that their agencies rely on information-sharing between local, state, and federal entities to effectively address threats.

- **Question for FBI, DOJ, DHS and EAC:** *What are each of your agencies doing to ensure sufficient information-sharing from local and state jurisdictions to your agencies?*
- **Question for FBI, DOJ, DHS and EAC:** *What obstacles, if any, have your agencies encountered in making sure that local and state entities are willing to quickly share threat information with your agencies?*

Question#:	1
Topic:	Presidential Briefing
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: During the hearing, Congresswoman Mucarsel-Powell asked whether each agency had briefed the President on Russian interference in the 2020 elections. As of May 1st, 2019, Director Krebs testified that the President still had not received a briefing on Russia interference in the 2020 elections. Each agency testified that they were "not aware" of such a briefing.

Can each of you confirm whether your Department has met with the President on election security and if so, how many times in the last year and if no, whether your Department has tried to schedule a meeting and been turned down?

Response: The Cybersecurity and Infrastructure Security Agency (CISA) defers to the White House and the National Security Council for questions concerning internal deliberations with regard to intelligence and national security.

Question#:	2
Topic:	Alerting Campaigns
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: An October 2018 report provided to the Senate Intelligence Committee by social media analytics firm Graphika indicates that Russian disinformation efforts may be focused on gathering information and data points in support of an active measures campaign targeted at the 2020 U.S. presidential election.

What specifically is DHS doing to alert campaigns of these issues and to prevent attacks?

Response: One of CISA's priorities for the 2020 election cycle is to work closely with Presidential and congressional campaigns, highlighting our services and resources as well as providing threat landscapes to candidates and their staff. CISA has already provided threat briefings to all the Presidential campaigns registered with the Federal Election Commission (FEC). We are also actively working with individual Presidential and congressional campaigns in securing their systems, to include vulnerability assessments. In addition to our direct engagement with campaigns, CISA has developed a suite of resilience products to assist stakeholders in identifying foreign influence operations and provide simple steps that can be taken to avoid becoming part of a foreign influence campaign. One example of these products is the campaign security checklist, which includes a list of simple steps that can be taken to manage risk to campaign systems and personal devices. This checklist has been shared with campaigns.

Question#:	3
Topic:	Updating State Systems
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: Mr. Masterson, you have extensive experience in election and cyber security. Yet, you testified last June that election infrastructure still sees quote: "the same vulnerabilities you see across the IT sector, managing software updates as well as general upgrades that need to take place to help with resiliency."

Response: Promoting cyber hygiene is one of CISA's primary goals in stakeholder engagement with all public and private sector partners. To promote this goal, CISA works with state and local election officials and the private sector election community on a voluntary, collaborative basis. We are currently working with all 50 states and over 6,000 local election offices to provide information regarding risk, including threats to election infrastructure and possible mitigations. In addition, we provide services, at no cost, to help owners and operators of election infrastructure to identify the exact vulnerabilities described in my testimony. As we do with owners and operators of other critical infrastructure, CISA stands ready to help the election community to identify and mitigate any vulnerabilities with their infrastructure. However, the Federal government cannot force owners and operators to take action. In addition to the election-specific services, we provide training to state and local officials regarding IT management and security best practices. Also, we have performed national and state-level table-top exercises to illustrate the value of practices like patching, network segmentation, access controls, and incident response plans. In June 2019, CISA hosted the second "Tabletop the Vote" exercise with our federal partners, state and local election officials, and private sector vendors to review coordination protocols and incident response plans. The Tabletop covered a number of pre-, post- and day of election scenarios, including voter registration compromises, equipment issues, and misinformation distributed over news and social media. Participants included representatives from 47 states, thousands of local election officials, the District of Columbia, U.S. Virgin Islands, along with our Federal partners. The purpose was to help build a deeper understanding on threats to election infrastructure, the federal government's capabilities to support state and local officials and exercise response plans and information sharing capabilities.

Question: What is preventing you from enacting these changes? What is DHS doing to work to ensure that these software updates are occurring in each state system?

Response: In many cases our elections customers have identified a lack of resources and IT support as the primary reason for their inability to patch, replace systems, or mitigate identified vulnerabilities. DHS works closely with the Elections Assistance Commission to ensure that state and local governments are using the election grant funding provided by Congress in 2018, 2020, and in the most recent CARES Act.

Question#:	4
Topic:	Regulating Vendors
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: As you all are aware, 97% of states and territories use vendors in some capacity. Three vendors control over 90% of this process; of those three, over 60 percent of American voters cast ballots on systems owned and operated by a single vendor. Despite the impact of vendors, there is no real regulation over vendors to ensure election security. As a result, we've seen serious issues with vendor security. H.R. 1 includes regulations on vendors, such that DHS and EAC could be able to complete supply chain security and other qualification mandates on vendors.

Do you think such regulation over vendors would be helpful?

Response: Upon congressional request, DHS has provided feedback and advice on proposed legislation regarding this and other election security issues. We stand ready to work with Congress on these issues.

DHS offers free critical product evaluations to all election system vendors. These evaluations are open-ended vulnerability tests of elections systems provided by the vendors.

Question: Given that H.R. 1 has not passed, what else is each of your agencies doing to ensure that vendors are not undermining election security?

Response: We have been pleased with the level of engagement and enthusiasm the private sector election vendors have shown in this testing. DHS defers to the U.S Election Assistance Commission (EAC) regarding their voting system testing and certification program, which is a first of its kind federal testing program used by virtually every state and all major voting system manufacturers. In addition, DHS offers free critical product evaluations to all election system vendors. These evaluations are open-ended vulnerability tests of elections systems provided by the vendors. We have been pleased with the level of engagement and enthusiasm the private sector election vendors have shown in this testing.

Question#:	5
Topic:	Working with Vendors
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: In June 2017, Jeanette Manfra testified that DHS was engaging with quote "many vendors of [voting machine] systems to look into conducting some joint forensics."

Which vendors you have worked with since June 2017 to conduct those forensics on machines and what specific tests have been conducted?

Response: While CISA works closely with voting machine vendors to test vulnerabilities, we do not publicly identify who we are working with or what services they are requesting. CISA offers the same no-cost support and services to private sector election technology providers as we offer to state and local officials. This includes critical product evaluations (CPEs), which are open-ended vulnerability assessments of the system provided by the vendor. At this time, CISA has completed three election-specific CPEs. The CISA Cyber Assessments team, in concert with ESI election security consultants, is conducting outreach to the elections community, including briefing Secretaries of State and the Election Infrastructure Sector Coordinating Council (EISCC) on the CPE capability. CISA's CPE capability has received increased interest from the vendor community and CISA is aiming to complete additional CPEs by September 2020.

Question#:	6
Topic:	Election Threats
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: The intelligence community has been universal in confirming the gravity of the threat to our elections. Indeed, Director of National Intelligence Daniel R. Coats testified last summer, along with the heads of the CIA, FBI, NSA, and DIA, that the United States is quote, "under attack." FBI Director Christopher Wray elaborated, "make no mistake: the threat just keeps escalating and we're going to have to up our game to stay ahead of it."

I'd like to hear from each witness: do you agree that there are serious threats facing our 2020 elections, yes or no?

Response: Yes.

Question#:	7
Topic:	Pressing Needs
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: If you received additional resources for your respective organizations to secure our elections, what would be the most pressing need for the additional funds?

Response: The Fiscal Year (FY) 2020 Consolidated Appropriations Act (Public Law 116-93) provided \$43.5 million for election security and countering foreign influence efforts, which is \$19.5 million above the budget request to support State, local, tribal, and territorial governments. These additional resources allow for additional capability and scalability of our support to election stakeholders. The increased funding provided by Congress in FY 2020 will help support activities including:

- Election Infrastructure-Information Sharing and Analysis Center deployment of end point detection and alerting capabilities;
- Data Retention, Storage and Surge Capabilities and threat intelligence platform enhancements;
- Additional malicious domain activity blocking and reporting and malware analysis;
- Election Infrastructure Security Specific Agency funding to drive enhanced planning across the elections community

Question#:	8
Topic:	Cybersecurity Coordinator
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

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

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

Response: Election security is a whole of government effort and CISA is the leading federal agency for election infrastructure security. We work closely with all our federal partners to provide state and local election officials the information they need to secure elections. The White House and NSC are providing DHS all the necessary support and resources to go out and accomplish this mission.

Question#:	9
Topic:	Election Auditability
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: Director Krebs of DHS's Cybersecurity and Infrastructure Security Agency, testified in May that he does not have 100% confidence that hacking will not take place in our electronic voting systems and, accordingly, that "auditability is a key tenet of cybersecurity." He also testified that DHS is "working with [the Election Assistance Commission] to incentivize auditability."

As of today, do all states have a system in place to ensure auditability of their elections? If no, how many do not and can you provide a list of the states that do not?

Response: The trend across the country is to replace outdated and unauditable voting systems with those systems that produce an auditable record. This includes the announcement from the two largest voting system vendors in the U.S. announcing that they will no longer sell unauditable direct recording device voting systems. One of CISA's top priorities is to encourage and incentivize efficient and effective auditability of election results. In November 2019, CISA announced that it is working with election officials and their private sector partners to develop and pilot an open source post-election auditing tool ahead of the 2020 elections. The tool is being created by VotingWorks, a non-partisan, non-profit organization dedicated to building secure election technology. CISA's investment is designed to support election officials and their private sector partners who are working to improve post-election auditing in the 2020 election and beyond. The auditing tool, known as Arlo, is open source software provided free for state and local election officials and their private sector partners to use. The first version of Arlo is already supporting pilot post-election audits across the country, including several from the 2019 elections.

We defer to the EAC on the number of states that do not have an auditable system in place for all election jurisdictions.

Question: According to a recent report by the Brennan Center, an estimated 27.5 million voters cast ballots on paperless machines in 2016. As states take step to improve election auditability, this number is estimated to decrease to 16 million in 2020. But this is still a very high number - keep in mind that the margin of victory in presidential elections has ranged from about 3-9 million since 1988, so 16 million votes without an auditable paper trail is a huge deal.

Response: Auditability is a core tenet of information security. The ability to audit systems, processes and procedures allows IT professionals to better understand risk, the current integrity of their systems and steps they can take to improve resilience across their infrastructure. In elections auditability necessarily includes the principle of software independence. Put simply,

Question#:	9
Topic:	Election Auditability
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

software independence simply means that an undetected change or error in a systems software cannot cause an undetectable change or error in an election outcome.

Question: If DHS believes audits are so essential, what specifically is DHS doing to ensure such end-to-end verifiability or post-election audits? What needs to happen to make sure every vote can be audited?

Response: One of CISA's top priorities is to encourage and incentivize efficient and effective auditability of election results. In November 2019, CISA announced that it is working with election officials and their private sector partners to develop and pilot an open source post-election auditing tool ahead of the 2020 elections. The tool was created by VotingWorks, a non-partisan, non-profit organization dedicated to building secure election technology. CISA's investment is designed to support election officials and their private sector partners who are working to improve post-election auditing in the 2020 election and beyond. The auditing tool, known as Arlo, is open source software provided free for state and local election officials and their private sector partners to use. The first version of Arlo is already supporting pilot post-election audits across the country, including several from the 2019 elections.

Question#:	10
Topic:	Threat Briefing
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: In response to QFRs for your testimony last year, Mr. Masterson testified that in February of last year, DHS, DNI, and the FBI gathered all state chief election officials at an intelligence community facility and provided one-time read-ins in a classified threat briefing.

Is there a plan to hold similar briefings leading up the 2020 elections and why or why not?

Response: In 2018 and 2019, CISA and our partners in the Intelligence Community provided one-time read-in classified threat briefings to state election officials. CISA will consider the practicality of providing another briefing to all state election officials closer to the 2020 election. In addition, through 2018 and 2020 CISA, in coordination with our colleagues at DHS Intelligence and Analysis and the intelligence community, provided a number of secret level briefings through secure video teleconferences.

CISA remains committed to sharing timely and actionable intelligence as broadly as possible across the election community. Our goal is to always push to have information declassified and pushed across the community broadly. When that is not possible, we push to have the intelligence downgraded and shared with the broadest section of the election community. In addition to these briefings, CISA has worked with private sector partners to provide unclassified threat intelligence briefings to state and local officials. These briefings have focused on adversary tactics and techniques, activity targeting elections in other countries and possible mitigations. Also, CISA, through the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), frequently shares threat information with state and local officials. We have all 50 states and the territories as members of the ISAC, as well as over 2,500 local election officials. The EI-ISAC helps ensure that actionable and timely information is reaching the field so that state and local officials can take the steps they need to manage risk to their systems.

Question#:	11
Topic:	Sharing with the Public
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: The Senate Intelligence Committee's report published October 8 concludes, and I'm quoting: Increased transparency is another critical priority if the United States is to defend itself against foreign influence campaigns. A dear lesson from 2016 is that the U.S. public needs information about influence campaigns prior to the election itself. That includes information about U.S. adversaries' attempts to undermine some candidates while assisting others. In 2016, the specific intent of the Russians was not made public during the election. . . . Between now and the 2020 election, the Intelligence Community must find ways to keep the U.S. public informed not only of individual influence operations, but the Community's assessment of the goals and intent of Russia and other foreign adversaries."

Can each of you describe your protocols for sharing threat information with the public on election day or leading up to the elections?

Response: CISA agrees that increased transparency is critical to mitigate the risk of foreign influence operations and we are focused on sharing information with key stakeholders and the American public. CISA has two overarching goals as it relates to sharing information:

- maintain confidence in the election process and results, and
- reduce the willingness of Americans to engage with or amplify foreign influence campaigns.

To do this, CISA has produced a range of public awareness and education products, which we are disseminating through our own channels as well as leveraging the existing networks of key stakeholders, including, for example, The American Association of Retired Persons (AARP), National Urban League, National Association of Latino Elected and Appointed Officials, National Association of Secretaries of State, National Association of State Election Directors and the U.S. Chamber of Commerce. As part of this effort, we created a "War on Pineapple" website and sparked a conversation on Twitter, utilizing a nonpolitical example to help Americans understand how adversaries take advantage of divisive issues to further divide us.

Following the 2016 elections, one of CISA's top priorities was to work with state and local election officials to establish communications protocols in order to guide how information will be reported and empower them to speak to activity targeting their systems or possible incidents. In February 2020, the Elections Infrastructure Subsector (EIS) Government Coordinating Council (GCC) issued a set of voluntary Threat Information Sharing and Incident Reporting Protocols, along with a supplementary Incident Communication Response Plan to improve the efficiency and effectiveness of information sharing between election stakeholders.

Question#:	11
Topic:	Sharing with the Public
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

In June of 2019, CISA hosted a second “*Tabletop the Vote*” exercise with our federal partners, state and local election officials, and private sector vendors to review coordination protocols and incident response plans. The *Tabletop* covered a number of pre-, post- and day of election scenarios, including voter registration compromises, equipment issues, and misinformation distributed over news and social media. Participants included representatives from 47 states, thousands of local election officials, the District of Columbia, U.S. Virgin Islands, along with our Federal partners.

Question#:	12
Topic:	Canada Protocol
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: Canada created the "Critical Election Incident Public Protocol," a series of steps to notify political parties and the wider public about foreign interference in elections in real time. Can each of you describe your thoughts on this process and whether the U.S. should adopt a comparable one?

Response: CISA agrees that increased transparency is critical to mitigate the risk of foreign influence operations and we are focused on sharing information with key stakeholders and the American public. CISA has two overarching goals as it relates to sharing information

- maintain confidence in the election process and results, and
- reduce the willingness of Americans to engage with or amplify foreign influence campaigns.

To do this, CISA has produced a range of public awareness and education products, which we are disseminating through our own channels as well as leveraging the existing networks of key stakeholders, including, for example, AARP, National Urban League, National Association of Latino Elected and Appointed Officials, National Association of Secretaries of State, National Association of State Election Directors and the U.S. Chamber of Commerce.

As part of this effort, we created a "War on Pineapple" website and sparked a conversation on Twitter, utilizing a nonpolitical example to help Americans understand how adversaries take advantage of divisive issues to further divide us. In addition, in February 2020, the EIS GCC issued a set of voluntary Threat Information Sharing and Incident Reporting Protocols, along with a supplementary Incident Communication Response Plan to improve the efficiency and effectiveness of information sharing between election stakeholders.

Question#:	13
Topic:	North Carolina Election
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: There were concerns in 2016 that North Carolina voter equipment was purchased by a firm targeted by Russian hackers. During the election, electronic poll books in Durham County - which allow poll workers to check in registered voters - mistakenly showed many voters as having already voted, ultimately resulting in an emergency move to paper pollbooks and long lines. There has since been concerns about whether malfunction was in some way connected to a Russian attack.

CNN reported that on June 5, 2019 DHS was planning to audit election equipment. Why did this investigation take so long and what is your organization doing to ensure that any future concerns are immediately investigated?

Response: CISA provides a variety of free assessments and services to our election community partners. These include incident response and analysis capabilities, however, CISA does not disclose who we are working with and what services they are using. Secretaries of State have discussed at times the types of services their state is receiving.

Question#:	14
Topic:	Ransomware Attack
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: Director Krebs recently pointed out the increase in ransomware attacks on small municipalities around the country, with 10 in Texas alone in the last few months.

What are your agencies doing to preemptively deter and respond to these attacks? Are the actors being prosecuted?

Response: A successful ransomware attack at a critical point before an election could limit access to information and has the potential to undermine public confidence in the election itself. To help address this threat, CISA is working closely with election officials and their private sector partners to protect election infrastructure and respond to possible ransomware attacks. This three-pronged approach includes raising awareness of the risks of and responses to these attacks, providing targeted cybersecurity services to protect voter registration databases, and implementing a coordinated vulnerability disclosure program in partnership with the EI-ISAC.

Regarding prosecution of ransomware perpetrators, CISA defers to the U.S. Department of Justice.

Question#:	15
Topic:	Cleared Officials
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: Six months after the 2016 attacks on our elections, the states wrote a letter to DHS stating that quote "nearly six months after the [critical infrastructure] designation and in spite of comments by DHS that they are rushing to establish election protections, no secretary of state is currently authorized to receive classified threat information that would help them to protect their election systems."

How many Secretaries of State are authorized to receive classified threat information to protect their election systems? Mr. Masterson testified last year before the senate that DHS is sponsoring up to three election officials in each state for security clearances. How many states you have already cleared three officials?

Response: As of February 2020, 38 Secretaries of State are authorized to receive classified threat information. Of the 12 states whose Secretaries of State do not have security clearances, seven have at least one official in the election office who can receive classified information. In addition, DHS and our Intelligence Community partners can provide 1 day read-ins to Secretaries of State and other election officials on an as needed basis.

Currently, 19 states have three officials cleared to receive classified information.

Question#:	16
Topic:	Protecting Vulnerable Counties
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: The Defending Digital Democracy Report wrote that, on pages 8-9: "disparities in cybersecurity resources and experience across jurisdictions creates vulnerabilities. Smaller jurisdictions with fewer resources may be seen as more vulnerable targets by adversaries. Our nationwide security survey of states and territories reinforced this, with the most frequent concern noted by election officials being insufficient resources to secure the process, especially in smaller counties."

Are your organizations prioritizing protecting more vulnerable counties with less resources?

Response: The threat landscape has changed significantly over the past decade, and individual states and counties cannot go it alone against the full assault of the Russian GRU and FSB. CISA stands ready to offer our resources and services, at no charge, to any state and local election jurisdiction that requests it so that we can provide a collective defense across the country.

Question: What is the protocol for ensuring protection of these communities?

Response: CISA has also done extensive outreach to state and local election officials to make them aware of these services. We've encouraged counties to sign up for EI-ISAC alerts so that they're aware of threats to their election infrastructure and to take part in other services, such as the Last Mile initiative. This initiative is geared towards county election officials specific to their jurisdictions about how to manage risk and threat, including how to talk to voters about the process and manage voters' expectations. CISA has delivered these products to over 1,900 jurisdictions in 21 states to date and is on target to deliver products to a total of more than 6,000 local election offices in 40 states before Election Day in November 2020. CISA also conducts tabletop exercises where thousands of local election officials, in coordination with their state election officials, discuss how information gets shared with the elections community to allow them to understand the threat or risk to their systems. In June 2019, CISA hosted a second "Tabletop the Vote" exercise with our federal partners, state and local election officials, and private sector vendors to review coordination protocols and incident response plans. The *Tabletop* covered a number of pre-, post- and day of election scenarios, including voter registration compromises, equipment issues, and misinformation distributed over news and social media. Participants included representatives from 47 states, thousands of local election officials, the District of Columbia, U.S. Virgin Islands, along with our Federal partners. The purpose was to help build a deeper understanding on threats to election infrastructure, the federal government's capabilities to support state and local officials and exercise response plans and information sharing capabilities.

Question#:	17
Topic:	Russian Voter Suppression Tactics
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: During the hearing, Congresswoman Scanlon asked the FBI about an October 3, 2019 advisory the FBI, along with DHS, issued an advisory to State election officials that the Russian government would be using voter suppression tactics to interfere in the 2020 elections, and obviously, we are extremely concerned about that. Ms. Floris could not speak to the specifics of (1) when the FBI learned about these Russian tactics and (2) how long after the FBI learned of this threat states and local officials were notified.

When did you learn of the threat issued in his advisory; when were states notified; and if there was a delay between, please state the basis for delaying reporting this information to the states.

Response: The advisory in question was not considered a notification of specific plans from identified threat actors but was rather an assessment that a tactic used by Russian actors in prior election cycles might well be used again. Therefore, it wasn't a specific notification intended for any particular state and was published "For Official Use Only" so as to raise general awareness among DHS and Federal Bureau of Investigation customers and partners. The same rationale covers the "Secret" version of the advisory that DHS Office of Intelligence and Analysis released beforehand.

Question#:	18
Topic:	Sharing Threat Information
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: In 2018, your department's "Cybersecurity and Infrastructure Security Agency" or CISA set up a war room and invited state and local officials and private sector technology providers to participate and share information, which was a strong step forward.

What is your organization doing to improve the real-time sharing of threat information in 2020?

Response: CISA has prioritized the expansion of EI-ISAC members to include additional state and local election officials. This is the hub of information sharing that we use to reach these officials. We currently have all representatives of 50 states and the territories as members of the EI-ISAC, as well as over 6,000 local election officials. This ensures that actionable, timely information is reaching the field so that they can take the steps they need to manage risk to their systems. CISA also funds the deployment of intrusion detection capabilities, known as elections-specific ALBERT sensors, to state and local election networks. ALBERT is a unique network monitoring solution that provides automated alerts on both traditional and advanced network threats, allowing state, local, tribal, and territorial (SLTT) organizations to respond quickly when their data may be at risk. CISA has now funded the deployment of these sensors to all 50 states and 175 local election jurisdictions, as of February 2020.

CISA is also working closely with the intelligence community to provide clearances and classified briefings, whether through secure video teleconferences or in person, as well as working with private sector threat intelligence authorities to state and local election officials. In February 2019, CISA officials provided updates to election officials on the full package of security resources that are available from the Federal Government, along with a roadmap on how to improve coordination across these entities. CISA also worked with our intelligence community partners to provide a classified briefing for election officials regarding the current threats facing our election infrastructure.

On Super Tuesday, CISA hosted both a classified and unclassified operations center to monitor any incidents affecting elections across those states. CISA coordinated efforts and sharing of information with our Federal, State, and local partners, political parties, election technology companies, and social media companies. CISA will reconvene the classified and unclassified operations center this November, just as we did in 2016 and 2018.

Question#:	19
Topic:	Deep Fake Technologies
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: Intelligence communities have reported that "deep fake" technologies are a major threat going into 2020.

Are your organizations actively looking into preemptively identifying and holding accountable individuals who attempt to use deep fake technologies / create false videos? How specifically are you doing this?

Response: Deepfakes can have serious real-world effects and can be used to effect changes in opinion, sentiment, motivation, decision making, and beliefs. There are useful detection technologies available today, and that technology continues to improve. However, even if a high percentage of Deepfakes prove to be detectable, they would still pose serious risk. Once false information is in circulation, it can be difficult to completely discredit. DHS works with law enforcement, the Intelligence Community, academia, and foreign partners to identify and study Deepfake-related technology. For example, DHS Science and Technology Directorate recently hosted a workshop on adversarial machine learning where experts examined threats and countermeasures related to Deepfake technology. DHS is pursuing solutions that leverage the best thinking and advances available from all quarters.

Question: How are you working with news organizations to work against these threats?

Response: DHS, through CISA's Countering Foreign Influence Task Force, also actively engages with social media companies to share information about ongoing and emerging risks. The Countering Foreign Influence Task Force does not suggest or direct that the social media companies take any particular action in response to engaging with the Countering Foreign Influence Task Force, but those companies may independently take mitigating steps that are informed by information shared by the Task Force. The strong relationships with social media platforms also allows DHS to share reporting of possible deep fakes from state and local election officials directly to the platforms.

Question#:	20
Topic:	Chinese Voting Machines
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: On November 18, 2018, Business News reported that China granted trademarks for Ivanka Trump to make voting machines.

Are these trademarks for machines in China or here? Do we accept voting machines in this country from foreign countries, particularly countries trying to attack us?

Response: DHS defers to EAC on this question.

Question#:	21
Topic:	Contact with Trump Campaign
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Jerrold Nadler
Committee:	JUDICIARY (HOUSE)

Question: The attack on our 2016 elections, including stealing thousands of documents from the DNC, DCCC, and the Clinton Campaign, underscore the importance of protecting our campaigns from attacks. Director Krebs has since emphasized the importance of protecting these campaigns, saying: "Shame on us if we're not ready this time around." During our hearing, you testified that you have "made contact with the Trump campaign."

Can you please explain how many times you've met with them, what recommendations you provided, and whether they adopted those recommendations?

Response: CISA stands ready to offer our suite of services to Federal political organizations and campaigns. CISA has already provided threat briefings to all the Presidential campaigns registered with the FEC, and with representatives of the Democratic National Committee and the Republican National Committee. We are also actively working with Presidential and congressional campaigns to identify vulnerabilities and secure their systems. CISA does not identify specific entities with whom it has engaged or to whom it has provided technical assistance.

Question#:	22
Topic:	Compliance Process
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Madeleine Dean
Committee:	JUDICIARY (HOUSE)

Question: In March of 2018, Ms. Manfra testified that many vendors submit equipment through a voluntary compliance process run by DHS.

How many vendors exactly have submitted to this process and what percentage of their equipment has gone through that process? Have you reached out to vendors who have not voluntarily submitted to compliance tests to coordinate security? Why or why not?

Response: DHS offers the same no-cost support and services to private sector election technology providers as we offer to state and local officials. This includes critical CPEs, which are open-ended vulnerability assessments of the system provided by the vendor. At this time, DHS has completed 3 election-related CPEs.

The CISA Cyber Assessments team, in concert with ESI election security consultants, is conducting outreach to the elections community, including briefing Secretaries of State and the EISCC on the CPE capability.

CISA's CPE capability has received increased interest from the vendor community and CISA is aiming to complete additional CPEs by September 2020.

Question#:	23
Topic:	Software Updates
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Madeleine Dean
Committee:	JUDICIARY (HOUSE)

Question: Like all technology in use, voting machines sold by vendors will require periodic updates and software patches.

What are the guidelines for updating these machines, are they manually updated to maintain an airgap, or are vendors given remote online access?

Response: DHS recommends the regular and timely patching of all IT systems, including election systems. For election systems, the deployment of security patches can be challenging because in many cases the voting systems are not networked and need to be updated individually instead of through internet-provided patches. In addition, DHS recommends isolating and air gapping voting systems, including local election management systems. DHS defers to the EAC for procedures regarding EAC-certified voting systems.

Question#:	24
Topic:	Election Security Teams
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Greg Stanton
Committee:	JUDICIARY (HOUSE)

Question: There have been cuts to DHS funding. The White House has also disbanded the Commission on Election Integrity and the Cyber Coordinator-the roles of those groups are now within DHS. Yet, in February, the Daily Beast reported that according to three current and former DHS officials, quote: "two teams of federal officials assembled to fight foreign election interference are being dramatically downsized." More specifically, one task force assembled to help defend our elections is now quote: "half the size it was two months ago" according to two DHS officials familiar with the task forces.

I understand that your director has confirmed that election security remains a priority for the Cyber Security and Infrastructure Security Agency (CISA). But I want you to answer very specifically: have teams dedicated to election security been cut, reduced or reorganized by this administration in the last year?

Response: Election security is a top priority for DHS and specifically CISA. Following the 2018 midterms, CISA transformed the Election Task Force into the Election Security Initiative, which has permanent staff to address both election infrastructure work and countering foreign influence work. We're aiming to have between 20-30 full time personnel for the 2020 election cycle and will be able to draw on field staff and other personnel across the Department as necessary. In addition to that personnel, on any given day hundreds of CISA employees across the country are engaged in election security work.

Question#:	25
Topic:	Needed Resources
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Greg Stanton
Committee:	JUDICIARY (HOUSE)

Question: DHS requested 20 new advisors to help in advance of the 2020 election cycle. Yes or no, do you feel you have the resources you need in the President's new budget-which again cuts CISA's budget-to protect our elections?

Response: Securing our elections is a top priority for DHS. The Department has the resources necessary to ensure that our state, local, and private sector partners are able to reduce and mitigate risks to our Nation's election infrastructure ahead of the 2020 elections.

The FY 2020 Consolidated Appropriations Act (Public Law 116-93) provided \$43.5 million for election security and countering foreign influence efforts, which is \$19.5 million above the budget request to support State, local, tribal, and territorial governments.

The FY 2021 President's Budget (PB) includes an increase for cybersecurity support services, which are available to be used on election systems. These include proactive vulnerability assessments, technical analyses, threat detection and response, and classified and unclassified information sharing. The FY 2021 PB also supports additional Cybersecurity Advisors (CSAs) which would expand the DHS cyber field presence and allow CISA to provide cybersecurity services to underserved geographic areas and stakeholder bases and to focus on critical functional cybersecurity issues such as election infrastructure. The FY 2021 PB reflects changing requirements in a year that does not include a major national election and will not have a negative impact on our election security mission.

Question#:	26
Topic:	Preemptive Actions
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Greg Stanton
Committee:	JUDICIARY (HOUSE)

Question: The Senate Select Committee's Intelligence Report concluded that the intelligence community is dependent on the states' doing their own investigation in order to collect information on potential breaches.

What are your agencies doing to ensure that you can preemptively detect breaches, and ensure adequate investigation of breaches following any issues on election day?

Response: CISA is working closely with our state and local partners to ensure they have adequate support and resources from the Federal government to identify data breaches long before Election Day. We have points of contact and trusted relationships across all 50 states so that election officials feel comfortable sharing this information, should a data breach occur.

On Election Day, CISA will move to a heightened state of operational readiness and will have both classified and unclassified operations centers to coordinate our efforts with representatives from federal, state and local partners, political parties, election tech companies and social media companies. CISA will also hold recurring touchpoints with the EI-ISAC and interagency partners. DHS Regional Teams have established relationships with state and local officials across the country. They will be operating on a heightened state of readiness on Election Day to report information to our Watch and Warning teams as well.

CISA will also stand up our National Cybersecurity Situational Awareness Room. This is an online portal for state and local election officials and vendors facilitates rapid sharing of information and it gives election officials virtual access to CISA's 24/7 operational watch floor. This concept was successful during the 2018 elections, enabling rapid reporting and timely response across multiple states at once. This Situational Awareness Room will continue to operate for next year's primary elections and on Election Day 2020. Together, CISA and our federal partners will ensure that the full resources of the federal government are available to support election officials if necessary.

Question#:	27
Topic:	Information-Sharing
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Lucy McBath
Committee:	JUDICIARY (HOUSE)

Question: Multiple witnesses testified that their agencies rely on information-sharing between local, state, and federal entities to effectively address threats.

What are each of your agencies doing to ensure sufficient information-sharing from local and state jurisdictions to your agencies?

Response: Over the last three years, CISA has greatly expanded its efforts to improve information sharing between state and local election officials and the Federal government. Some examples of this work are below:

- CISA works the EI-ISAC to provide threat and vulnerability information to state and local officials. The EI-ISAC has representatives co-located with CISA's operations center to enable regular collaboration and access to information and services for election officials.
- CISA funds the deployment of intrusion detection capabilities, known as elections-specific ALBERT sensors, to state and local election networks. ALBERT is a unique network monitoring solution that provides automated alerts on both traditional and advanced network threats, allowing SLTT organizations to respond quickly when their data may be at risk. CISA has now funded the deployment of these sensors to all 50 states and 175 local election jurisdictions.
- In July 2018, CISA worked to establish communications protocols with the state and local election officials to improve the efficiency and effectiveness of information sharing between election stakeholders. They have been updated for 2020.
- In February 2019, CISA officials provided updates to the Secretaries of State, state election directors, and members of the GCC and Sector Coordinating Councils on the full package of election security resources that are available from the Federal government, along with a roadmap on how to improve coordination across these entities. DHS also worked with our IC partners to provide a classified one day read-in for these individuals regarding the current threats facing our election infrastructure.
- In June 2019, CISA hosted a second "*Tabletop the Vote*" exercise with our federal partners, state and local election officials, and private sector vendors to review coordination protocols and incident response plans. The *Tabletop* covered a number of pre-, post- and day of election scenarios, including voter registration compromises, equipment issues, and misinformation distributed over news and social media. Participants included representatives from 47 states, thousands of

Question#:	27
Topic:	Information-Sharing
Hearing:	Securing America's Elections Part II: Oversight of Government Agencies
Primary:	The Honorable Lucy McBath
Committee:	JUDICIARY (HOUSE)

local election officials, the District of Columbia, U.S. Virgin Islands, along with our Federal partners.

Question: What obstacles, if any, have your agencies encountered in making sure that local and state entities are willing to quickly share threat information with your agencies?

Response: The biggest obstacle that CISA encountered with state and local governments after the 2016 election was a lack of trust and understanding of the role DHS can play in election security. Since 2016, CISA has dedicated extensive time and resources to building and growing our relationships with state and local election officials from nearly zero relationship and little trust to today, where we are working with all 50 states and more than 6,000 jurisdictions. Throughout 2018 and 2019, we have had robust engagement and information sharing processes with state and local partners regarding risks and threats to election infrastructure – and we'll continue to strengthen these relationships in 2020.