

THREATS TO THE HOMELAND

HEARING

BEFORE THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 24, 2020

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs



U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio	GARY C. PETERS, Michigan
RAND PAUL, Kentucky	THOMAS R. CARPER, Delaware
JAMES LANKFORD, Oklahoma	MAGGIE HASSAN, New Hampshire
MITT ROMNEY, Utah	KAMALA D. HARRIS, California
RICK SCOTT, Florida	KYRSTEN SINEMA, Arizona
MICHAEL B. ENZI, Wyoming	JACKY ROSEN, Nevada
JOSH HAWLEY, Missouri	

GABRIELLE D'ADAMO SINGER, *Staff Director*

JOSEPH C. FOLIO III, *Chief Counsel*

MICHELLE D. WOODS, *Director of Homeland Security*

MARGARET E. FRANKEL, *Professional Staff Member*

DAVID M. WEINBERG, *Minority Staff Director*

ZACHARY I. SCHRAM, *Minority Chief Counsel*

ALEXA E. NORUK, *Minority Director of Homeland Security*

CHRISTOPHER J. MULKINS, *Minority Deputy Director of Homeland Security*

LAURA W. KILBRIDE, *Chief Clerk*

THOMAS J. SPINO, *Hearing Clerk*

CONTENTS

Opening statements:	Page
Senator Johnson	1
Senator Peters	4
Senator Lankford	14
Senator Hassan	17
Senator Romney	19
Senator Rosen	22
Senator Scott	24
Senator Paul	26
Senator Portman	29
Senator Carper	32
Senator Hawley	36
Senator Sinema	38
Prepared statements:	
Senator Johnson	49
Senator Peters	51

WITNESSES

THURSDAY, SEPTEMBER 24, 2020

Hon. Christopher A. Wray, Director, Federal Bureau of Investigation, U.S. Department of Justice	5
Hon. Christopher Miller, Director, National Counterterrorism Center, Office of the Director of National Intelligence	8
Hon. Ken Cuccinelli, Senior Official Performing the Duties of the Deputy Secretary, U.S. Department of Homeland Security	10

ALPHABETICAL LIST OF WITNESSES

Cuccinelli, Hon. Ken:	
Testimony	10
Prepared statement	70
Miller, Hon. Christopher:	
Testimony	8
Prepared statement	63
Wray, Hon. Christopher A.:	
Testimony	5
Prepared statement	53

APPENDIX

Responses to post-hearing questions for the Record:	
Mr. Wray	77
Mr. Miller	80
Mr. Cuccinelli	90

THREATS TO THE HOMELAND

THURSDAY, SEPTEMBER 24, 2020

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m., in room SD-342, Dirksen Senate Office Building, and by videoconference, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Portman, Paul, Lankford, Romney, Scott, Hawley, Peters, Carper, Hassan, Sinema, and Rosen.

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. Good morning. This hearing will come to order.

I want to first welcome and thank our witnesses: the Honorable Christopher Wray, the Director of the Federal Bureau of Investigation (FBI); the Honorable Christopher Miller, the Director of the National Counterterrorism Center (NCTC); and the Honorable Ken Cuccinelli, the Senior Official Performing the Duties of the Deputy Secretary.

This is our annual threat hearing. When I take a look at all the threats that this Committee has considered and all the threats facing this Nation, I think it is pretty interesting, how many hearings we have held on so many of these things.

Before I proceed, I guess I would ask for unanimous consent (UC) to have my written statement be entered into the record.¹

But if you consider these threats—for example, I will just quick go down the list: cyber attacks, and these are cyber attacks, ransomware, intellectual property theft, something that we are concerned about right now as we try and develop vaccines, but the hundreds and billions of dollars of economic loss due to intellectual property theft; potential cyber attacks and threats against our critical infrastructure; drug trafficking and the overdose crisis; gangs like MS-13; electromagnetic pulse (EMP) and geomagnetic disturbance (GMD) threats to our electrical grid; the malign use of drones; human trafficking; election security; and school and other mass shootings. These are issues, these are threats that this Committee has not only held hearings on but passed some pretty significant pieces of legislation.

One hearing we had talked about school shootings. We have had the parents of Luke Hoyer and Max Schachter come in from Park-

¹The prepared statement of Senator Johnson appears in the Appendix on page 49.

land, Florida, to describe, hopefully what could be some common-sense solutions to help prevent or minimize the destruction from some of these mass shootings.

And so as we consider all these things—and we will be considering these today in our hearing—I do want to raise the troubling aspect of what is happening currently in the streets of America. As serious as all these threats that I just mentioned are, I have a growing fear that what is happening on the streets of America actually represents a greater threat for our long-term democracy.

As Senator Peters pointed out yesterday, and I am sure will point out again today, the mass shootings over the last couple years certainly have—instead of being perpetrated by Islamist terror, there is a greater percentage, a growing percentage, a majority now perpetrated by white supremacists. But as Acting Secretary Wolf said in our hearing yesterday, what is happening in terms of mass shootings over the last couple years is completely different versus what has happened in the last 4 months.

I just want to cite a study. This was published by U.S. Crisis Project. It was a joint effort by the Armed Conflict Location and Event Data Project and Princeton University. And what this group did is they actually took a look at what is happening in the streets. They analyzed and they provided data on the last 3 months of demonstrations. What they found is there have been more than 10,600 total.

They also went back to July 2019 and said that, on average, at least for July, there were 1,400 demonstrations in 2019.

So you take a look at that, and you extrapolate and say, a normal level of demonstrations every month is about—or over 3 months would be 4,200. So this year we have had 10,600 or an excess number of about 6,400.

They also analyzed who is protesting. Who are these demonstrators? And about 7,750 of those protests have been linked to Black Lives Matter in all 50 States and in D.C.

Now, what they found is that of the 10,600, about 95 percent were peaceful. In other words, 5 percent turned violent, turned into some kind of riot. The peaceful ones were peaceful in about 2,440 locations. But the 5 percent that turned violent, that ended up being a riot, whether it was property destruction or loss of life, occurred in about 220 locations.

Now, I think as reported, it was pretty minimal. It is only 5 percent turned violent. That represents almost 570 riots that occurred in this Nation over the last 3 months that they studied. Almost 570. And we have seen loss of life. We have seen destruction of property.

In my own State, in Wisconsin, in Kenosha, the protest turned into property destruction, dozens of businesses burned down, the downtown all boarded up. And, of course, the final night of those riots, two people tragically lost their life as well.

And so now we have just seen in Louisville last night where two police officers were shot, and our thoughts and prayers go out to them and their families for a speedy and fully recovery. First of all, why were those people protesting? Why did that turn into a riot?

They were protesting because they did not agree with our system of justice where a grand jury took a look at all the evidence and

brought forward an indictment. But it just was not the indictment or enough indictments that they wanted, so rather than accepting our judicial system that has served this Nation well for as long as we have been a Nation, these individuals turned to rioting, and it turned to destruction.

So what I would like to do right now is ask the Senate Recording Studio to play a short little video of a supposedly peaceful protest following President Trump's acceptance speech at the White House.

[Videotape played.]

Now, fortunately, Senator Paul, his wife, Kelley, and their guests were not harmed, but they were scared, unbelievably, and they had every right to be frightened by how they were accosted and how they were threatened. That is not a peaceful protest. And, the fact of the matter is when you take a look at these statistics from this center, the study found that there were no riots in Seattle's Capitol Hill Organized Protest (CHOP) Zone, or the Nation formerly known as Capitol Hill Autonomous Zone (CHAZ). So I am not exactly sure of these statistics, but once again, 570 peaceful protests turned into rioting, turned into property destruction and loss of life.

By the way, I concede the point that the mass shootings, a majority of those come from white supremacists. Those people—and, by the way, I denounce white supremacists. I am not defending them in any way, shape, or form. But those 7,750 demonstrations, that 570 turned into riots and property destruction and loss of life, those are not being perpetrated by white supremacists. Those are being perpetrated by people with leftist ideology that are perpetrating the rioting and the anarchy that we simply cannot allow to continue in this country.

The other thing I have to point out before I turn it over to Ranking Member Peters is even peaceful protests that continued to linger day after day after day, as quite honestly happened in Kenosha, where the downtown was boarded up, even if it does not result in direct property loss or loss of life, the fact of the matter is those types of protests can turn into sieges that deny other Americans their constitutional right of being able to operate a business or be employed in a business or, quite honestly, allow themselves to provide for themselves and their family.

So this is a serious issue. We cannot just slough it off. So many members of the mainstream media continue to slough it off like, "Oh, these are largely peaceful protests." I will point out the number again: almost 570 that turned into riots, into property destruction, and loss of life. Those are the facts. I do not like it. But of all the threats this Nation faces right now, this current one gives me the greatest cause for concern right now. So hopefully we can have a great discussion of all the threats, but, again, I want to highlight how serious the current threats are, what is happening in our streets today, what happened in Louisville last night, what a serious threat that poses and who exactly—what ideology, what side of the political spectrum are those protests springing from? Senator Peters.

OPENING STATEMENT OF SENATOR PETERS¹

Senator PETERS. Thank you, Mr. Chairman, and thank you to each of our witnesses for being here today. While our Committee has no shortage of serious and consequential issues to tackle, our annual threats hearing is one of the most important opportunities that we have to discuss how we can better safeguard our Nation.

We continue to face a number of security threats, both old and new. Over the past year, since we last held this hearing, unfortunately that list has only continued to grow.

Not only do we continue to face critical threats from foreign and domestic terrorism, cyber attacks, and efforts by foreign governments to sow chaos within our country, we are also dealing with a once-in-a-lifetime pandemic that has tragically taken the lives of over 200,000 Americans.

This public health disaster has also further exposed a significant security risk embedded in the tools we use every single day to connect us with the world.

As we have moved more of our daily lives online because of coronavirus, bad actors have exploited technological weaknesses to attack the platforms we use for remote school and work.

Adversaries are working to infiltrate private companies and government agencies who are part of the critical race to find a vaccine.

Both foreign and domestic actors have also seized on misinformation and disinformation, chipping away at the very fabric of our democracy and sowing discord and mistrust in the institutions we rely on every day to keep us safe.

The scourge of white supremacist violence is a long-standing issue but is now again one of the largest terrorist threats to American safety and security.

I am alarmed that this administration continues to downplay this threat and the root causes driving these violent ideologies.

We cannot be shortsighted when it comes to protecting our national security. As threats continue to develop and evolve, our national security agencies must be willing to adapt.

We count on the Department of Homeland Security (DHS), the National Counterterrorism Center, and the FBI to work together and to provide a unified effort to defend the homeland.

As we discussed at yesterday's hearing, I am concerned that DHS has suffered because of the lack of qualified, consistent, and stable leaders at the agency's helm.

While I am disappointed the Department does not believe the Acting Secretary can testify alongside his counterparts from the FBI and the National Counterterrorism Center on these important issues during his confirmation process, I am looking forward to the testimony from all three of the officials here today.

Many Americans will never know the names of the thousands of personnel that work tirelessly behind the scenes at each of your agencies to keep our country safe.

But we are all counting on you and your teams to address the known threats to our safety and anticipate the emerging as well as the unknown dangers our communities are going to face in the weeks, months, years, and even decades ahead.

¹The prepared statement of Senator Peters appear in the Appendix on page 51.

I am grateful to each of you for joining us here today. I look forward to hearing from you about the threats that America currently faces, what your departments are doing to address each of these threats, and how this Committee and your agencies can continue to work together to protect our national security.

Thank you.

Chairman JOHNSON. Thank you, Senator Peters, and I think our witnesses will hear that repeatedly, because I think on a bipartisan basis we truly do appreciate your service to this Nation and certainly the service and sacrifice of the men and women that work in each of your departments and agencies.

But it is the tradition of this Committee to swear in witnesses, so if you will all stand and raise your right hand. Do you solemnly swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. WRAY. I do.

Mr. MILLER. I do.

Mr. CUCCINELLI. I do.

Chairman JOHNSON. Thank you. Please be seated.

Our first witness is the Honorable Christopher Wray. Director Wray is the Director of the Federal Bureau of Investigation. On August 2, 2017, Director Wray was sworn in as the eighth FBI Director. He previously served as Assistant Attorney General (AAG) at the Department of Justice (DOJ) in the Criminal Division. Director Wray.

TESTIMONY OF THE HONORABLE CHRISTOPHER A. WRAY,¹ DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. WRAY. Good morning, Chairman Johnson, Ranking Member Peters, Members of the Committee. I am honored to be here today on behalf of the men and women of the FBI to discuss our Nation's top threats from the FBI's perspective and what we are doing to counter those threats.

I know we all share a lot of the same concerns about topics ranging from international and domestic terrorism to cybersecurity to the violence in our streets, and particularly this year to the threat of foreign influence in our elections, just to name a few. I look forward to updating you on these and other important topics this morning.

But I would like to begin by covering a few items that have been particularly top of mind for us at the FBI over the past few weeks.

First, terrorism remains the FBI's top priority. Though the nature of that threat has evolved significantly since 9/11, we are ever vigilant in our efforts to prevent attacks by international terrorist groups like al-Qaeda and Islamic State of Iraq and Syria (ISIS). Those groups pose a threat not just to Americans overseas, but also here at home, most notably by those we call "homegrown violent extremists (HVE)," often lone actors inspired by foreign terrorists, self-radicalized typically online, and motivated to attack soft targets with readily available weapons.

¹The prepared statement of Mr. Wray appears in the Appendix on page 53.

But we are also working around the clock to prevent attacks by domestic terrorists who are inspired by one or more extremist ideologies to commit violent acts. In recent years, we have been laser-focused on threats posed by racially or ethnically motivated violent extremists, and they, too, are often radicalized online and mobilize quickly to carry out their violent plan—people like Richard Holzer who our Denver Joint Terrorism Task Force arrested on hate crime charges late last year while he was planning to blow up a synagogue in Pueblo, Colorado.

As with any terrorism case, we are focused on disruption, on making arrests before a criminal can act. Just this year alone, through the hard work and dedication of countless men and women both at the FBI and across our partner agencies, we have successfully thwarted terrorist attacks in Kansas City, in Tampa, Cleveland, Oklahoma City, Boston, Phoenix, and other locations.

Now, in recent months, we have witnessed protests in various places around the country, and many Members of Congress have raised a variety of questions about those protests. And although the majority of protesters have been peaceful, we have opened investigations on individuals involved in criminal activity at these protests, some of whom adhere to violent extremist agendas designed to sow discord and upheaval.

Now, let me be clear. We do not investigate groups or individuals based on ideology or on the exercise of First Amendment-protected activity alone. But when the ideology leads someone to commit criminal acts and pursue violence, the FBI will not hesitate to take appropriate action. That is why we have been working closely with our Federal, State, and local partners to ensure the safety of our citizens, including, I should add, the safety of all those trying to exercise their First Amendment rights peacefully. We in law enforcement must keep our communities safe and secure while safeguarding our citizens' constitutional rights and civil liberties. And as I have said before, one need not and must not come at the expense of the other.

We also remain focused on other threats. In less than 2 months, Americans will exercise one of their most cherished rights: to vote in a free and fair election. Americans must have confidence in our voting system and our election infrastructure, and that is why the security of our elections is and will continue to be one of our highest priorities. We are not going to tolerate foreign interference in our elections, and we are working closely with our Federal, State, and local partners as well as the private sector to share information, bolster security, and identify and disrupt any threats.

Just recently, for example, we shared threat indicators with Facebook and Twitter that allowed them to take down fake accounts created as part of a Russian disinformation campaign before those accounts could develop some kind of broader following.

Turning to the cyber arena, we are focused on an increasingly diverse array of threats from our cyber adversaries, from State-sponsored Chinese intrusions to intrusions by Russia, Iran, North Korea, sophisticated cyber criminals seeking to exploit technical vulnerabilities primarily for personal profit.

Last week, I announced the FBI's new cyber strategy, leveraging our unique expertise and authorities to impose risk and con-

sequences on our cyber adversaries. We are focusing on results on impact, and that means we are working to enable our partners' operations as well as our own.

So, for example, the FBI and National Security Agency (NSA) recently joined to expose highly sophisticated Russian military intelligence malware, providing the private sector and other government partners the indicators they need to disrupt that tool.

And just last week, our investigations enabled a coordinated mix of disruption actions against five different Iranian hacking groups, three of which worked for the Iranian Government, including criminal charges by DOJ, Treasury Office of Foreign Assets Control (OFAC) sanctions, and Cybersecurity and Infrastructure Security Agency (CISA) and FBI alerts enabling potential victims to protect themselves.

We also face the increasingly blended threat of State-sponsored economic espionage facilitated by cyber intrusions. In July, based on the FBI's investigative work, DOJ indicted two Chinese hackers working with the Ministry of State Security for carrying out a global computer intrusion campaign targeting hundreds of victims, including companies developing Coronavirus Disease 2019 (COVID-19) vaccines, testing technology, and treatments. With that kind of behavior, China continues to undercut their own claims of being a trusted and effective partner in the international community.

Last week, we unsealed charges against five Chinese hackers who were targeting victims around the world from their safe haven in China. With our partners, we arrested two of their co-conspirators in Malaysia and seized or took down hundreds of the hackers' accounts, servers, and domains.

Now, I have touched on only a handful of the important threats we face, and only lightly at that, and, of course, there are many significant others. As the threats evolve in scale, impact, complexity, and agility, we are relying on our deep well of expertise, intelligence, and partnerships. I am committed to ensuring that the Bureau does great work while adhering to our core tenets of fidelity, bravery, and integrity.

In these challenging times, I remind my folks that we have to keep calm and tackle hard, remaining faithful to our core values and best traditions while making sure that we are always doing the right thing in the right way.

Thank you. I would be happy to take your questions.

Chairman JOHNSON. Thank you, Director Wray.

Our next witness is the Honorable Christopher Miller. Mr. Miller was sworn in as the seventh Director of the National Counterterrorism Center in August 2020. Prior to his confirmation, he served as the Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism. Mr. Miller previously served as the Special Assistant to the President and Senior Director for Counterterrorism and Transnational Threats at the National Security Council. Mr. Miller served in the U.S. Army and has extensive experience with interagency and joint special operations. Mr. Miller.

TESTIMONY OF THE HONORABLE CHRISTOPHER MILLER,¹ DIRECTOR, NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. MILLER. Chairman Johnson, Ranking Member Peters, and distinguished Members of the Committee, it is with deep humility that I appear before you today to present my views on the state of our war against Islamist jihadist terrorist groups and other extremists that mean us harm. I represent an enormously talented and committed group that is on duty 24/7/365 to protect our citizens from terrorist attack.

Before I begin my prepared remarks, I want to publicly thank the Department of Justice for their tireless pursuit to bring the Beatles to justice in partnership with our great friends in the United Kingdom (UK). The Beatles were ISIS leaders involved in the brutal killing of Americans. Although our efforts can never replace their loved ones, we are hopeful that the families receive some degree of closure. This is a reminder to our enemies that we never forget and will pursue justice to the ends of the Earth.

Nineteen years ago, after the shock of al-Qaeda's devastating attacks abated, our Nation set out to accomplish three objectives: one, harden our borders; two, go overseas to destroy the safe havens and sanctuaries of al-Qaeda and its associated groups and attrit their combat forces; and, three, address the drivers of instability that created al-Qaeda by supporting like-minded partners in their efforts to combat Islamist extremism.

Due to the enormous dedication, selfless service, and sacrifice of hundreds of thousands of Americans and like-minded foreign partners, we have been remarkably successful in accomplishing the first two objectives. I sense that we are on the verge, if providence is kind, of transitioning from a U.S.-led, partner-enabled campaign to an era where local and regional partners take the lead and we provide them niche support to fill gaps in their security, intelligence, informational, and legal architectures.

I must be clear and not histrionic. Our enemies will successfully attack us again as their adaptation and innovation is driven by a profound hatred for what we represent. This is our terrorists' dilemma and their strategic advantage. They only need to be successful once while our defenses must be successful all the time for preventing a cataclysmic attack.

But our enemies have profoundly underestimated the resilience of the American people time and again. I wonder if the 9/11 al-Qaeda leaders regretted their decision to attack us. I am confident the survivors must. They thought us soft and spoiled and morally unanchored. They are now either dead, imprisoned, or in hiding awaiting death or capture. Their ideology is debunked in the overwhelming majority of the Islamic world. No one today misjudges our resolve and commitment to protecting the security of our citizens and using all available instruments of national power against those that bring war and violence to our shores.

However, as we have experienced in the past, the purveyors of extremism will periodically amass the resources required to attack us. My principal concern is their potential acquisition and use of

¹The prepared statement of Mr. Miller appears in the Appendix on page 63.

weapons of mass destruction (WMD). If history is an accurate guide, weapons developed are ultimately used. I do know that the American people can withstand anything they throw at us, and the use of WMD by a terrorist group would make our successful pursuit of the 9/11 attackers pale in comparison. Those that underestimate the fortitude, toughness, grit, and resolve of the American public do so at their profound peril, and any such attack would guarantee their elimination.

ISIS, which originally formed as al-Qaeda in Iraq, is in crisis. Its vaunted caliphate is destroyed, and its ideology is exposed as a brutal, perverse, and horrifying abomination. The world recognizes that a positive and magnificent faith was hijacked by a handful of corrupt, selfish opportunists.

ISIS' territorial defeat in Syria and Iraq has forced the group to return to its insurgent roots and increased its reliance on its global branches and networks to project a narrative of strength. With superb partners from the 86-member coalition that defeated ISIS in the Middle East, we continue our efforts to render ISIS permanently impotent.

Even as we continue to combat these traditional enemies, we face new ones, including increasingly aggressive groups aligned with Iran and domestic violent extremists (DVE) motivated by a variety of ideologies. I am hopeful that in the coming year or two we will be successful in destroying the remnants of al-Qaeda's leadership and continue the attrition of ISIS, guaranteeing that this does not become a multi-generational war.

For the past 19 years, I have been involved in this struggle at all levels, from the moonscape of southern Afghanistan in 2001 to Baghdad in 2003 to senior policy and strategic leadership in Washington, D.C., and internationally as a counterterrorism (CT) strategist, adviser, and policymaker. The only sacrosanct lesson I have learned is that we must maintain pressure on these groups to preclude them from establishing safe haven where they can rest, train, plot, and project combat forces.

We must continue to be chastened by our relaxing of this constant pressure in 2011, which allowed for the creation of the largest, most successful terrorist insurgency in modern history in Iraq and Syria. It is a testament to the sacrifice of a generation that we are now at a place where terrorism is not the primary national security priority but, rather, another issue of concern. But we must not overcorrect or disinvest before we solidify our gains and make them enduring. This war has been long. Many are tired. We face new crises and challenges. We have sacrificed greatly. But as wars near their end, victory requires continued commitment and focus. This is what we owe the next generation, that we saw it through and we ended it on our terms.

I thank you for this body's uncompromising support and partnership. I rest easier knowing that your support will continue as we maintain pressure on al-Qaeda and ISIS in these final battles. I look forward to your questions.

Chairman JOHNSON. Thank you, Director Miller.

Our final witness is the Honorable Ken Cuccinelli. Mr. Cuccinelli is the Senior Official Performing the Duties of the Deputy Secretary of Homeland Security. He previously served as the Acting

Director of U.S. Citizenship and Immigration Services (USCIS) and also served as the Attorney General (AG) of the Commonwealth of Virginia, where he led the State's fight against human trafficking. Mr. Cuccinelli.

TESTIMONY OF THE HONORABLE KEN CUCCINELLI,¹ SENIOR OFFICIAL PERFORMING THE DUTIES OF THE DEPUTY SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. CUCCINELLI. Good morning, Chairman Johnson, Ranking Member Peters, and distinguished Members of the Committee. Thank you for the opportunity to testify today. I am here to discuss the myriad of threats facing the American people and our homeland.

In 2020, the men and women of the Department of Homeland Security have carried out their protective mission with professional excellence as our Nation faces unprecedented and dynamic challenges. From the pandemic to riots to natural disasters, the Trump administration has ensured that our personnel have the vital support and the resources they need to address evolving threats while continuing to fulfill our enduring no-fail missions.

DHS has a clear mandate from President Trump: at all times, in all decisions, in all dangers, to keep the safety and prosperity of the American people as our first priority.

Today I will briefly comment on three national threats that deserve specific attention: civil unrest, domestic terrorism, and transnational criminal organizations (TCOs). When we talk about domestic terrorism, we are talking about threats or acts of violence carried out against people or critical infrastructure in the United States to advance an ideological agenda or coerce policy or social change. These are generally conducted by Americans and not linked to foreign terrorist organizations. Americans have the right to believe whatever they want, but there is no right to carry out acts of violence to further those beliefs. That is when we move from protected speech to domestic terrorism.

When the civil unrest by violent anarchists dragged on for months in Portland, Oregon, and local leadership refused to cooperate with Federal law enforcement, the Department of Homeland Security defended the Federal courthouse without hesitation, in partnership with the U.S. Marshals there. Despite being pelted with improvised explosive devices (IEDs), Molotov cocktails, fireworks, metal pipes, hammers, and more, our Federal officers were resolute, sustaining more than 340 injuries in the course of their duties.

Lawlessness has festered in too many of our communities, from Chicago to Seattle, Minneapolis to New York, even Lancaster, Pennsylvania, and Kenosha, Wisconsin. The Department will always uphold the right to peacefully protest, but there is no constitutional right to loot, to burn, or to assault others.

President Trump has made it clear that we cannot and will not allow acts of violence, intimidation, or chaos to prevail in American streets, and the Department of Homeland Security is proud to participate in implementing such policies.

¹The prepared statement of Mr. Cuccinelli appears in the Appendix on page 70.

On the transnational criminal organization front, as we frequently call them—and beyond illegal immigration at our border, we are also contending with the most deadly organizations in the Western Hemisphere: the Mexican drug cartels. To put it in context, the power of these transnational criminal organizations is so great that it is a destabilizing force to many governments in our hemisphere. Their attempts at drug smuggling and human trafficking, not to mention their regular brutal and violent tactics, must be addressed.

Last year in America, we lost 71,000 Americans to drug overdoses. They happened in every one of your States and every one of your communities, and I know all of you are familiar with and touched by those tragedies. Consistently, the majority of these deadly drugs and opioids are produced and smuggled by criminal organizations across our Southern Border. Working daily to decrease the flow of illegal drugs, DHS has seized 4 million pounds of hard drugs. It is worth noting that we are on track to seize drugs at roughly twice the rate of the previous 8 years. So in these 4 years, we have seized about as many drugs as had been seized in the previous 8, of the hard drugs. We are talking about fentanyl, meth, that level of drug seizures.

Transnational criminal organizations and their allies are not content profiting off the destruction of lives through the drug trade. They are also destroying lives through human trafficking. The brand-new 330 miles of border wall in high-impact sectors pushes human traffickers and drug smugglers to locations where we are best equipped to catch them: ports of entry (POEs). It makes their transnational efforts much harder and makes America safer. That is another reason why this administration's delivery on the promise to build that wall and the system that goes with it so very important.

Finally, while I addressed election security at length in my written testimony, I do want to reiterate that our goal at DHS, our fundamental goal, is to ensure that American voters decide American elections. As we sit here in September 2020, that seems an important point worth reiterating.

Finally, we do need legislative help from Congress in at least two areas. There are many we work together in, but there are two I would like to highlight.

We need greater authority—or some authority to designate transnational organized crime at a level below a foreign terrorist organization but giving us authorities above the level of mere criminal law. We will not prosecute our way out of the TCO problem.

We also need the authority to address the drone threat in an appropriate manner. We cannot study the problem forever. We do have some authorities provided by Congress, but we need to be able to bring them down and have the money, the appropriations, to purchase the equipment to allow us to do that. This problem is well studied. The danger is understood, and we are, frankly, behind the curve in being equipped to address it, I would note especially, in my view, at airports, the borders, and sensitive sites.

The threats facing our homeland are vast and varied, but I can promise you the men and women of DHS are committed to rise and

face the evolving threats of tomorrow, embracing their duty to safeguard the American people.

Thank you. I am now happy to answer your questions.

Chairman JOHNSON. Thank you, Mr. Cuccinelli.

Unfortunately, Democrat Leader Schumer is obstructing the workings of the Senate, and so we are bound by some arcane Senate rule that, because of his lack of consent, his obstruction, our hearing has to have a hard stop 2 hours after convening the Senate for business. So, again, unfortunately, I am going to have to limit the amount of time of questioning to 5-minute rounds to make sure that every Senator gets a chance to ask a question, and I will keep people closely to that 5 minutes. So you will hear me interject if you are running over 5 minutes. I will also ask the witnesses to be looking at their clocks as well and not ramble on past the 5-minute time. I want to make sure every Member gets a chance to ask questions.

For the time being, I will defer my questioning, but I will for sure get it in, even if that means a Member does not get to ask questions toward the tail end of the hearing. But I will defer to Senator Peters right now.

Senator PETERS. Thank you, Mr. Chairman. Again, thank you to each of our witnesses for being here today.

Director Wray, I am going to start with you and talk about election integrity, which you raised in your opening comments. It is important for us to put this all in perspective, and we know people are actually voting today in states all across the country. In fact, in Michigan, today is the day that you can go to your clerk and vote, and we are going to have—well over 2 million ballots are being mailed out starting today for absentee voters.

You said last week at the House hearing that, “the steady drumbeat of information” is your No. 1 concern for the election. You noted that the threat can lead to, I will quote again, “a lack of confidence in the American voters and citizens and the validity of their vote.”

So given the COVID-19 pandemic, we are seeing many more people vote by mail. As I mentioned, unprecedented numbers of absentee ballots have been asked for in the State of Michigan. I want to dispel some of this drumbeat of misinformation that we are hearing out there. So my question is very direct. Is voting by mail secure?

Mr. WRAY. Senator, I think what I would say is this: We take all election-related threats seriously, whether it is voter fraud, voter suppression, whether it is in person, whether it is by mail. And our role is to investigate the threat actors.

Now, we have not seen historically any kind of coordinated national voter fraud effort in a major election, whether it is by mail or otherwise. We have seen voter fraud at the local level from time to time, and so my comments should in no way be construed as minimizing how seriously we take our responsibility to investigate such incidents or the potential impact those things could have at the local level. So it is on our radar.

Certainly to change a Federal election outcome by mounting that kind of fraud at scale would be a major challenge for an adversary, but people should make no mistake we are vigilant as to the threat

and watching it carefully because we are in uncharted new territory. I think as far as risk assessments of any particular State's processes or systems, I would defer to Mr. Cuccinelli and DHS CISA because that is really more in their lane.

Senator PETERS. Right, but your answer is clear. You have not seen any widespread fraud by mail. It is something the FBI watches continuously to make sure that that is not happening.

Mr. WRAY. That is something that we would investigate seriously.

Senator PETERS. Absolutely.

Mr. WRAY. And aggressively.

Senator PETERS. So the next question is, effective interagency coordination is obviously going to be very important. You mentioned, Mr. Cuccinelli, with DHS, we are all on this to make sure that our votes are counted and it is a fair and free election. So the question is: What does that interagency cooperation look like? More specifically, who is in charge? Of all of you that are involved in election security, who is actually in charge? Is it the White House? Is it the FBI? Is it Cyber Command (CYBERCOM)? Is it another entity? Who should we look to as being in charge?

Mr. WRAY. So I will start, and maybe Mr. Cuccinelli would want to chime in as well. We all work together. We all have lead in different aspects of the problem. We have command posts where we are all—we have people from each other's agency stationed on that to ensure that the glue, the connective tissue is there.

As far as foreign influence, malign foreign influence here domestically, investigating that is the FBI's lead, as well as investigating cyber intrusions into election infrastructure. But DHS takes the lead in terms of protecting infrastructure and mitigation and response to that. You mentioned CYBERCOM. Obviously, to the extent that there is offensive cyber—

Senator PETERS. So there is not one entity necessarily in charge. You just take care—you have your different lanes to run in, you cooperate, but there is not one person that is going to be—

Mr. WRAY. As is true, frankly, with counterterrorism.

Senator PETERS. OK.

Mr. WRAY. Right. We all work together. We are all lead on different parts, and we work together.

Senator PETERS. I appreciate it. In the limited time I have, Director Wray, just a final question, because you mentioned a foreign government influence in the election and misinformation. Give us some advice. How can American voters recognize an attempt by a foreign government to influence their opinion and vote? It is important, I know behind the scenes you are working, we have all the different agencies that are working. But how do we let the American voter know this is basically a disinformation campaign that is perpetrated by a foreign government? How should they recognize that?

Mr. WRAY. I think it is a challenge, as your question alludes to. I would say when it comes to information about their vote itself, where to vote, when to vote, hours of the polling places, information about the results, things like that, it is very important that Americans get that information from their official state or local

election website as opposed to relying on something that might be on social media, for example.

As far as getting their news, which might shift or influence their views more broadly, I would encourage people to be critical thinkers and to get their news from a variety of sources and make up their own mind and be a skeptical, discerning electorate, which is what I think is the best defense against malign foreign influence and disinformation.

Senator PETERS. I am out of time. Thank you.

Chairman JOHNSON. Senator Lankford.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Gentlemen, thank you very much for the work, and please thank the folks that work around you that we do not get a chance to meet in this pleasant setting when we get a chance to gather every time we gather. Tell them thank you because they do a lot of work behind the scenes.

Director Wray, I want to be able to ask you about some of the violence that has happened across the country in the past several months. We have had hundreds and hundreds of peaceful protests on racial injustice around the country that we are grateful as a country we have that option to be able to have peaceful protests and people are allowed to be able to speak out and point issues out. But some of them have turned very violent, and in some of your testimony in the House, it seemed that you were trying to connect some groups. Have you been able to identify groups or entities behind the scenes that seem to be organizing nationally to foment violence in some of these events? Or are you seeing just spontaneous events or small groups that are unconnected with others?

Mr. WRAY. So, Senator, I appreciate the question, and I appreciate the opportunity to try to be as clear as I can because this is an important topic.

I think the first thing, big picture, is, as the Chairman referenced in his opening comments, when you look across the country, you have three broad categories. You have the peaceful protesters. That is maybe the biggest number of people. Then you have a second category which is what I would describe as “criminal opportunists” engaged in looting, low-level vandalism, et cetera. But then you have a third group, and while it might numerically be the smallest, it is by far and away the most dangerous and most serious and the one that we have to go after the most aggressively, which is the people who are clearly violating Federal law, IEDs, Molotov cocktails, specific targeting of law enforcement, arsons of government facilities and businesses, et cetera. Who those people are—that is our priority, that is our focus—varies, their motivation of what drives them from day to day, city to city.

However, we have certainly seen a number of violent anarchist extremists participating in that mix. I have gotten a lot of questions from a lot of people about Antifa, for example, so let me try to be as clear as I can about that. Antifa is a real thing. It is not a fiction.

Now, we have seen organized, tactical activity at both the local and regional level. We have seen Antifa adherents coalescing and working together in what I would describe as small groups and

nodes. All of this I said last week, but some of it got more clearly conveyed than others.

We have a number of predicated investigations into some anarchist violent extremists, some of whom operate through these nodes and subscribe to or self-identify with anarchist extremism, including Antifa. We will not hesitate to aggressively investigate that kind of activity. So we are going to be looking at and we have been looking at their funding, their tactics, their logistics, their supply chains, and we are going to pursue all available charges.

Also, in addition to that group, there are what I would describe as more militia types, and we have had plenty of those, and we have a number of investigations into those as well.

But I think trying to put a lot of these things into nice, neat, clean buckets is a bit of a challenge because one of the things that we see more and more in the counterterrorism space is people who assemble together in some kind of mish-mash, a bunch of different ideologies. We sometimes refer to it as almost like a “salad bar of ideologies,” a little bit of this, a little bit of that, and what they are really about is the violence. And we are not going to stand for the violence.

Senator LANKFORD. Nor should you, and the American people are grateful for that. Peaceful protest is encouraged and allowed in our country. Violence is not. You and I have spoken several times about Oklahoma-specific issues and the McGirt decision from the Supreme Court last year and the significant change that is for the FBI and Oklahoma. We are grateful for your engagement, and I continue to be able to ask for your engagement for law enforcement there in Oklahoma as we deal with the dynamics of that decision and what that means for us, and we are grateful for that.

Director Miller, before we run out of time—and I have only got a few seconds, and I apologize for that—there is the issue of China. Director O’Brien has made the comment that there is a rise in China trying to be able to engage in our election this year, and he identified that as one of our greatest threats. Can you briefly comment on that and what you are seeing right now? Is it just influence or is it in actual cyber attacks in our system?

Mr. MILLER. Thanks, Senator. I look at international terrorism specifically. I am not really familiar with the—

Senator LANKFORD. OK. Can anyone else comment on that briefly?

Mr. CUCCINELLI. Briefly. Each of the two areas you mentioned, China is a major threat. They are a rising power, and they have every intention of trying to rival and surpass us as a Nation, and they have stolen our intellectual property at a level Director Wray said last week in a phrase I thought was very applicable. “The greatest transfer of wealth in the history of the world” is the Chinese stealing intellectual property from Americans, and for their strategic purpose, military, intelligence, and their economy.

We also face them trying to exercise influence via money and their media enterprises, much more overtly than most other countries are even able to. And last, and absolutely not least in this country, is their massive trade with us, which can be a positive, of course, for both sides, but is also used as a lever of influence.

Senator LANKFORD. Thank you.

Chairman JOHNSON. Senator Lankford, we were just informed that Senator Schumer did not invoke the rule today, so we do not have a hard stop. You have another minute and 15 seconds if you would like to do that, and if Senator Peters would want to tack on another 2 minutes now, or we can do that later. But you can continue your questioning for another minute and 15 seconds. Then we will have 7-minute rounds.

Senator LANKFORD. Great. Thank you. I appreciate that. Let me do my last minute and 15 seconds here. I do want to drill down on this issue about China and trying to malign influence for the election in particular. When Director O'Brien made that comment, obviously we are dealing with Russia and what they did in 2016. We are all very aware of how they were trying to engage in our election. But his comment seemed to be that China is being even more aggressive behind the scenes this time than Russia was. We also know that Iran is trying to be able to influence our elections. I did not know if there was any clarity that any of you could bring to that. Obviously, he is not sitting at the table today, but if there are any other comments about that.

Mr. CUCCINELLI. I would just note that the way China acts in that arena is different than Russia and Iran, in part because they have so many more levers. Iran and Russia do not have the trade with us that China has. They do not have the relationships at every level of government that China has. And they do not have the connections to our economy and so forth.

So they do not have the levers that China has available to them. We have seen through this year COVID was an excellent example as we roll into the election season where they have Ambassadors in other countries, they have their foreign minister. They are taking on false narratives aimed at the United States very overtly and then spreading them through their media outlets in ways that our other opponents do not have available to them. So it is a very unique attack.

Senator LANKFORD. Thank you.

Chairman JOHNSON. Senator Peters, would you like to take your 2 minutes now? Just so everybody knows, I am in quarantine, so I will not be voting. We have an 11:30 vote, so I will definitely defer my questioning to the very end. But, Senator Peters, do you want to go? Or should we go to Senator Hassan?

Senator PETERS. If I could, I will just take a quick 2 minutes. It will be a quick question to continue with Director Wray.

Director Wray, online extremist conspiracy theories kind of have jumped out of obscure Web forms and, unfortunately, now are prominently featured on traditional social media. Even more concerning, they are manifesting themselves in real-world incidents of violence.

So my question to you, Mr. Wray, is: Is there a risk that foreign actors will try to leverage some Americans' belief in some of these conspiracy theories that are floating around quite widely? And will they use that to engineer some violent confrontations? How concerned should we be about that?

Mr. WRAY. Certainly there are sort of two strands that you are alluding to there that we are concerned about. One is the sheer impact of social media on the threats that we face. So in the terrorism

context, we say that terrorism today moves at the speed of social media, and that is really across all the different terrorist threats.

Then, separately, you have this effect also facilitated by social media where foreign adversaries will identify trends, divisive issues, in some cases conspiracy theories, that they will then in effect piggyback on and amplify and push to suit their own policy goals and propaganda. And we see that across a range of adversaries—Russia, of course, but also China, also Iran. And so it is a real concern.

Now, whether or not the second trend will ultimately manifest itself in terms of violence, hard to say, but certainly there is an effort to sow upheaval and discord, and as we have seen around the country, discord and upheaval can lead to dangerous violent criminal activity that we will have to go after very aggressively.

Senator PETERS. This is something the FBI is very focused on, I would hope?

Mr. WRAY. Yes.

Senator PETERS. Good. Thank you.

Chairman JOHNSON. Senator Hassan.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you, Mr. Chair and Ranking Member Peters, for this hearing. Thank you to our witnesses for being here today, and please thank all the women and men with whom you serve for their excellent work keeping us safe.

This hearing is about threats to the homeland. Before we begin, we must acknowledge a new and dangerous threat to our country and our Constitution: the President of the United States' refusal to promise a peaceful transfer of power if he loses the election.

Today I call on every person who has sworn an oath to uphold the Constitution, including my fellow Senators, to condemn the President's remarks and to recommit to ensuring a peaceful transfer of power, whatever the outcome of this election. Some of the Members of this Committee from both parties have already done so, and I appreciate their words. I hope that the rest of the Committee will speak out as well.

Now, to Director Wray, at last year's threats to the homeland hearing, we discussed the growing threat of ransomware attacks to our communities. Over the past 6 months, there has been a further uptick in ransomware attacks on hospitals and schools amid the COVID-19 pandemic. Just this month, a ransomware attack on a German hospital led to the death of a patient, and there has been a spate of ransomware attacks on our schools as districts have migrated to online learning. Our communities do not have the resources to effectively counter a wide range of cyber threats on their own, including ransomware.

Director Wray, I appreciated in your opening comments your discussion of cyber threats. Could you drill down a bit more on what the FBI is doing to help protect State and local governments and other non-Federal partners from ongoing cyber attacks and to deter malicious cyber adversaries?

Mr. WRAY. Senator, I appreciate the question, and I do recall our exchange from last year. Certainly, ransomware is a particularly concerning part of the cyber threat that we face and the threat of

ransomware against State and local governments is particularly high. There are a variety of reasons why ransomware actors target municipalities, hospitals, police forces, et cetera.

Senator HASSAN. Right.

Mr. WRAY. One of the things that we have done recently is through our National Cyber Investigative Joint Task Force, we have brought together a whole-of-government effort to focus across multiple agency, intelligence community (IC), and law enforcement on the most damaging ransomware variants. And some of that is through investigative activity disruptions; some of that is through outreach and engagement where we work very closely with CISA at DHS to help educate those entities on how to better harden and protect their infrastructure, because certainly having good cyber hygiene backups, et cetera, is one of the best defenses against ransomware.

We are seeing—and it is something that concerns me in particular—a growing trend to see ransomware actors essentially sharing ransomware across different organized criminal activities.

Senator HASSAN. OK.

Mr. WRAY. So that basically means that some of the most sophisticated forms of ransomware are now potentially available to less sophisticated actors. It is sort of a version of cyber crime as a service, which is deeply troubling and just increases the risk. We are also seeing a greater trend of ransomware actors essentially piecemeal pushing out the information. In other words, rather than just locking it up and encrypting it and holding it ransom, they are essentially releasing little bits at a time into the public domain as a way of increasing their leverage.

Senator HASSAN. The pressure, right. Thank you. I appreciate that very much, and I look forward to continuing to work with you on that.

Director Wray, I also wanted to touch on another issue. I was pleased to see Tuesday's announcement about Operation Disruptor, an effort to stop drug trafficking on the Dark Web. This operation resulted in the seizure of hundreds of kilograms of illicit drugs, including fentanyl, and dozens of firearms, as well as the arrests of 179 people. Needless to say, this was a significant operation. I appreciate the work of all of the Federal agents who carried it out.

Last week, I wrote a letter to you and the Attorney General asking for more information about efforts to combat drug trafficking on the Dark Web. Senators Cornyn and Feinstein on the Judiciary Committee joined the letter as well. We requested a reply by October 15th. Can you commit to a written response by that date, which is still 3 weeks away?

Mr. WRAY. I certainly will get you a response as promptly as possible. Not having had a chance to read the letter yet, I do not know how involved a response it would mean. But certainly we appreciate your focus on the issue, and Joint Criminal Opioid Darknet Enforcement (J-CODE), which is essentially the operation that we have stood up that spins off these things like Operation Disruptor, is, I think, a really exciting, effective tool, a coordinated inter-agency tool—it is not just the FBI—to disrupt and dismantle darknet marketplaces, which is really a particularly important part of the opioid problem that we are all facing.

Senator HASSAN. Absolutely, so I thank you. I would look forward to a further conversation about what additional resources Congress could provide to help bolster those efforts. But I am going to move on to one last question now, if that is all right.

To Director Miller and Director Wray, last December a member of the Saudi military in the United States on a training mission killed three people and injured eight at a naval air station in Pensacola, Florida. Al-Qaeda's Yemeni affiliate claimed credit for the attack, marking the terrorist group's first successful attack in the United States in several years.

Director Miller and Director Wray, do you feel confident with the adequacy of screening done by the United States on foreign military trainees entering our country? And how would you assess the vulnerabilities of this exchange program? I will start with you, Director Miller.

Mr. MILLER. Thank you, Senator. Obviously of great concern, and thanks for the question. An adaptive, innovative enemy that means us great harm, they found a loophole. The loophole has been closed. I am confident now in the Department of Defense's (DOD) efforts to recognize how security protocols and screening need to work. But they found a loophole, and they exploited it.

Senator HASSAN. Thank you. Director Wray?

Mr. WRAY. I do think that the Department of Defense has taken important strides to address the vulnerability that was there. Of course, there is also an important role for the Saudi Government to play, and they have been cooperative at different times on this issue. But they are an incredibly important partner if we are going to be able to prevent something like what happened at Pensacola again.

Senator HASSAN. Thank you, and I appreciate all of your work very much.

Last, Director Miller, as a New Hampshire Senator, I thank you for everything that you have done to bring the killers of James Foley to justice.

Mr. MILLER. Thank you, Senator.

Chairman JOHNSON. Senator Romney.

OPENING STATEMENT OF SENATOR ROMNEY

Senator ROMNEY. Thank you, Mr. Chairman, and thank you to each of the panelists for the work that you do. I deeply appreciate the work of the men and women who work in your respective organizations that are working every day to keep us safe.

Director Wray, with regards to foreign cyber threats and theft, I think we can agree that the best defense is a good offense. China, Iran, and Russia are only going to stop attacking in a cyber way if they are hurt more than we are. I guess the question is: Do you believe that our offensive cyber efforts are as effective as they should be? And if not, what should we be adding?

Mr. WRAY. So certainly I agree with you that an important part of fighting back against our foreign adversaries in the cyber realm is offense as well as defense. That is a big part of this new strategy, FBI strategy that I rolled out, which is the idea, as I sort of maybe obliquely referenced in my opening statement, about focusing on results and maximizing impact. Sometimes the way to maxi-

mize impact is through law enforcement action that we would take. Sometimes it is through sanctions. But sometimes it is through offensive cyber operations. And we are very focused on making sure that intelligence and information that we develop through our investigative work is shared with our partners to enable their operations offensively.

And so through our National Cyber Investigative Joint Task Force, we are much more effective in partnering with the relevant IC and DOD agencies on that. I think that obviously it is a growing area, and we are getting more sophisticated all the time, and you will never find an FBI Director that would not welcome more tools. But I do think we are moving in the right direction, and I think you are right to raise the issue.

Senator ROMNEY. Thank you, sir.

Director Miller, I appreciate your clear-eyed, unvarnished update on where we are. With regards to weapons of mass destruction, do other nation-states recognize just how severe a threat it would be for a weapon of mass destruction to fall in the hands of a non-State actor and to be used against us, or anyone else, for that matter? Do they recognize that? And are they taking sufficient actions to secure their nuclear capabilities?

Mr. MILLER. Thanks, Senator, for that question. I can say definitively with our partners that they take it seriously. I cannot dispute the fact that some rogue regime might find strategic value in providing such weapons. Obviously, if a nation-state was so unsophisticated to do something like that, I feel strongly that it would probably result in just catastrophic effects on them.

What we are seeing really is they recognize—our terrorist enemies recognize that that is the one thing they have not been able to use against us. We have targeted again and again and will continue to prioritize any terrorist groups that are trying to acquire those types of weapon systems.

Senator ROMNEY. Thank you.

Director Wray and Mr. Cuccinelli, I think we have watched with dismay as what had begun as peaceful protests turn violent, where heavily masked, apparently organized individuals come in and do destruction, and in some cases cause death. It seems in many respects that we are not as effective as we would like to be in preventing or stopping people of that nature. Sometimes we wonder, well, do we need more police on the front lines? Do we need the National Guard? Do we need heavier equipment? Other times it is like, no, no, that will only encourage violence to occur.

I guess the question is this: Given your experience so far, what are we doing wrong? What should we be doing better to prevent what began as peaceful protests from being, if you will, kidnapped by these small groups of, whether it is Antifa or other violent groups of anarchists? How can we shut them down as violence begins to occur in a way that we are not doing now?

Mr. WRAY. I will start and then turn it over to Mr. Cuccinelli. I think at a big-picture level, if you look across the country, the places that have been most effective in countering the kind of violence and dangerous criminal activity that you are describing and preventing those bad actors from hijacking otherwise peaceful protests has been quick, prompt, robust partnerships between Federal,

State, and local law enforcement. And where all the partners have really worked together quickly all on the same page, all with the same mission, all aligned, it has usually been nipped in the bud, which has allowed both peaceful protests to continue, but it has also prevented dangerous violence from really fomenting and spreading.

Mr. CUCCINELLI. Yes, Senator, I would add that—first of all, I would double down on the Director’s comment about the necessity of State, local, and Federal cooperation. Where you see ready, smooth cooperation at the professional level—we are not talking about, mayors and city councils. We are talking about when they do not interfere with their police’s ability to interact with those of us at DOJ and DHS, that is where you see success. I would say in terms of tactics, it is a peace through strength approach. It is not that we want to engage in the battles. It is that we want to deter them and allow the peaceful protesting to go on peacefully. The way that has succeeded around the country over the last several months is where there is sufficient, responsible law enforcement in place, violence is deterred and peaceful protesting can continue.

I would just note this is overwhelmingly or largely in the hands of State and local authorities. We have limitations on our Federal jurisdictional authority, more so at DHS than DOJ, but we all respect our legal boundaries of authority. And that leads many people sometimes to be frustrated about why we might not be doing more in City X. We will take Portland. We have Federal facilities that we were addressing and protecting, and the people there, but there is no jurisdiction on the part of Homeland Security to police Portland in the way their police do, even though their police will not cooperate frequently with our officers, and the result is greater violence.

Senator ROMNEY. Thank you.

Mr. CUCCINELLI. Thank you for your concern.

Chairman JOHNSON. Thank you, Senator Romney.

Mr. Cuccinelli, just real quick, you sent me a video of a press conference with, I think, the chief of police of Chicago, a pretty disturbing video. If you could just quick describe that, I think this would be a good time to have you do that.

Mr. CUCCINELLI. So the video the Chairman is referring to is the July 20th press conference by Superintendent Brown, who is the police chief in Chicago. And you will recall when he had 49 officers injured during what amounted to an attack on a Christopher Columbus statue in that city. And that press conference, the first 14 minutes, is, in my view, the most clear and simple description—and he shows it to you. He just do not tell you; he shows you the video footage of the transformation of what clearly starts out as what looks like any other peaceful protest in any other city, literally marching down the street, police protection in front and back to take care of traffic.

And then it makes a left turn into the park, and they use drone footage. They show you people changing into the black block anonymous clothing. They show you people dropping bags worth of weapons to be used against the police. They show you the transformation of the PVC pipes used to hold the banner and pulling

those apart and then using those as weapons, the use of umbrellas. And it is truly one of the clearest examples and best explained that I have seen anywhere since these protests turned violent have happened this summer. It is the July 20th press conference by Superintendent Brown of Chicago, and I would urge anyone interested in this subject to pull it up on YouTube and watch it.

Chairman JOHNSON. Thank you, Mr. Cuccinelli. It certainly shows that in this case it was not spontaneous violence. This was well organized, well planned—

Mr. CUCCINELLI. Clearly planned ahead, yes.

Chairman JOHNSON [continuing]. Preplanned, and it was violent. Senator Rosen.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you, Mr. Chairman. Thanks to the Ranking Member. And thank you to all of you for being here today and for the important work that you and your teams do and the analysis that you are all engaging in.

Earlier this month, we know Americans learned from drafts of the 2020 DHS Threat Assessment that white supremacists present the greatest terror threat to our Nation. The earliest draft refers to white supremacist extremists, and I quote, “presenting the most lethal threat”; whereas, later drafts of the report softened the language on the white supremacist threat.

Mr. Cuccinelli, I was alarmed to see a whistleblower complaint from Brian Murphy at DHS alleging that you personally ordered him to “modify the section on white supremacy in a manner that made the threat appear less severe to ensure they matched up with the public comments by President Trump.”

Mr. Cuccinelli, do you agree with FBI Director Wray that the top threat we face from domestic violent extremes stem from racially and ethnically motivated violent extremists?

Mr. CUCCINELLI. I certainly think that the lethality analysis that you cited is correct. It has been the position of the Department of Homeland Security for some time. It has not been changed despite the implications of your question. And I continue to believe that that is true. And it is not a belief. It is just looking at the data. When white supremacists act as terrorists, more people per incident are killed. That is a higher lethality. That is what we are referring to.

Senator ROSEN. So then why the change between the earlier and most recent drafts to soften the language if you believe that that is true?

Mr. CUCCINELLI. But we have not softened the language, and you will see when the final report is out that what you are describing is still in our homeland threat assessment. So your concerns in that regard I can put to rest.

Senator ROSEN. Why did you order Mr. Murphy then to downplay the threat?

Mr. CUCCINELLI. Oh, I absolutely did not do that. That did not happen.

Senator ROSEN. So you do not have the metrics that you personally used to assess the intelligence products. Would you provide those that you would say that they are good or bad, how you as-

sessed the threats, and to be sure that we are not downplaying the threats?

Mr. CUCCINELLI. The metric used with respect to the subject you and I were just talking about is the number of deaths. It is a ratio, deaths per incident. And because that ratio is highest among domestic violent extremists, among white supremacist terrorists, as opposed to the other types that we face, that leads to the conclusion mathematically that they have the highest lethality, at least in recent years.

Senator ROSEN. I look forward to working with you and your team on trying to work on stopping those threats, to eliminate those threats, and keep our communities safer. But I do have another question for you while I have you here. I am disturbed—I guess that is a mild way to put it—by the allegations we have all heard about forced hysterectomies taking place in an U.S. Immigration and Customs Enforcement (ICE) facility in Georgia. These are assaults on women's bodies, and there must be accountability.

Have you gone down to visit the facility in Georgia? And if so, who was with you?

Mr. CUCCINELLI. Senator, I agree with you that those are shocking allegations, and as a result, I immediately dispatched a team from outside of ICE, including a doctor from the U.S. Coast Guard (USCG), an attorney, and one member of my staff who is a retired Army nurse as well to review the records in that facility. I am happy to report that at this stage—the Inspector General (IG) is still doing a more in-depth review, but at this stage the documentation indicates that there were, over the course of 4 years, two hysterectomies performed on two women, and that is confirmed by the nearby medical facility where those procedures take place. They came to the same numerical conclusion that we did. But as I said, the Inspector General is continuing to investigate that.

I should also add that one of the lawyers that filed a complaint last Friday was reported by the Associated Press (AP) as indicating that they had not actually talked to anyone who had a hysterectomy, but that they wanted the Department to investigate the subject, which is not, of course, a legitimate basis to bring a complaint. But that was learned after the fact.

Senator ROSEN. Thank you. I appreciate that. But you did not answer the question. Did you go down to Georgia yourself with that team, sir?

Mr. CUCCINELLI. No, I did not go with that team. I dispatched that team to go literally within a day or two of the allegation—

Senator ROSEN. So you have not been there for yourself. That is all I am asking.

Mr. CUCCINELLI. I have not been to that facility.

Senator ROSEN. Thank you.

I would like to move on to Director Miller and talk a little bit about Iran quickly in the time we have left. In your testimony, you noted that Iran has the ability to employ and support terrorism within the United States. You also stated that Hezbollah has extended its reach into the United States in recent years. For instance, as recently as 2018, two Iranians were arrested in the United States for surveiling Iranian activists and Jewish groups and passing the information back to Iran. So can you please outline

for us the threat to the homeland from Iran and its terrorist proxy Hezbollah?

Mr. MILLER. Yes, thank you, Senator, for that great question of great concern. As we all know, Iran is the greatest State sponsor of terror in the world and continues to plot against America all the time, almost as it is part of their strategic calculus and I am greatly concerned by their continued ambition as well as aggressiveness, and it is something that, of course, all three of us at this table look at probably several times a day, and our men and women are on point on this, but absolutely of concern. But at this point, a lot of times the Iranian bark is louder than the bite, and we want to keep it that way, but it is still obviously one of our principal threats.

Senator ROSEN. Thank you. I look forward to working with you to find out what Congress can do to improve interagency collaboration to keep Iran's bark worse than its bite, particularly when it comes to homeland threats.

Thank you, Mr. Chairman. I yield back.

Chairman JOHNSON. Thank you, Senator Rosen. Senator Scott.

OPENING STATEMENT OF SENATOR SCOTT

Senator SCOTT. Thank you, Chairman Johnson, for hosting this today. I want to thank each of our witnesses here today for what you do. I want to particularly thank Director Wray for his efforts after Parkland, and I had a great trip to, I guess it is called, the "Tip Center." And it is a wonderful group of people that are working hard to make sure with a lot of tips, how to figure out how to make sure things get directed down to the right person. And then I also want to thank Director Wray for his efforts after the Pensacola shooting to keep us informed and try to figure out how we make sure something like that does not happen again. So I want to thank all the individuals working at the FBI for their hard work.

It is disgusting, what has been going on with law enforcement, how law enforcement has been treated and, the insults they are taking, the things that are thrown at them, and it is just disgusting. It reminds me of what happened to people that were coming back from Vietnam and they were treated disgustingly. They are not the ones who chose to go. They chose to defend the freedom of this country, and they followed the orders that they were given.

So last week, I did a resolution on the Senate floor supporting the men and women of law enforcement, and it shocked me but the members of the Democrat Party decided to block it. I just cannot imagine that just a simple resolution to support the members of law enforcement would not get supported by everybody in this country, especially in the U.S. Senate.

What are you all doing to—or how does that impact the morale of the people in law enforcement when you see how badly law enforcement is treated? And what are you all doing to make sure that the members of law enforcement that you work with, and others, are safe?

Mr. WRAY. Senator, I appreciate both your comments about the FBI and even more in some ways your concern about the men and women of law enforcement around this country. I will say that this

is personal for me and personal for us at the FBI. All of these State and local law enforcement departments that we are talking about have members on our task forces, and we work with them every day. I will tell you that the rate of violence, including felonious lethal violence, against law enforcement is up significantly this year from last year. And when I say it is personal, I mean that in a different sense as well, which is one of the things I started doing when I became Director was that I decided I was going to call every time an officer was killed in the line of duty, shot and killed, or killed by an adversary, I was going to call the chief or sheriff myself. My staff gives me a picture of the dead officer, a description of his family, and I call the chief or the sheriff, and we have a conversation, and I express my condolences. I will tell you that I have had to make way too many of those calls, and, in fact, in late August, early September of this year, in about one 15-day period, I had to make seven of those calls. That is basically one every other day.

Each one of those officers was a son or a daughter or a mother or father, beloved family members, community members, and all they do is get out and try to serve the public. And sometimes I scratch my head at why more people cannot appreciate how special it is for somebody to be willing to get up every morning and put his life on the line or her life on the line for a complete stranger. To do it once is extraordinary, but to get up and do that for a living day after day after day after day. And when you pack on top of that the impact of COVID on law enforcement, I think there are close to 90 law enforcement officers around this country who die as a result of COVID. I mean, you put all those things—partly because they are out there protecting the public, so they are more at risk. And it breaks my heart.

Senator SCOTT. Director Miller, how does it make you feel when you see how badly law enforcement is being treated right now? And what are you doing to make sure people are safe?

Mr. MILLER. My father was a career law enforcement officer. Of course, in my current capacity I am focused on international terrorism, but as a citizen and as a son of a father who dedicated his career, I am also incredibly humbled by the commitment and the selfless service of our law enforcement men and women.

Senator SCOTT. Mr. Cuccinelli.

Mr. CUCCINELLI. Senator, DHS has more law enforcement officers than any other entity in the country, and so we take your question very seriously. And it is certainly something that we talk about in the leadership, maintaining that morale. They are doing something, as the Director described, that no one else in America is asked to do. There is nobody else in this country we ask to get up every morning, put on a gun, with the possibility of them using it, to stand between us and evil. And there are no real signs that evil is going away, so we are going to keep needing these folks.

I think back to George Washington's descriptions of veterans: your ability to recruit your next round of troops—I am paraphrasing, of course—is going to be heavily dependent on how they see your treatment of the last round of troops, the veterans, of course, for him coming out of the Revolutionary War. And the same is true for our police officers. They deserve our respect in a way

that very few other people in our society do. And what we have found is that while the public discussion can be very rough and tumble, I will describe it, they respond very positively when they see leadership in their department going out and affirmatively defending them and taking the position you just described. So I know they appreciate it when they see you do it. I know they appreciate it when they see those of us in leadership at DHS do it, because they tell us that. It really does matter a lot that you all in this body pay them the respect they are due. I am sorry the resolution played out the way it did. I am as shocked as you are just based on the subject matter. But it is very important that you all use your leadership to encourage law enforcement all across the country.

Senator SCOTT. By the way, thanks for reaching out. We had 51 members of law enforcement die in the line of duty in my years as Governor, and I had the opportunity—I went to all their funerals, and you get to meet their families, and, almost all of them seemed to have young kids, and your heart goes out to them. So thank you to each of you for what you are doing, and please let anybody you come in contact with with regard to law enforcement know how much we appreciate them.

Thank you.

Chairman JOHNSON. Thank you, Senator Scott. Senator Paul.

OPENING STATEMENT OF SENATOR PAUL

Senator PAUL. I would like to begin by wishing a speedy recovery to the two police officers in Louisville who were shot yesterday in the line of duty. I join Senator Scott and others in saying that we have to appreciate our police more generally. They are protecting us from the vandals, the marauders, the arsonists in our cities. It is not just the Democrat proposition of defunding the police that threatens us. It is also the idea that if we do not appreciate our police, we will not have more volunteering to become policemen in the next generation. So I think it is absolutely imperative that we do show our appreciation for these people who are risking their lives to keep us safe.

My wife and I know about this personally, as you saw from the video going into this. We were attacked by a mob in D.C. just a few weeks ago. For those of you who doubt that the mob had violent intent, immediately after we were safely in the hotel, or somewhat safe in our hotel, one of the police officers was assaulted and received stitches in his face. I guess what bothered me is, I commend them for their heroism, and I truly believe they saved our lives. But the person who assaulted the policemen was from out of State. I think Federal charges were lodged, but then he was released on his own recognizance. I tweeted out, somewhat snarkily, “If you are looking for him, you may look in Kenosha.” But I think we do have to investigate these people and we have to put blame where blame is. We need to find out who is financing them. If you are from out of State and you attack someone in D.C., I would think that the FBI or Federal authorities should investigate: How did he get there? Who is paying for it?

I can tell you that Black Lives Matter is supporting these folks and that we should not shy away from attributing blame where

blame goes. When we were attacked, the head of Black Lives Matter in Louisville had this to say. She said, "We can see the fear in their faces, and that is how we want them to live." Their goal is terrorism. They are admitting it.

If you look at their exchanges online in social media, they are saying their goal is to terrorize public officials and really anybody. Many of the people in the restaurants that are being terrorized are not public officials, but their goal is terror.

Now, whether or not that equates to something that you can legally investigate, I do not know. But we should know that, and we should let corporate America know that. Corporate America is giving millions of dollars to something they perceive as an antiracist group. In reality, it is a group that is funding terror and funding terrorists to go from city to city.

I do not think probably anyone can comment directly on the police officer that was assaulted that was protecting my wife and I, but I guess in general, Director Wray, does a police officer being attacked by someone who came from another State, do you think that can fall under the purview of the FBI? Is the FBI in general investigating cases like this where people from out of State are doing something? You would think it would be a local crime to be investigated, but if they are from out of State, is there a Federal angle to an investigation?

Mr. WRAY. Senator, first let me say I appreciate your sympathy and appreciation to that officer, and while we are pleased that the offender was charged, obviously the release is concerning.

I would say that when it comes to interstate travel, there are sometimes Federal charges that we can bring, so there are Federal rioting charges that have an interstate nexus that we have started trying to use around the country where we can. And there are a variety of sort of interstate commerce type hooks that we can look to. We are aggressively looking for a lot of the same kinds of things that you are pointing to: funding, supply chains, networks, communications with others in different parts of the country. Certainly the interstate travelers are often some of the most serious offenders. I know that in Portland, for example, there were a couple of individuals that I can think of off the top of my head who were coming from a different State, who were in one case threatening to blow up a building, in another case attempting to attack a building, and charges were brought in both of those instances.

So wherever we can find a tool or a legally available weapon to go after those people, we are going to use it, because while there are certainly a large number, even a majority of people who are out there protesting peaceful, it does not take very many, as you experienced, you and your wife, in the really shocking video that was played, it does not take very many people to suddenly cause very serious harm.

Senator PAUL. I think the frustration is that there is one guy on the Internet who—I think he has been arrested 26 times, and there has to be some sort of cumulative nature to that many crimes that we have to be at some point able to hold them. I do think re-arresting is a good idea. If I were in Portland, I would arrest them all every night, the ones that are committing infractions. It is not life in prison, but you should get 24 hours in a cell and a trial or a

hearing the next day and be booked. But we have to do something. I think the lack of doing anything is encourage more of this.

The people who were in the mob that attacked us, within like—how the Internet works. Within 20 minutes, people were isolating their faces and saying, “Here is a picture of him in Louisville,” “Here is a picture of him in Memphis,” “Here is a picture of him in Portland.” So there is some connection, and it costs money to travel places, and there were dozens staying in hotels near the White House that average over \$500 a night. So I think it is important that we look at it.

Now, I am very concerned about free speech and not going after groups for speech. I actually sympathize with some of the reforms. I had an act called the “Breonna Taylor Act” to get rid of no-knock raids because I think they endanger police officers and people behind on the raids. And many police officers actually agree that the no-knock raids may not be necessary. But at the same time, if the trail leads to Black Lives Matter, there is an important public service to the corporations who think they are giving money to a peaceful protest or to a peaceful antiracial group, they need to be aware if they are being flown around. So there is an important, I think, call to not having more money flood into a group if that is what is happening.

And so all I would say is that we should not be afraid of allegations that this is just a peaceful group so we cannot touch them, that we do need to trace the money from people who are committing crimes. If it is coming from an organization that may have multipurposes and say they have a First Amendment right, they do not have a right to fund mayhem. I hope it will be pursued, and feel free to respond to that or not.

Mr. WRAY. Thank you, Senator. Just two quick points. One, I could not agree more on the repeat offender aspect of it, and one of the things that we are doing in Portland and in other places is trying to work with our State and local partners to essentially identify who is it who is just going in and out of the State and local system, either because they are getting released on bail, otherwise, and see—prioritize those individuals to see if there is some Federal charge, because often that can result in detention and more stiff sentences.

And then on the funding piece, following the money is kind of our bread and butter. It is something we are looking at, as I said, including—which I think goes a little bit to your last point, including situations where somebody might be misrepresenting what it is they are fundraising for, right? So certain crowdsourcing activities where somebody contributes thinking they are giving for something that is First Amendment activity, but, in fact, it may be being used for something else that is much more pernicious. And so we are looking at that, too.

Senator PAUL. Just one quick final comment. The people who are being hurt the worst are the people who live in these communities. So the people who say, “I want to help people in the poor sections of Chicago or the poor sections of D.C.,” need to realize when you burn down the last pharmacy, when you burn down the last McDonald’s or Walmart, it hurts the people who live there and many of these businesses will not get back. And that cannot be em-

phasized enough from a humanitarian point of view. We have to end the violence because you are hurting the very people you think you are trying to help.

Thank you.

Chairman JOHNSON. Thank you, Senator Paul. I really do appreciate your comments, and I really am sorry that you and your wife had to endure that type of abuse. Senator Portman.

OPENING STATEMENT OF SENATOR PORTMAN

Senator PORTMAN. Thank you, Mr. Chairman. As we have seen today, our annual discussion about the threats to the homeland is full of threats. It is a busy time for all of you, and I want to start by thanking the men and women who work for you, and I hope you will pass along our respect and support for them. We rely on them, as Senator Paul has just indicated, to keep us all safe and keep our communities safe, and at the State and local level, but also the people who you represent here today.

We have a lot of threats. We are in the middle of a Presidential election, and there are, foreign actors trying to intervene in our election again. That is a threat. We are experiencing these protests in the wake of the tragic deaths of George Floyd, Breonna Taylor, and other events. As I have repeated many times, of course, I support people's right to protest peacefully. It is protected by our Constitution. I also support police reform, and it was discussed earlier that some things have been blocked around here. We actually had a police reform bill that was very common-sense and had a lot of provisions that were appealing on a bipartisan basis. It was blocked even from consideration by the other side. Now, I think that is cynical, and I think we should have had that debate and discussion, and we should have passed something, including some ideas that Senator Paul just talked about.

But I got to tell you, the riots and particularly the damage to our communities, the arson, the looting, the desecration of property—by the way, when I say “our communities,” often these are communities of color, and nothing upsets me more than seeing the entrepreneur in one of these communities, like the African American guy in Ohio or the Hispanic woman I have seen in other news broadcast who says, “I spent my life building this business, and now it has been destroyed.” And, of course, the harm to individuals, to citizens, and particularly the violence against Federal, State, and local officers.

Director Wray said it was heartbreaking, and I think that is a good way to put it. These people are doing their job. By the way, they get paid very little compared to what a lot of people are getting paid around this place or, frankly, even some of the demonstrators who are assaulting them. Taking out their frustrations on these guys is not fair. It is unacceptable.

I want to again express my condolences for Dave Underwood. He was one of yours, DHS Protective Service officer who was killed while trying to protect the courthouse in Oakland, California. Three hundred injuries, we heard today, over 300 injuries have been sustained in Portland. Of course, we wish all those officers a speedy recovery, including getting their sight back and their hearing back. It was just discussed that two officers were shot last

night, and these two officers, of course, we all wish them a speedy recovery. But to their families—you talk about trying to recruit people into this business. Wow, I wonder what their families think about that.

I actually was with a family recently—it was 2 weeks ago. I was in Cleveland, Ohio, at a visitation for Officer Jimmy Skernivitz, and Jimmy was one of your guys in a way. Officer Skernivitz was working with the FBI and working with State and local law enforcement, a Cleveland police detective on a violent crime task force, Operation Legend. He was gunned down in his car by three teenagers, unprovoked, just gunned down in his car. And his family was incredible. They were so courageous in response to this and so committed to the notion that Jimmy died in service to his country, which is exactly what he wanted to do in life. And God bless them, it is like talking to the families of our military who have fallen. But this violence must stop. This, too, is a threat to our homeland.

We have talked today, as Director Miller has said, that the terrorist groups al-Qaeda, ISIS, and others continue on the attack. That is a threat. We cannot forget. We cannot take our eye off the ball. As we have heard from CISA here in this Committee consistently, these cyber attacks are on the rise. By the way, this Committee is focused on that a lot and will continue to. We did a Permanent Subcommittee on Investigations (PSI) recently about this issue, and I think, as you know, Deputy Secretary Cuccinelli, I am very concerned about the Federal Information Security Management Act of 2002 (FISMA) implementation at some of our Federal agencies. They are just not doing it. They are not protecting themselves, which means they are not protecting the taxpayers, not protecting the government. And we are going to have some legislation on that, but we have to work together to put the firewalls in place more effectively.

I am going to ask about three specific threats quickly, the first of which is these transnational terror groups that are shipping poison into our communities, and they keep doing it, and it has increased. I am pleased that 4 million pounds of hard drugs have been recently apprehended, crystal meth, heroin, cocaine, and so on. I do believe that the ultimate answer to this issue lies on the demand side, and we have done a lot here. We have spent over \$5 billion of additional Federal money just in the last few years on prevention, on treatment, services, on longer-term recovery, and we have to keep that up. Unfortunately, we have seen a reversal during the COVID period the last several months on overdoses and overdose deaths after finally getting to the point where we were making progress on that, a 20-percent reduction in Ohio in 2018 of overdose deaths after three decades of increases. But now we are going the other way. So we have to deal with the supply side, too, because when it flows into this country, this poison, it is cheaper. It is more accessible.

I want to focus just for a second on fentanyl. We know it mostly comes from China. We know it mostly comes by the mail. The Synthetics Trafficking and Overdose Prevention (STOP) Act, you all worked with us on that legislation. We got it passed. It is supposed to keep this stuff from coming in from China. Just quickly, how do you think it is working? And I know on either side of the panel

here we have a lot of experience with the STOP Act. How is it working from a Customs and Border Protection (CBP) point of view and from an FBI point of view?

Mr. CUCCINELLI. From a CBP point of view, they have started aggressively pursuing small package inspections at a level that we have not done before, and that has proven fruitful. Of course, our adversaries adjust. They tend to be adjusting by going through Mexico. That is their path of adjustment that we are observing. But we are going to keep up the pressure in that space. If for no other reason it is like my comments earlier about driving people to the ports of entry. If we can minimize their opportunity points, we can focus our efforts, all of us together, on those avenues of approach that we know they are using. And we do need the help of this body to continue that effort, and I know that the commitment is there. I know especially on this sort of particular issue, Senator, you have been very strong for a long time, and we very much appreciate that at DHS.

Senator PORTMAN. Let us get the STOP Act in place. I think you are absolutely right. And it is not coming by mail from Mexico, as I understand it—

Mr. CUCCINELLI. Right.

Senator PORTMAN [continuing]. As much as it is coming over land, although it is some of both, so the STOP Act helped there, too. I know I am getting close to—over my time, but, Mr. Chairman, I do not know if you would not mind giving me a chance just quickly to ask about the two other threats, and we will get back to you, Director Wray, in writing, if that is OK.

One is safeguarding our research, and I love what you said about the greatest transfer of wealth in the history of the world. This threat from China and other countries who have systematically targeted our research and the most promising researchers is a threat to the homeland. It really is. I guess what I would say is with this new legislation that came out of this Committee, the Chairman marked it up, it has gone to the floor in the sense it is part of a proposal by Senator McConnell, Safeguarding American Innovation Act. Would that help you, Director Wray, to do your job? You say you have opened every 10 hours another China-related investigation, 2,500 open investigations. This, as you know, provides you a new criminal fraud charge under Title 18. Would that give you the tools and help you to be able to protect the homeland from this threat?

Mr. WRAY. Senator, I very much appreciate the legislation. We do think it will help. I want to just underscore some of the points that you have made there. From our perspective—and I have said this repeatedly and publicly since pretty early in my tenure as FBI Director—there is no adversary that presents a broader and more comprehensive threats to our democratic ideas, our innovation, our economic security than the Government of China. We are up about 1,300 percent in terms of economic espionage investigations that tie back to China over the past decade, 2,000-plus active investigations tied back to the Government of China, by far the biggest chunk of our counterintelligence portfolio. China sees itself on the issues that you are raising in terms of research as engaged in an international talent war, and so we have this perverse phenomenon

where you have essentially a pipeline of U.S. technology, intellectual property, and research back to China for their nationalistic purposes, essentially misappropriating U.S. taxpayer dollars in the process.

I appreciate the leadership you have shown through legislation and otherwise on this topic. We are trying to tackle it through investigations. I think we have had about a Talent Plan arrest a month almost this year. It covers almost every region of the country. We are also very concerned about China's military-civil fusion policy where essentially they overtly are focused on channeling even what might appear to be civilian research intellectual property and innovation back to advance their military aims. And as one illustration of that, as certain Members of this Committee may know, we have now recently started discovering People's Liberation Army (PLA) researchers here in this country who were concealing—

Senator PORTMAN. People's Liberation Army.

Mr. WRAY [continuing]. Their ties back to the PLA. And so that is a real concern as well. So this is a major issue, and it is our highest counterintelligence priority for a reason, because it is going to shape what this country is like in 25 or 30 years.

Senator PORTMAN. My time has expired, and I appreciate your indulgence, Mr. Chairman. Let me just say this: Your personal commitment to this is very much appreciated, and it was not always so at the FBI. As you know, when we had our hearing after our year-long investigation, it was shocking what we learned, and the FBI, to their credit, testified and said basically, "We have been asleep at the switch on this for a while, two decades, and we need to increase what we are doing in terms of prosecutions and investigations," and, boy, they have. So DOJ and FBI have really stepped up, and, unfortunately, it is absolutely necessary.

So my last question for you, Mr. Cuccinelli, was about the Non-profit Security Grant Program. I am going to follow up with you in writing about that. We appreciate the additional funding. We think it is working. We have some good experience back home with groups that are not just getting the funding but they are getting your expertise. They are getting the best practices. They are getting the professional help as to how to protect themselves. These are synagogues and churches and mosques, and pushing back against the domestic terrorism threat, including Islamic extremists and white supremacists. So we thank you for your support of that program. We hope we continue. I know you have a new grant program you are looking at that we will follow up with.

With that, thank you, gentleman, very much. And thank you, Mr. Chairman, for your indulgence.

Chairman JOHNSON. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you very much. I want to say while Senator Portman is still in the room, the legislation he referred to as bipartisan legislation, he and I are the co-authors, and I want to second his sentiments with respect to the good work the FBI is doing in support of our efforts. This is legislation that should be before the Senate, should be debated before the Senate, and we

should have the opportunity to see this signed into law. I just wanted that to be on the record.

Senator PORTMAN. Well said. Thank you.

Senator CARPER. I want to begin my questioning, Mr. Chairman and colleagues, and let me just say to our witnesses thank you for being here, thank you for the work that you do. Thank you very much for the work that the people you lead do for all of us every single day.

Before I ask a question, though, I just want to take maybe a minute to address yesterday's developments in Louisville, Kentucky. My sister lives in Winchester, Kentucky, not all that far from Louisville, so this is personal for our family.

Yesterday we learned that no one has been charged in connection with Breonna Taylor's death, and we need to know why. Breonna Taylor's family needs to know why. Meanwhile, all of us need to remember the words of Breonna Taylor's mother from earlier this summer, and here are her words: "This is so much bigger than her, but we cannot get justice with violence. It does not make sense. It does not help. It does not help her. It does not help us."

She goes on to say, "It does not help the world we live in. You cannot fight violence with violence." The words of Breonna Taylor's Mom.

Add to her words the words just yesterday of our former Vice President, Joe Biden. He said, "Violence is never and can never be the answer." "Violence is never and can never be the answer."

And as we seek the whole truth in the death of Breonna Taylor, we must not sully her memory by perpetrating the same violence that took her from her family.

Meanwhile, I would ask that all of us pray for the two police officers who were shot last night in Louisville, as we pray for Breonna Taylor's family and especially her Mom.

Now, I want to turn to domestic terrorism, if I can, and this will be a question for Director Wray. Director Wray, tragically, in recent years we have seen an increase in targeted violence, especially gun violence, perpetrated in this country, as you know better than any of us. You may have heard me say that in order to address the problem, we need to address not just symptoms of the problems but the root causes of those problems.

When I was privileged to lead this Committee as its Chairman, I worked with then-Secretary of the Department of Homeland Security Jeh Johnson to ensure that the Department had the needed resources to address the root causes of violent extremism through its Office of Community Partnerships (OCP).

Director Wray, two questions, if you will. Why have we seen such a rise in racially and ethnically motivated extremism and violence in this country in recent years? Why?

Mr. WRAY. Senator, I appreciate your concerns, and I share many of those concerns. I guess I would say the why is something that we all struggle to really get our arms around. I think one important part of that phenomenon, which I referred to earlier, is the role of social media. As I said, terrorism today now moves at the speed of social media. And so, in effect, what you have is a phenomenon where disaffected, angry, hateful people who are maybe separated geographically and maybe are largely lone actors are

now able to essentially spin each other up by being virtually connected in a way that they could not before. And the more of that that occurs through encrypted messaging platforms and places like that as well, the more of that I think we can expect to see, unfortunately and tragically.

The angry person who wants to lash out, who is living at home in Mom's basement, maybe before was all by himself. Now he is talking to similarly situated people all over the country and, indeed, all over the world and is more likely to get encouraged and galvanized and to take hateful and abhorrent ideas and turn them into dangerous, all too often lethal violence.

Senator CARPER. Thank you very much. When my sister and I were kids growing up—we grew up in Danville, Virginia, the last capital of the Confederacy, and I remember taking a school trip. My whole seventh grade class went to Richmond, and we had the opportunity to actually meet the Governor of Virginia when we were like 12 years old. It was an amazing experience, one I will never forget.

A couple of years ago there was a demonstration. There was violence in Richmond, Virginia, as you will recall. We had people there that were folks from the Ku Klux Klan (KKK), people who were instigating racial violence. Death occurred. And the President, our President, was asked to comment, and he said, "There are good people on both sides."

I would suggest that words like that from our President give courage and strength to racial extremists to act out and to be not just vocal but actually to embrace violence. And that is something that needs to stop.

Let me ask, how is the FBI working to ensure that when you come, Director Wray, when you come before this Committee next year, the threat from domestic extremists is reduced? And how can Congress be helpful in that regard? Make us a guided missile.

Mr. WRAY. Senator, I think a few things. How are we working? We have asked all of our Joint Terrorism Task Forces (JTTF), which means that we are able to leverage not just FBI personnel but, essentially 4,500 investigators around the country, to make sure that they are focusing on domestic terrorism in addition to international terrorism. They were already doing that, but one of the things that we did just recently was elevate racially motivated violent extremism to the same national threat priority band as ISIS and homegrown violent extremists, who are the folks here who are inspired by foreign terrorist organizations.

I created a Domestic Terrorism Hate Crimes Fusion Cell, which brings together the expertise of both our domestic terrorism investigators and analysts with our hate crimes investigators and analysts, and that is designed to make sure that we are getting the synergies that are necessary there. We have already made significant progress there, the first time that I can think of where we were able to proactively disrupt an attack using a hate crime charge involving the attempt to attack a synagogue in Colorado that I referenced earlier.

Certainly we need agents, analysts, we need data analytic tools, and we ultimately are going to need a solution to the end-to-end encryption problem which plagues law enforcement on an increas-

ingly constant basis. And so there are a number of things that we would potentially turn to Congress for help with there.

Senator CARPER. Thanks. Mr. Chairman, I have one last question. Can you indulge me for about 2 more minutes?

Chairman JOHNSON. OK.

Senator CARPER. Thanks very much.

Mr. Wray, can you give us some examples of what Russia, China, and Iran have been doing to spread disinformation and misinformation ahead of the election? How does the Bureau work to proactively combat this misinformation?

Mr. WRAY. I would refer you to the Office of the Director of National Intelligence (ODNI's) public statement that is the unclassified version of what the intelligence community assesses from our foreign adversaries with respect to election interference, and it goes through a description of China, Russia, and Iran. All three countries are highly sophisticated actors with different capabilities pursuing different means—in the case of the Russians and the Iranians, heavy use of online tools, for example. You have heard about the use of social media. We are seeing online journals, fake placement of stories, things like that, use of proxies by the Russians, for example.

On the Chinese, as I mentioned before, in many ways it is our greatest counterintelligence threat to this country, and their malign foreign influence efforts are different, as Mr. Cuccinelli said, different from the Russians, but much broader and wider in terms of their reach to not just Federal officials but State and local officials. They use economic levers very heavily. We are mostly concerned about subversive, undeclared, coercive, or criminal means. There is obviously all kinds of overt lobbying that occurs by these countries, but those are the means that we are most concerned about.

Senator CARPER. Thank you. Of the three countries, Director Wray, which poses the biggest threat to the upcoming election versus the longer term? Which of the three countries—Russia, China, and Iran—which poses the biggest threat to the sanctity of this upcoming election?

Mr. WRAY. I do not think I could really rank them. I mean, all three are ones that we are very concerned about in different ways. So it is not really an apple-to-apple comparison.

Certainly, as I have said before, the Russians are engaging—and as the ODNI's statement on behalf of the intelligence community says, they are engaged in a range of measures. But also the Chinese have recently been expanding their influence efforts, which is part of why after the midterm elections, with the Foreign Influence Task Force that I created early in my tenure, we broadened and significantly added resources to that task force to add not just Russia but to add China and Iran as well, because those countries are very much looking for different ways to take a page out of the malign foreign influence playbook that they have seen elsewhere.

Senator CRAPO. Director Wray, thank you so much. Our thanks to all of our witnesses.

Mr. Chairman, thank you for your generosity with an extra 3 minutes and 39 seconds. Thank you.

Chairman JOHNSON. Senator Hawley.

OPENING STATEMENT OF SENATOR HAWLEY

Senator HAWLEY. Thank you, Mr. Chairman. Thank you, Director and the other witnesses, for being here.

Let me just pick up on something that you testified to earlier, Director Wray. You talked about evidence of organized tactical activity by some groups as part of the recent rioting and violent looting that we have seen across the country. In Louisville, of course, last night, we saw egregious acts of violence, two police officers shot. I have seen this in my own State. We have had nine police officers—nine—shot in St. Louis, in that city alone, since June, just since the month of June.

There appears to be some footage that is circulating on the Internet from Louisville last night that shows a parked U-Haul waiting for a crowd and which it looks like contains signs that say things like, “Abolish the Police,” along with shields and perhaps other paraphernalia that can be used for violence.

I understand the FBI is going to assist in investigating the shootings that happened in Louisville, but I want to ask you to what extent are you investigating coordination between extremist elements in the violence that we have seen across the country.

Mr. WRAY. Senator, I appreciate the question. As you anticipate in it, we are very focused on what we would call the most dangerous actors, which tend to be the ones who are most coordinated and, therefore, potentially able to cause the most harm and most damage. So we are looking in a number of places. Without reference to any specific investigation, we are aggressively investigating funding streams, tactics, logistics, travel, networks, that kind of thing.

What we are finding is that a lot of the activity is organized at what I would call more of a tactical level than a strategic level and organized more locally and regionally in small groups or nodes than in a more structured, hierarchical way across the country. But that in no way diminishes how serious and dangerous it is. We do not view how nationally organized something is as a proxy for how dangerous it is, and so we are aggressively investigating all the kinds of things that you would expect us to be investigating in pretty much every State in the country right now.

Senator HAWLEY. These local and regional nodes are, is it safe to say, using social media as a means to communicate with each other as they plan their activities?

Mr. WRAY. They are, but let me just add a finer point on that. We see a lot of communication on social media in what I would call sort of more benign ways, but a lot of the communication with each other that is the more telltale or revealing is happening locally, sometimes through encrypted channels that they think will cause them to be able to hide from law enforcement, and in some cases they are able to hide from law enforcement, which is a real frustration. But we are taking steps to try to make sure that we can break through some of those barriers and try to uncover some of the stronger evidence of what we are seeing reports of around the country.

Senator HAWLEY. Thank you for your attention to this, and I certainly hope that you continue to devote every resource that you can to these investigations, to the potential coordination here, and es-

pecially for violence that is being directed against law enforcement, whether it is in Louisville, whether it is in St. Louis, whether it is in Seattle, Portland, wherever, it does not matter. Law enforcement, when they are under attack in what appears to be in some instances, again, a coordinated fashion, particularly, of course, if it crosses State lines and is coordinated across State lines, then I think it deserves your attention, and I am glad that you are giving attention to that.

Let me switch gears and ask you a little bit about Chinese espionage and COVID. In May of this year, you released a public warning that organizations researching COVID-19 with an eye towards the vaccine, you released a warning about possible Chinese espionage activity related to the pharmaceutical research, health research, and ultimately vaccine development. Can you give us a sense here, are Chinese hackers still trying to steal research related to a COVID-19 vaccine? What is the latest that you know?

Mr. WRAY. Certainly, as you reference, we are seeing very aggressive activity by the Chinese and in some cases by others to target our COVID-related research, whether it is vaccines, treatments, testing technology, et cetera. Sometimes you can almost—without being too descriptive in an open setting, we can almost see, track like a news report from some company or research institution that is announcing or revealing some progress, because, of course, a lot of this is getting discussed in the media, and then almost within days, we will see cyber targeting that ties back to Chinese actors focusing on those institutions. And so that is why we, working with DHS, thought it was so important to put out information.

We are also engaging, as the FBI does all the time, directly with targeted organizations, victims, institutional victims, to help them better protect themselves. But the Chinese cyber threat is a major concern and something that we are prioritizing through our National Cyber Investigative Joint Task Force, which brings together intelligence community and law enforcement assets to try to take a whole-of-government response to this.

Senator HAWLEY. Give me your sense of what you are seeing in terms of the hacking activity and the espionage activity. Is it directed toward end product, is your sense? Or do you get any sense that hackers or other agents of China, the Chinese Government, are trying to disrupt the research itself, interfere with the development of either the collection of data or a vaccine?

Mr. WRAY. I am trying to think of the best way to summarize what we are seeing. I guess what I would say is it is clearly targeting the former, that is, targeting information about progress in much the same way, the same playbook that we are seeing from Chinese hackers across other kinds of industries and research and innovation. Rather than innovate themselves, they are trying to essentially jump to the front of the line by stealing information from others.

Senator HAWLEY. Thank you again for your work on this and your continued attention to what it is obviously a vital national security interest of this Nation.

A final question here just as I go. What about connection to the Chinese Government? We have been talking about Chinese hackers, Chinese espionage. Have you seen any clear connection or how

much clear connection have you seen to the Beijing Government itself in these efforts?

Mr. WRAY. Of course, what you are raising there is the very important question of attribution, and the standards that the intelligence community uses for attribution are different than, say, maybe the private sector might use. But as I sometimes say, nothing says attribution like an indictment. As you know, we have brought some significant indictments against Chinese hackers that do tie back to the Ministry of State Security (MSS) specifically on a number of occasions, and these are targeting not just American companies, American research institutions, but also similar institutions among some of our closest allies, and targeting personally identifiable information (PII), of Americans. Chinese hackers have essentially stolen the PII of about half the adult population of the United States.

Senator HAWLEY. That is a shocking number. Thank you for your work on this.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator Hawley
I believe Senator Sinema is——

OPENING STATEMENT OF SENATOR SINEMA

Senator SINEMA. Yes, that is right. Thank you, Mr. Chairman. I appreciate our witnesses joining us today for this important hearing.

As a Senator from a border State, I know it is critical that we work together to tackle threats against the homeland and along our Nation's borders. I remain committed to working every day in a bipartisan fashion to secure Arizona's border, keep Arizonans safe, and ensure that migrants are treated humanely and fairly. A key part of this overall effort is successfully tackling the challenge at our Nation's ports of entry.

My first question is for Mr. Cuccinelli. Arizona ports of entry are among the busiest in the Nation, and the goods and people flowing through them play critical roles in both Arizona's and the Nation's economy. CBP employees work hard every day to facilitate the flow of lawful trade and travel, but our Nation continues to struggle with significant amounts of illicit drugs entering our Nation through our ports.

With a month yet to go in fiscal year (FY) 2020, CBP is reporting they have already seized more marijuana, methamphetamine, and fentanyl at ports of entry than they did in 2019. So I strongly believe that technology is part of the answer here, which is why I worked with Senator Cornyn to introduce the Southwest Border Security Technology Improvement Act to improve DHS technology planning.

But I want to get your take on this challenge. What actions does DHS need to take now at our ports of entry to better respond to the ongoing threat this flow of drugs represents?

Mr. CUCCINELLI. Thank you, Senator, and zeroing in on your question on the ports of entry, the most important program running is the nonintrusive inspection effort. As I mentioned earlier, one of the advantages of the expanded security along the border, including the building of the border wall, is that we are funneling

more traffic from between ports of entry into ports of entry, and that means that we are able to confront these threats on our terms and on our turf. It does not mean they are not dangerous. It does not mean there are not a lot of them. But we have had great success in the last 4 years in seizing hard drugs, the ones that do the most harm in the most communities in your State, in every State, of course. We have seen great success in that area, as I said in my opening remarks. But we will do better still as we expand the availability of nonintrusive inspection ability.

And you mentioned how busy the ports in Arizona are. You are absolutely correct. One of the beauties of this particular technology—and I know it is part of why you support adding technology to the suite of problem-solving tools—is that it increases the efficiency of the port itself. It operates in such a way that does not require as much manpower or time to accomplish the same security goals. That is the very definition of increasing efficiency.

So we are also using nearby—not in Arizona yet, but hopefully to come soon—more autonomous surveillance around ports of entry to provide greater situational awareness and security to not just our employees but everybody coming through those ports of entry as well. So I look forward to expanding those efforts in the future, and your help and cooperation and support of that is much appreciated.

Senator SINEMA. Thank you.

For my next question, I would like to ask both Mr. Cuccinelli and Director Wray to weigh in. The entities behind these drugs are transnational criminal organizations. After the TCOs move their contraband through our ports, they launder their profits, and recent media reports indicate that TCOs have been able to use major banking institutions for money-laundering purposes.

So what additional steps do DHS and the FBI need to take together and separately to cutoff these TCOs' access to money laundering?

Mr. CUCCINELLI. Senator, I will start, and then turn it over to Director Wray. As I mentioned up front, one of the areas we believe that you all in Congress can be most helpful to us in this particular battle with these most evil people in the Western Hemisphere is to provide us some tools that allow designation somewhere below a foreign terrorist organization because of the sweeping capture of much of society because of how these organizations are interconnected with the Mexican society so thoroughly, but above the level of mere prosecution one person at a time, that allow us to attack the organizations at a strategic level and bring them down to help Mexico regain more control of its own country and protect ours at the same time.

So that is an area we would be very happy to partner with you on. It is definitely an area where there is potential for improvement, and one of the key areas you touch on is money. Mr. Miller talked about ISIS and al-Qaeda in particular. They are out, they believe, on some holy war. And the folks in the TCOs, they are not out there for what they think of as God, or maybe they do, but it is for money. And if we can get at the money and start to cutoff their ability to gain the benefits of their evil produce in the case of drugs and trafficking in the case of humans, we are going to

really be able to start to put a major dent in their operations, in their threat to both Mexico and to the United States.

Mr. WRAY. I would agree with what Mr. Cuccinelli just said. I would just add that we have found over 112 years at the FBI that whatever kind of enterprise we are talking about—in this case, the transnational criminal organizations—if you really want to dismantle the enterprise, you have to go after the money as well, because, in effect, the money becomes their infrastructure. And so, the value of global crime ranges between \$1 and \$2 trillion annually. But about \$300 billion are attributed to U.S.-based transnational criminal organization networks. And so figuring out a way to cutoff their access to money is ultimately going to be one of the most critical parts of making sure that the strategy is not just effective but enduring.

Senator SINEMA. Thank you, Director Wray, and thank you, Mr. Cuccinelli.

Mr. Chair, I do have further questions, but in the interest of my time expiring, I will submit them for Mr. Cuccinelli and for Director Wray, and I will yield back the balance of my time.¹

Thank you, Mr. Chairman.

Chairman JOHNSON. I appreciate that, Senator Sinema.

So let me begin first by saying that of all the listed threats that I began the hearing with, I do not even think I mentioned border security. We have probably done a pretty good job of covering most, but I did not put a stopwatch on this. I think it is also true it kind of confirms what I ended up with, talking about what I believe is our current greatest threat to our democracy, and that literally is the rioting, the anarchy, the fact that the adherence to the rule of law is actually a question in this country today. I think probably there was more time devoted during this hearing, more questions asked, more answers given in terms of what we are seeing right now.

I appreciate that, and I want to ask you, Mr. Cuccinelli, as a former Attorney General, one of the things I am highly concerned about, again, just the lack of adherence to the rule of law, the rejection of it, as we saw in the protests in Louisville yesterday because people did not agree with what happened in a grand jury.

One of the things that disturbs me is the movement toward anti-bail laws, the fact that we actually have people donating to organizations that will pay bail so that we, in effect, have what we saw at the border, catch and release; now we have catch and release in our cities.

Can you just speak to—by the way, Senator Paul talked about how the officer who was assaulted that had protected him, the person who assaulted him was charged and then released. We do not know whether he will ever be prosecuted because I am not sure he will ever be found.

So, Mr. Cuccinelli, can you just kind of speak to my concern about this moving toward anti-bail laws, the individuals that are paying to bail people out so they can get right back on the street and riot the next night?

¹The questions of Senator Sinema appears in the Appendix on page 78.

Mr. CUCCINELLI. Senator, that is a major concern. It does invoke State and local authority to a significant degree, not necessarily in D.C. where Congress can have a say. Senator Paul did touch on this earlier. And we see this almost recycling of criminals because they walk out in so many jurisdictions, whether it is New York or Portland.

The notion that anti-bail legislation is somehow a reform that improves the criminal justice system honestly escapes me. And, mind you, that is coming from someone who has been a 25-year advocate for criminal justice reform, including what was passed by the Congress and President Trump less than 2 years ago.

So that is the perspective that I come to this from, including my time as an Attorney General. This was not an issue we faced in Virginia because we did not have localities nor did we have at the State level this sort of treatment of bail as a punishment as opposed to a safety mechanism and a part of the justice process, which is what we are seeing in other parts of the country.

I would just note also Senator Portman made comments that I wanted to dovetail off that are similar to yours, Mr. Chairman. One of the most disturbing aspects of this summer of violence has been the overt encouragement of many who are in governmental positions of leadership, whether it is the Speaker of the House attacking law enforcement, using phrases like "storm troopers" to describe Federal law enforcement doing their job properly. There was not even any question on her part about them not doing the job right. And these are people doing the job she as a Member of Congress has cast for them. Or if it is Mayor Wheeler in Portland who is encouraging violence, and we see this rife across large swaths of our political arena.

I appreciate Senator Carper's comments in referencing Breonna Taylor's mother's comments. I think those were extremely appropriate, and they are helpful, and we appreciate hearing them from leadership in this country. But so much of the political leadership in the country has encouraged this violence. It has been a shocking aspect to the last 4 months that I find as a former Attorney General and in my current role at the Department of Homeland Security just shocking and is really contrary to the ideals and values of this country.

Chairman JOHNSON. It should surprise no one when we put forward this greater leniency. That is what is happening. That is what anti-bail laws are. It is certainly what happens when people contribute to organizations that bail people out and put them back out on the street. That is greater leniency that is leading to greater lawlessness. It should come as no surprise.

So Senator Carper asked, are there things that we should do? Do we need to potentially create new crimes?

I will ask you, Director Wray, I know Attorney General Barr has spoken about, whether he mused about it, whether he is serious about charging people with sedition. But what can we do to gain control over our cities? Again, almost 570 of these peaceful protests turned to riots, violence, and death. This is completely unacceptable. We need to get control of the situation. What do we need to do to get control of the situation?

Mr. WRAY. Certainly, Mr. Chairman, you touched on one issue, which is it is hard enough to make sure that the men and women of law enforcement can do what they need to do to arrest people the first time without having to go back out and rearrest the same person over and over again. And Senator Paul touched on that a little bit in his comments as well.

As I said, I think in response to one of your colleagues' questions, when Federal, State, and local law enforcement all work together, which we do all the time around this country, and do it promptly, that is when we are able to see the best results, everybody trying to look for what they can best contribute to the phenomenon. And, of course, in your home State, while there was significant damage in a short period of time, comparatively quickly—I say compared to some other parts of the country—different parts of law enforcement all banded together, worked hand in hand, and managed to bring law and order much more quickly by comparison. So while there was significant and tragic damage there, and, of course, some fatalities and injuries, it could have been a heck of a lot worse. But I think that illustrates how important partnership is to dealing with this particular problem.

Chairman JOHNSON. Thank you, Director Wray.

Senator Portman, I will just ask you again, I know you stayed behind as a backup. I appreciate that with me being remote. Do you have a couple more questions before—I have a few more myself.

Senator PORTMAN. Let me, just if I could, follow up a little bit on one. Thank you, Mr. Chairman.

I told the Chairman earlier I thought I was the last speaker when I questioned last time, so I went a little long because I was the only one in the room. But in this new virtual world, we had others, so I apologize to my colleagues for taking more time.

The third threat I did want to talk about was this domestic terrorism threat, and sometimes it is white supremacists, anti-Semitic, as an example, hateful attacks, or sometimes it is Islamic extremists. But this is something that, again, the Department has begun to focus on more. Mr. Cuccinelli, I understand that DHS recently released the implementation plan for your Countering Terrorism and Targeted Violence (CTTV) Strategic Framework.

Mr. CUCCINELLI. Yes.

Senator PORTMAN. This Committee, again, has been very active on a particular part of the response, which is these Nonprofit Security Grant Programs (NSGP). It basically is a Federal Emergency Management Agency (FEMA) grant program that goes out usually to a faith-based organization, say a synagogue, a church, or a mosque, but all nonprofits are eligible, and it is for security enhancements and now can be used, thanks to DHS, even for armed security. But a lot of it is just about getting the expertise, being sure that these organizations know where do you place the cameras, how do you ensure that things are locked, and you can help them by just doing a walk-through often.

Thirty-two organizations in Ohio have received a combined total of \$2.3 million in grants in fiscal year 2020, and they are using it well, in my view, and I have had a chance to visit with them.

One thing we did last year that I thought was quite effective is we had a conference in Columbus, Ohio, and we had the FBI there, Director Wray. They did a great job. We also had DHS there, Secretary Cuccinelli, and they did a great job of just explaining what the threat was and kind of starting down the process of what do you do to respond to it. The folks in the room, this was the Sikh community, the Muslim community, the Jewish community, the Christian community. Everybody was there. People really appreciated it, and I think that is one thing to think about, is the possibility of doing more of these around the country where you have a conference and bring together some of the leadership and just so people get a better sense, one, of what is going on in the real world out there in terms of this threat, and it is not a classified environment, but you were able to provide some very good information and then, second, what do you do about it.

So that is my question to you: What more can we do? I know you have a new grant program. I would like to hear about that. But if the two of you could speak—or all three of you speak briefly about this issue, that would be great.

Mr. CUCCINELLI. Yes, just this month the first tranche of the new grant dollars—I want to say \$10 million—went out to 29 recipients, and that is, as so much of the DHS responsibility in the domestic arena is prevention, it goes hand in hand with standing up Targeted Violence and Terrorism Prevention (TVTP), the office there for Targeted Violence. And we are doing it—some people are familiar with the U.K. model. They have this big, huge group of people that works for their Federal Government that goes out to try to interdict terrorism, not in a law enforcement fashion but more like an intervention before violence occurs.

That is a very different model than we are taking. We have just started building out. We have our first 12 full-time employees for regional directors to expand partnerships so that we get a whole-of-America, including working with exactly those nonprofits you are talking about, Senator, to integrate them into our preventive efforts, both planning for their resistance to potential for assaults, but also for their partnership in intervening when they see people going down a path that may lead them to violence.

And so that is the approach that we are taking in that office. It is one of the areas of greatest expansion that you will see over the course of the next year at the Department of Homeland Security as we grow that effort out into communities across the country. And certainly you describe one way that those contacts can be made more deeply and more quickly, and we are very open to repeating that sort of performance.

Senator PORTMAN. Thank you. I appreciate the commitment to it. I think it does make sense. In a sense you are leveraging the Federal dollars significantly by getting this cooperation.

Mr. CUCCINELLI. Right.

Senator PORTMAN. As Director Miller knows, in Columbus, Ohio, I think the first indictment was made several years ago of an Islamic terrorist who the FBI had worked with through an informant, and we were able to stop a horrific act.

What really happened was that the Muslim community in Columbus, Ohio, was cooperating with local, State, and Federal law

enforcement to be able to find that individual and to prevent what would have been, a terrible loss of life. So that is an example where just having those relationships made a big difference, and it was at every level of government.

Do you have any thoughts on this, either Director Wray or Director Miller?

Mr. WRAY. I guess I would just add that I think community engagement is something that is critical to dealing with what we consider the biggest threat to the homeland, which is this combination of homegrown violent extremists and domestic violent extremists, all of whom are typically lone actors, easily radicalized online, attacking soft targets with readily accessible weapons. Because that is such a challenge for law enforcement, one thing that we have seen both with the attacks we have thwarted and prevented and, unfortunately, the attacks that have occurred that we have investigated after the fact is that almost every time, if you look back, there was someone along the way—a friend, a family member, a co-worker, a neighbor, a classmate, what have you—who knew the person well enough to notice the transformation from radicalization of whatever kind it was to mobilization. And so you have often heard the saying, “If you see something, say something.” Most of us when we hear that, we think of the unattended backpack in the Greyhound bus terminal or something. Of course, we want people to call when that happens. But we are trying to push out through all of our field offices—and I have been to all 56 of them and met with communities I think in every single one—if you see something about somebody, we need you to say something. I have been encouraged by those instances where sometimes having wrestled with great interpersonal demons, a family member, a parent, will say—and think about how hard that is, “My 18, 19-year-old child is going off the rails, and I am concerned he might do something. And they call us. And it is a heck of a lot better situation both for them and, more importantly, for the public, if we can do something before that person acts.

Senator PORTMAN. Thank you, Mr. Director.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thanks, Senator Portman. Again, thanks for sticking around there and backing me up.

Director Miller, I feel a little bad that you have not been fielding a whole lot of questions and providing a whole lot of answers. I would like to think it is because the foreign threats the National Counterterrorism Center is normally known to address have been reduced, but I know that is not the case. I think the main reason is kind of what I stated in my opening, that the unrest, the rioting, the lawlessness, the anarchy on the streets of America are just posing a more pressing risk and a greater risk to our overall democracy. I do want to give you a quick opportunity here at the tail end of the hearing here. Is there anything else that you think is important that the American people understand about what you are trying to do to keep this Nation safe, the men and women in your agency?

Mr. MILLER. Chairman, I am not offended in the least. I think that is really a testimonial or a testament to the success we have had in the last 19 years, that it is no longer the principal concern

of this Committee and others, and that is all right. That is what we wanted. We said this was going to be a generational war. We did not want it to be a multigenerational war. So I take great solace in the fact that we are talking about other things for a change.

I just want to highlight in closing, thank you for allowing me the opportunity to make a few comments. We just need to finish this thing and maintain our focus and not, to use a cliché, take our foot off the gas too soon. The support of this Committee and the Senate and Congress, writ large, is so important to that. I really thank you for the opportunity to make a few comments.

Chairman JOHNSON. I appreciate the point you made about 2011, bugging out of Iraq way too early, which gave rise to ISIS and the caliphate and all that terror that resulted from that. So we have to learn from that type of blunder. We have to learn those types of lessons.

Finally, Director Wray, this is not on threats, but I just have to take this opportunity to ask you a couple questions about our investigation and the unfortunate fact that my frustration level got to the point where I had to subpoena the FBI now. I appreciate the fact that we have had conversations, and since that point in time, the FBI has become more responsive. But the fact of the matter is we are in our second extension. My staff continues to not obtain the materials. They are having to go into the reading room, which is very inefficient and, quite honestly, so much of the material they are reviewing is not sensitive, it is not overly classified, there is no reason we cannot take possession of it.

I think my first question is, really ask you to kind of look into that, be a little bit more open with the information that I think Congress certainly deserves and, quite honestly, the American people have a right to know what all happened. But can you make that commitment to really take a look at that and prod the people that work under you to make this kind of information readily available directly to our Committee to have it in our possession?

Mr. WRAY. Yes, Mr. Chairman, I will certainly drill into it further and have my staff look and see if there are ways in which we can improve the process. The reading room construct that you have described is, of course, a process that we and others in the intelligence community use with really all committees for this kind of information. But we have surged additional resources to your request, and we have brought staff from multiple divisions. Of course, we are working with other agencies, and a lot of times the information or at least the parts of the information that make something classified are other agencies' information, and that makes it more complicated.

But we are going to continue to work as hard as we can in good faith to be responsive and accommodating, and I appreciate your forbearance and the conversations we have had lately.

Chairman JOHNSON. OK. I appreciate that. One particular piece of information that is frustrating my staff is there are unclassified text messages from Andrew McCabe which are not being made available to us. So would you commit to making those things available to us, delivered to us in our possession?

Mr. WRAY. I will be happy to look into that and have someone get back to you as quickly as we can about where that stands.

Chairman JOHNSON. OK. I appreciate it.

In the Department of Justice Inspector General Horowitz's report, former Assistant Director Bill Priestap was quoted as saying that the FBI did not have any indication whatsoever as of May 2017 that the Russians were running a disinformation campaign. Because my staff uncovered four classified footnotes—and, again, I think that just points to why this is so important that we make this information available. But in those four classified footnotes, we now know the FBI in early October 2016, the Crossfire Hurricane team actually did obtain information from a Steele subsource that “he was suspected of being linked to Russian intelligence services and rumored to be a former Foreign Intelligence Service of the Russian Federation (KGB SVR) officer.”

In January 2017, the FBI started interviewing those subsources and found out that Steele's reporting was misstated or exaggerated, that it was based on rumor and speculation, that the subsource never expected Steele to put the primary subsource's statements in reports or present them as facts, that he or she made it clear to Steele that she had no proof to support the statements from her subsources, that it was just talk, word-of-mouth hearsay, conversations you had with friends over beers, statements made in jest.

So, again, the FBI had indication also possible infiltration of the Steele organization by Russian intelligence services. Again, this was in January 2017. So that indication of a subsource possibly being a KGB officer in October 2016. January 2017, they found confirmation of that and how grossly unreliable the Steele dossier was, and yet the investigation continued. It continued to the point where we set up a Special Counsel to take a look at this largely based on the Steele dossier.

I think my question on this is: As the current FBI Director, do you believe the Crossfire Hurricane investigation should have proceeded at all once the FBI knew that the KGB might have been one of Steele's subsources and that Russian disinformation was contained in the Steele dossier?

Mr. WRAY. Mr. Chairman, first let me try to answer your question this way: I think the Inspector General's report about the Crossfire Hurricane investigation describes conduct that I consider unacceptable, unrepresentative of who the FBI is as an organization, and cannot be allowed to be repeated. I have implemented over 40 corrective measures to address those issues.

Some of what you are touching on is relevant as well to the ongoing John Durham investigation with which we are fully cooperating, even to the point of having agents who are working on it with him. So I want to be a little bit careful about how I weigh in on that. But, of course, as you know, the Justice Department has concluded that the Carter Page Foreign Intelligence Surveillance Act (FISA) applications, at least after that date, should not have been submitted, and all this happened before I became FBI Director, but I believe the DOJ officials who were around at the time have now said they would not have signed those applications. So I think to some extent, that speaks for itself.

Chairman JOHNSON. From my standpoint, it is pretty obvious that past January 2017, there should have been no further investigation into the Trump campaign's possible collusion with Russia.

The information backed predicate to investigation crumbled and simply did not support it any further.

My final question. You said you were not FBI Director back then, but you were in March 2018, and in March 2018, the FBI provided a briefing to the Senate Select Committee on Intelligence in which they briefed that Committee that the Steele reporting was reliable.

Now, again, we just talked about what the FBI knew and when they knew it as early as October 2016 and certainly by January 2017 that the Steele dossier was not reliable. So my question for you is: That happened on your watch. How could that happen? How could the FBI go in and brief the Senate Select Committee on Intelligence over a year later when they knew the Steele dossier was not reliable and brief the Senate Committee that it was?

Mr. WRAY. Mr. Chairman, the issue you are raising is one that I have been in close contact with Chairman Graham about. I will say this: The briefing in question, as I understand it, was a staff-to-staff briefing, and it was happening at a time when we were largely in stand-down mode because of the Special Counsel investigation. So obviously I am concerned about what I have heard about that briefing, but I probably for right now should just leave it at that.

Chairman JOHNSON. I just want to ask, are there employees of the FBI that were part of that briefing that are still employees? And has there been any disciplinary action taken against those individuals? Because just saying it was an FBI briefing to staff, that is still the FBI briefing Congress. This is a year after the fact that we knew the Steele dossier was not reliable.

Mr. WRAY. First let me say by describing it as a staff briefing, that is in no way intended to suggest that that is not important. But, second, as to disciplinary action, I believe that all of the most senior executives involved in the investigation and including in that—who participated in that briefing are all gone from the FBI. In some cases people have been fired, in other cases people have retired or resigned, all on my watch.

As far as disciplinary action beyond that, every individual who is referenced in the Inspector General's report at any level, even in passing, has been referred to our Office of Professional Responsibility and our Inspection Division for possible disciplinary action.

Now, these tend to be people who are more at a line level, and as far as disciplinary action toward them, that has largely been a little bit on a standstill in order to accommodate Mr. Durham and his investigation at his request. There are certain steps that we have to wait on in order to let him complete his investigation, with which we are, of course, fully cooperating, as the Attorney General has said quite publicly on a number of occasions.

Chairman JOHNSON. I appreciate your answer, and, listen, I think we share the same goal here. We have to restore the credibility to the FBI, and the only way to do that is the FBI has to come clean, if needed, has to clean house to a certain extent. But the American people need to understand what happened, and they need to have assurance that the FBI will take corrective actions and hopefully put policies in place where this will never happen again.

So, again, I look forward to working with you, really encourage full expeditious cooperation. The American people have a right to know. They should have known, quite honestly, years ago.

I want to thank all the witnesses for your service, for your sacrifice. As was said by most Members of this Committee, please convey to the men and women that work with you our appreciation for their service and sacrifice. I need to underscore the point. I truly believe the vast majority of Americans are so appreciative of what law enforcement does, what it does every day, day in and day out, trying to keep our cities, our States, this country safe. I think it is just an abomination, quite honestly, that there is this defund the police movement, that there are so many people attacking law enforcement. We need to support law enforcement. As a number of Members certainly pointed out, how are we going to recruit the fine men and women that put their lives on the line to keep us safe if we keep denigrating them and we keep attacking them?

I hope that people hearing this hearing today understand that there is a great deal of support for law enforcement, and I think that is, by and large, the vast majority of Americans. So, again, God bless everybody in law enforcement, and God bless everybody in your departments and agencies.

With that, the record will remain open for 15 days until October 12 at 5 p.m. for the submission of statements and questions for the record.

This hearing is adjourned.

[Whereupon, at 12:38 p.m., the Committee was adjourned.]

A P P E N D I X

Opening Statement of Chairman Ron Johnson “Threats to the Homeland” September 24, 2020

As submitted for the record:

In the wake of the September 11th terrorist attacks, we reshaped our homeland security apparatus to better prepare for the next attack. Now, 19 years later, as we continue to mourn those lost, we must also honor the memory of the attack by ensuring that our nation’s homeland security defenses evolve to counter an ever-changing threat landscape. Today, we will hear testimony from leaders from the Federal Bureau of Investigation, the National Counterterrorism Center, and the Department of Homeland Security, who are at the forefront of the fight to protect the Nation from persistent foreign and domestic threats.

In addition to traditional terrorist threats, we face growing threats of violence within our own borders. In the past four months, we have seen our nation vandalized, looted, and attacked by violent opportunists and criminals looking to exacerbate tensions and inflict harm. My home state, Wisconsin, has been especially affected by both violent rioting and civil unrest. While I strongly support the right of Americans to protest injustices, I am calling for the violence against property, law enforcement and fellow Americans to end immediately.

While we have focused our attention on violent opportunists, there has been violence perpetrated by domestic extremists from all ideological backgrounds. In addition to calling out violent rioting, we must also address the extremists who call for violence, regardless of their affiliation. Antifa, anti-government extremists and white supremacists have all exploited this nationwide unrest to promote their radical agendas and sow discord within our society.

We must remain vigilant in our fight against international Islamist terrorism and radical domestic violent extremists. Our Committee has been engaged with DHS, the FBI, and NCTC to ensure resources are being appropriately allocated based to counter foreign and domestic terrorist threats.

In addition to an evolving terrorism threat landscape, in recent years our country has had to adapt to emerging cyber and critical infrastructure related attacks. We have seen foreign adversaries target our institutions through ransomware attacks, intellectual property theft, and the spreading of disinformation in an attempt to undermine our Democracy.

As complex as these threats are, our efforts to combat them were made even more challenging as the coronavirus pandemic spread across the globe. Now adversaries not only attempt to weaponize the virus, but they are also attempting to steal intellectual property of U.S. government-funded COVID-19 vaccine development. COVID-19 has added another layer to complexity to our government’s efforts to protect and secure the homeland, as agencies work to respond to the pandemic while balancing their traditional priorities, such as border security, emergency response, and counterterrorism.

I want to thank the brave men and women in uniform for working to keep America safe. Two weekends ago we saw a horrific attack on law enforcement, when two sheriff’s deputies

were shot in the head. Almost nineteen years to the day after the September 11th terrorist attacks, it is a tragedy that this is how we now treat those who work to protect us.

I also want to thank Director Wray, Director Miller, and Mr. Cuccinelli for appearing before the Committee today and I look forward to your testimony.

**U.S. Senate Committee on Homeland Security and Governmental Affairs Full
Committee Hearing: Threats to the Homeland**

September 24, 2020

Senator Gary C. Peters, Ranking Member

Opening Statement As Prepared for Delivery

Thank you, Mr. Chairman and thank you to our witnesses for joining us today. While our Committee has no shortage of serious and consequential issues to tackle, our annual threats hearing is one of the most important opportunities we have to discuss how we can better safeguard our nation.

We continue to face a number of security threats, both old and new. Over the past year, since we last held this hearing, that list has only grown.

Not only do we continue to face critical threats from foreign and domestic terrorism, cyber-attacks, and efforts by foreign governments to sow chaos within our country, we are also dealing with a once-in-a-lifetime pandemic that has tragically taken the lives of over 200,000 Americans.

This public health disaster has also further exposed a significant security risk embedded in the tools we use every day to connect with the world.

As we have moved more of our daily lives online because of Coronavirus, bad actors have exploited technological weaknesses to attack the platforms we use for remote school and work.

Adversaries are working to infiltrate private companies and government agencies who are part of the critical race to find a vaccine.

Both foreign and domestic actors have also seized on misinformation and disinformation, chipping away at the fabric of our democracy, and sowing discord and mistrust in the institutions we rely on to keep us safe.

The scourge of white supremacist violence that is a long-standing issue but is now again one of the largest terrorist threats to American safety and security.

I'm alarmed that this Administration continues to downplay this threat and the root causes driving these violent ideologies.

We cannot be shortsighted when it comes to protecting our national security. As threats continue to develop and evolve – our national security agencies must be able to adapt.

We count on DHS, the National Counterterrorism Center, and the FBI to work together and provide a unified effort to defend the homeland.

As we discussed at yesterday's hearing, I am concerned that DHS has suffered because of the lack of qualified, consistent and stable leaders at the agency's helm.

While I am disappointed the Department does not believe the Acting Secretary can testify alongside his counterparts from the FBI and the National Counterterrorism Center on these important issues during his confirmation process, I am looking forward to the testimony of the three officials with us today.

Many Americans will never know the names of the thousands of personnel working tirelessly behind the scenes at your agencies to keep our country safe.

But we are all counting on you and your teams to address the known threats to our safety, and anticipate the emerging and unknown dangers our communities will face in the weeks, months, years and even decades ahead.

I'm grateful to each of you for joining us today. I look forward to hearing from you about the threats America currently faces, what your departments are doing to address those threats, and how this Committee and your agencies can continue working together to protect our national security. Thank you.



Department of Justice

STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED
"WORLDWIDE THREATS"

PRESENTED
SEPTEMBER 24, 2020

STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED
“WORLDWIDE THREATS”

PRESENTED
SEPTEMBER 24, 2020

Good afternoon, Chairman Johnson, Ranking Member Peters, and Members of the Committee. Thank you for the opportunity to appear before you today to discuss the current threats to the United States Homeland. I am pleased to be here representing the nearly 37,000 dedicated men and women of the FBI.

While the COVID-19 pandemic has presented unique and unprecedented challenges to the FBI workforce, I am proud of their dedication to our mission of protecting the American people and upholding the Constitution. Hostile foreign actors, violent extremists, and opportunistic criminal elements have seized upon this environment. As a result, we are facing aggressive and sophisticated threats on many fronts. Whether it is terrorism now moving at the speed of social media, or the increasingly blended threat of cyber intrusions and state-sponsored economic espionage, or malign foreign influence and interference or active shooters and other violent criminals threatening our communities, or the scourge of opioid trafficking and abuse, or hate crimes, human trafficking, crimes against children — the list of threats we are worried about is not getting any shorter, and none of the threats on that list are getting any easier.

Counterterrorism

Preventing terrorist attacks remains the FBI’s top priority. However, the threat posed by terrorism — both international terrorism (“IT”) and domestic violent extremism — has evolved significantly since 9/11.

The greatest threat we face in the Homeland is that posed by lone actors radicalized online who look to attack soft targets with easily accessible weapons. We see this lone actor threat manifested both within Domestic Violent Extremists (“DVEs”) and Homegrown Violent Extremists (“HVEs”), two distinct sets of individuals that generally self-radicalize and mobilize to violence on their own. DVEs are individuals who commit violent criminal acts in furtherance of ideological goals stemming from domestic influences, such as racial bias and anti-government

sentiment. HVEs are individuals who have been radicalized primarily in the United States, and who are inspired by, but not receiving individualized direction from, Foreign Terrorist Organizations (“FTOs”).

Many of these violent extremists, both domestic and international, are motivated and inspired by a mix of ideological, socio-political, and personal grievances against their targets, which recently have more and more included large public gatherings, houses of worship, and retail locations. Lone actors, who by definition are not likely to conspire with others regarding their plans, are increasingly choosing these soft, familiar targets for their attacks, limiting law enforcement opportunities for detection and disruption ahead of their action.

DVEs pose a steady and evolving threat of violence and economic harm to the United States. Trends may shift, but the underlying drivers for domestic violent extremism — such as perceptions of government or law enforcement overreach, socio-political conditions, racism, anti-Semitism, Islamophobia, misogyny, and reactions to legislative actions — remain constant. As stated above, the FBI is most concerned about lone offender attacks, primarily shootings, as they have served as the dominant lethal mode for domestic violent extremist attacks. More deaths were caused by DVEs than international terrorists in recent years. In fact, 2019 was the deadliest year for domestic extremist violence since the Oklahoma City Bombing in 1995.

The top threat we face from domestic violent extremists stems from those we identify as Racially/Ethnically Motivated Violent Extremists (“RMVE”). RMVEs were the primary source of ideologically-motivated lethal incidents and violence in 2018 and 2019 and have been considered the most lethal of all domestic extremists since 2001. Of note, the last three DVE attacks, however, were perpetrated by Anti-Government Violent Extremists.

The spate of attacks we saw in 2019 underscore the continued threat posed by DVEs and perpetrators of hate crimes. The FBI works proactively to prevent acts of domestic terrorism and hate crimes. For example, in November 2019, the Denver Joint Terrorism Task Force arrested Richard Holzer on federal charges of attempting to obstruct religious exercise by force using explosives. This disruption is just one example of the strength of our Domestic Terrorism-Hate Crimes (“DT-HC”) Fusion Cell. Our Counterterrorism (“CTD”) and Criminal Divisions (“CID”) working together were able to prevent a potential terrorist attack before it occurred and, for the first time in recent history, make a proactive arrest on a Hate Crimes charge. Through the DT-HC Fusion Cell, subject-matter experts from both CTD and CID work in tandem to innovatively use investigative tools and bring multiple perspectives to bear in combatting the intersecting threats of domestic terrorism and hate crimes, preventing attacks and providing justice to victims.

We recognize that the FBI must be aware not just of the domestic violent extremism threat, but also of threats emanating from those responding violently to First Amendment-protected activities. In the past, we have seen some violent extremists respond to peaceful movements through violence rather than non-violent actions and ideas. The FBI is involved only when responses cross from ideas and Constitutionally-protected protests to violence. Regardless of the specific ideology involved, the FBI requires that all domestic terrorism

Investigations be predicated based on activity intended to further a political or social goal, wholly or in part involving force, coercion, or violence, in violation of federal law.

HVEs and FTOs have posed a persistent threat to the Nation and to U.S. interests abroad, while their tradecraft, tactics, and target sets have evolved. The international terrorism threat to the U.S. has expanded from sophisticated, externally-directed FTO plots to include individual attacks carried out by HVEs who are inspired by designated terrorist organizations. As stated above, the FBI assesses HVEs are the greatest, most immediate international terrorism threat to the Homeland. These individuals are FTO-inspired individuals who are in the U.S., have been radicalized primarily in the U.S., and are not receiving individualized direction from FTOs. We, along with our law enforcement partners, face significant challenges in identifying and disrupting HVEs. This is due, in part, to their lack of a direct connection with an FTO, an ability to rapidly mobilize without law enforcement detection, and their frequent use of encrypted communications.

Many FTOs use various digital communication platforms to reach individuals they believe may be susceptible and sympathetic to violent terrorist messages. However, no group has been as successful at drawing people into its perverse ideology as ISIS, which has proven dangerously competent at employing such tools. ISIS uses traditional media platforms as well as widespread social media campaigns to propagate its ideology. Terrorists in ungoverned spaces — both physical and virtual — readily disseminate propaganda and training materials to attract easily influenced individuals around the world to their cause. With the broad distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable persons of all ages in the U.S. either to travel to foreign lands or to conduct an attack on the Homeland. Through the Internet, terrorists anywhere overseas now have direct access to our local communities to target and recruit our citizens and spread their message faster than was imagined just a few years ago.

We remain concerned that groups such as the Islamic State of Iraq and ash-Sham (“ISIS”) and al-Qaeda intend to carry out large-scale attacks in the U.S. Despite their territorial defeat in Iraq and Syria, ISIS remains relentless and ruthless in its campaign of violence against the West and has aggressively promoted its hateful message, attracting like-minded violent extremists. The message is not tailored solely to those who overtly express signs of radicalization. It is seen by many who use messaging apps and participate in social networks. Ultimately, many of the individuals drawn to ISIS seek a sense of belonging. Echoing other terrorist groups, ISIS has advocated lone offender attacks in Western countries. Recent ISIS videos and propaganda have specifically advocated attacks against soldiers, law enforcement, and intelligence community personnel.

As noted above, ISIS is not the only terrorist group of concern. Al-Qaeda maintains its desire for large-scale, spectacular attacks. While continued counterterrorism pressure has degraded the group’s Afghanistan-Pakistan senior leadership, in the near term, al-Qaeda is more likely to focus on building its international affiliates and supporting small-scale, readily achievable attacks in key regions such as East and West Africa. Simultaneously, over the last

year, propaganda from al-Qaeda leaders seeks to inspire individuals to conduct their own attacks in the U.S. and the West. For example, the December 2019 attack at Naval Air Station Pensacola demonstrates that groups such as al-Qaeda continue to be interested in encouraging attacks on U.S. soil.

The FBI regularly reviews intelligence to ensure that we are appropriately mitigating threats from any place by any actor, and the possible violent responses and actions. We are sensitive to First Amendment-protected activities during investigative and intelligence efforts so as to ensure that our investigative actions remain aligned with our authorities and are conducted with the appropriate protections in place for privacy and civil liberties.

As the threat to the United States and U.S. interests evolves, we must adapt and confront these challenges, relying heavily on the strength of our federal, State, local, Tribal, and international partnerships. The FBI uses all lawful investigative techniques and methods to combat these terrorist threats to the United States. Along with our domestic and foreign partners, we are collecting and analyzing intelligence concerning the ongoing threat posed by violent extremists motivated by any ideology and desire to harm Americans and U.S. interests. We continue to encourage information sharing, which is evidenced through our partnerships with many federal, State, local, and Tribal agencies assigned to Joint Terrorism Task Forces around the country. Be assured, the FBI continues to strive to work and share information more efficiently, and to pursue a variety of lawful methods to help stay ahead of these threats.

Election Security

In less than two months, Americans will exercise one of their most important and cherished freedoms; the right to vote in a democratic election. Our nation is confronting multi-faceted foreign threats seeking to both influence our national policies and public opinion, and cause harm to our national dialogue. The FBI and our interagency partners remain concerned about, and focused on, the covert and overt influence measures used by certain adversaries in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic processes.

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. This year's election cycle, amid the COVID-19 pandemic, provides ample opportunity for hostile foreign actors to conduct disinformation campaigns and foreign influence operations in an effort to mislead, sow discord, and, ultimately, undermine confidence in our democratic institutions and values and in our government's response to our current health crisis.

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, the Foreign Influence Task Force (“FITF”) was established to identify and counteract malign foreign influence operations targeting the United States. The FITF is led by the Counterintelligence Division and is composed 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. Through the efforts of the FITF, and lessons learned from both the 2016 and 2018 elections, the FBI is actively engaged in identifying, detecting, and disrupting threats to our elections and ensuring both the integrity of our democracy is preserved and the will of the American people is fulfilled.

Protecting policymakers is an important part of our efforts to combat malign foreign influence and protect our elections. As you are aware, the FBI and our interagency partners have been providing ongoing election security threat briefings to Congress. We will continue to do so throughout the fall and into the future, where there is actionable intelligence.

Lawful Access

I want to turn now to an issue continuing to limit law enforcement's ability to disrupt these increasingly insular actors. We are all familiar with the inability of law enforcement agencies to access data, even with a lawful warrant or court order, due to "end-to-end" encryption. Increasingly, device manufacturers and communications service providers have employed encryption in such a manner that only the users or parties to the communications can access the content of the communications or devices. This is known as "end-to-end" encryption.

This development has meant that, in recent years, the FBI has observed a decline in its ability to gain access to the content of both domestic and international terrorist communications, due to the widespread adoption of encryption for Internet traffic and the prevalence of mobile messaging apps using end-to-end encryption as default.

The FBI certainly recognizes how encryption increases the overall safety and security of the Internet for users. But, in fulfilling the FBI's duty to the American people to prevent acts of terrorism, this kind of end-to-end encryption creates serious challenges. Accessing content of communications by, or data held by, known or suspected terrorists pursuant to judicially authorized, warranted legal process is getting more and more difficult.

The online, encrypted nature of radicalization, along with the insular nature of most of today's attack plotters, leaves investigators with fewer dots to connect. As was evident in the December 9, 2019, shooting at Naval Air Station Pensacola that killed three U.S. sailors and severely wounded eight other Americans, deceased terrorist Mohammed Saeed Alshamrani was able to communicate using warrant-proof, end-to-end encrypted apps deliberately to evade detection by law enforcement. It took the FBI several months to access information in his phones, during which time we did not know whether he was a lone wolf actor, or whether his associates may have been plotting additional terrorist attacks.

If law enforcement loses the ability to detect criminal activity because communication between subjects — data in motion — or data held by subjects — data at rest — is encrypted in such a way making content inaccessible, even with a lawful order, our ability to protect the American people will be degraded. Providers and law enforcement must continue to collaborate to explore possible technical solutions that would provide security and privacy to those using the Internet while also contributing to the FBI's ability to complete its mission.

Despite the successes that result from the hard work of the men and women of the FBI, our Joint Terrorism Task Forces, and our partners across the government, terrorism continues to pose a persistent threat to the Homeland and our interests overseas.

China Threat

The greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It is a threat to our economic security and by extension, to our national security.

As you have seen from the recent closure of the Chinese Consulate in Houston, this issue is not just an intelligence issue, or a government problem, or a nuisance largely just for big corporations who can take care of themselves. Our adversaries' targets are our nation's core economic assets — our information and ideas, our innovation, our research and development, our technology. No country poses a broader, more severe threat to those assets than China. It is the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history. If you are an American adult, it is more likely than not that China has stolen your personal data.

In 2017, the Chinese military conspired to hack Equifax and made off with the sensitive personal information of 150 million Americans — we are talking nearly half of the American population and most American adults. Our data is not the only thing at stake here — so is our health, livelihood, and security.

The FBI is opening a new China-related counterintelligence case approximately every ten hours. Of the nearly 5,000 active FBI counterintelligence cases currently underway across the country, almost half are related to China. And at this very moment, China is working to compromise American health care organizations, pharmaceutical companies, and academic institutions conducting essential COVID-19 research. They are going after cost and pricing information, internal strategy documents, personally identifiable information — anything that can give them a competitive advantage.

It is important to be clear: this is not about the Chinese people as a whole, and certainly not about Chinese-Americans as a group, but it is about the Chinese government and the Chinese Communist Party. Every year, the United States welcomes more than 100,000 Chinese students and researchers into this country. For generations, people have journeyed from China to the United States to secure the blessings of liberty for themselves and their families — and our society is better for their contributions. So, when the FBI's refers to the threat from China, we mean the Government of China and the Chinese Communist Party.

Confronting this threat effectively does not mean that we should not do business with the Chinese. It does not mean that we should not host Chinese visitors. It does not mean that we should not welcome Chinese students or coexist with China on the world stage. But it does mean that when China violates our criminal laws and international norms, we are not going to tolerate it, much less enable it. The FBI and our partners throughout the U.S. government will hold China accountable and protect our nation's innovation, ideas, and way of life — with the help and vigilance of the American people.

Cyber

With the advent of the COVID-19 pandemic, the nature of the cyber threat has become increasingly concerning. As more individuals telework and increasingly use the cloud, we encounter less secure networks. As a result, the scope of our cyber threats has changed, the impact has deepened, and many of the players have become more dangerous as we have become increasingly vulnerable. We are still seeing hack after hack and breach after breach. We hear about it daily in the news. The more we shift to the Internet as the conduit and the repository for everything we use and share and manage, the more danger we are in.

Today we are worried about a wider-than-ever range of threat actors, from multi-national cyber syndicates to nation-state adversaries. And we are concerned about a wider-than-ever gamut of methods continually employed in new ways, like the targeting of managed service providers —MSPs — as a way to access scores of victims by hacking just one provider.

China's Ministry of State Security ("MSS") pioneered that technique and, as you saw in July, we indicted two Chinese hackers who worked with the Guangdong State Security Department of the MSS. These individuals conducted a hacking campaign lasting more than ten years, targeting countries with high technology industries, to include the United States. The industries targeted included, among others, solar energy; pharmaceuticals; and defense. Cybercrimes like these, directed by the Chinese government's intelligence services, threaten not only the United States but also every other country that supports fair play, international norms, and the rule of law, and they also seriously undermine China's desire to become a respected leader in world affairs.

Theft of intellectual property is not the only cyber threat presented by the People's Republic of China ("PRC") government. They are also working to obtain controlled defense technology and developing the ability to use cyber means to complement any future real-world conflict. All of them, and others, are working to simultaneously strengthen themselves, and weaken the United States. And we are taking all these nation-state threats very seriously.

But as dangerous as nation-states are, we do not have the luxury of focusing on them alone. We also are battling the increasing sophistication of criminal groups that place many hackers on a level we used to see only among hackers working for governments. The proliferation of malware as a service, where darkweb vendors sell sophistication in exchange for cryptocurrency, increases the difficulty of stopping what would once have been less-dangerous offenders. It can give a ring of unsophisticated criminals the tools to paralyze entire hospitals, police departments, and businesses with ransomware. Often the hackers themselves have not become much more sophisticated — but they are renting sophisticated capabilities, requiring us to up our game as we work to defeat them, too.

Hackers have not relented under the COVID-19 pandemic. On the contrary, they have attempted to compromise the computer systems of hospitals and medical centers to obtain patient

financial data, medical records, and other information. In addition, such attacks on medical centers may lead to the interruption of computer networks and systems putting patients' lives at an increased risk when America faces its most dire health crisis in generations.

Conclusion

Chairman Johnson, Ranking Member Peters and Members of the Committee, thank you for the opportunity to testify today. I am now happy to answer any questions you might have.

**Hearing before the U.S. Senate Homeland Security and Governmental Affairs Committee
"Threats to the Homeland"**

**Mr. Christopher Miller
Director, National Counterterrorism Center
Office of the Director of National Intelligence**

September 24, 2020

Opening

(U) This year, the United States and its allies have sustained pressure against key terrorist organizations, including al-Qa'ida, ISIS, and groups aligned with Iran, disrupting numerous plots and further diminishing their ability to target the United States and U.S. interests overseas. Concerning al-Qa'ida, U.S. and French operations this year have removed the group's long-time leader in Yemen, Qasim al-Rimi, as well as its veteran commander for North Africa, Abdelmalek Droukdal. Against ISIS, the U.S.-led coalition has continued targeting the group's leadership cadre following the October 2019 raid that removed amir Abu Bakr al-Baghdadi, killing several prominent commanders and hampering the group's resurgence. Finally, the United States and its allies have ramped up diplomatic, military, and economic efforts against Iran and its partners and proxies, including individuals who have conducted attacks that targeted U.S. personnel.

(U) While recognizing these successes, we also understand the challenge of translating these tactical wins into lasting gains. Time and time again, terrorist groups have absorbed similar losses only to reconstitute by exploiting local instability, adapting their tactics, and waiting out CT pressure. We need only refer to AQAP which, despite years of concerted pressure, was able to confer with a U.S.-based violent extremist who went on to kill three Americans at the Naval Base in Pensacola in December 2019, underscoring the resilience of such groups and their threat to the United States. Additionally, jihadist groups continue to stoke and harness instability in a growing number of countries, particularly in Africa, and are accruing new resources and expanding operations. Meanwhile, Iran's intensified use of violence and militant allies to expand its influence in the Middle East heightens the overall threat to U.S. and allied interests.

(U) In the United States, we face the enduring challenge of Homegrown Violent Extremists (HVEs) inspired by the global jihad as well as the growing threat of Domestic Violence Extremists (DVEs). These lone or loosely-organized actors seek to use violence to advance a wide-range of extremist agendas, and their diffuse nature adds to the challenge of detecting and disrupting their activities. Finally, broader global trends including the COVID-19 pandemic, the rapid

development of pertinent technologies including encrypted communications, and the intensifying competition for global influence, all of which may provide terrorists with new opportunities to evade authorities and carry out attacks.

Homeland

(U) We continue to assess that the preeminent terrorist threat to the United States comes from lone-actors or small cells motivated by a diverse range of ideologies. These include HVEs who have conducted three attacks this year, targeting law enforcement personnel and military facilities. DVEs have also been active, conducting three attacks against police and civilians in 2020. The majority of DVE attacks since 2018 have been carried out by Racially or Ethnically Motivated Violent Extremists (RMVEs), whose attacks have been the most lethal of DVE attacks. Some RMVEs in the United States draw inspiration from and are influenced by like-minded violent extremists overseas, who have conducted lethal attacks in at least four countries since 2018. DVEs are aggressively leveraging the online space to recruit new followers, network, and instigate violence. Many of these groups and individuals have sought to exploit and aggravate heightened societal tensions in the United States stemming from the COVID-19 pandemic and protests. My colleagues from FBI and DHS will use their testimony to expand on how these violent extremists are shaping the domestic threat environment.

(U) As NCTC's role in joint analysis to better understand and deter DT actors has grown, we are also realigning resources to enhance our ability to detect and prevent terrorist travel to the United States. These adjustments will strengthen NCTC's role as the national CT identity intelligence leader and further enhance our identity discovery, screening and vetting, and information sharing abilities.

ISIS

(U) U.S. and coalition CT efforts in the past year have killed prominent ISIS leaders and disrupted the terror group's operations in several regions, but the group continues to pursue an aggressive global strategy. Following the death of the group's leader in October 2019, the United States and its partners have successfully targeted other prominent ISIS figures including its spokesman Abu Hasan al-Muhajir and senior leader Hajji Taysir, a veteran member of the group who had overseen the group's insurgent and global terrorism operations. In addition, the United States is working to pressure the group's networks where they're strongest, in Diyala and Kirkuk Governorates in Iraq, and in eastern Syria.

(U) Despite these successes, ISIS has repeatedly demonstrated the ability to rebound from severe losses over the past six years by relying on a dedicated cadre of veteran mid-level commanders, extensive clandestine networks, and downturns in CT pressure to persevere. The group has appointed a new leader, Muhammad Sa'id Abdal-Rahman al-Mawla—also known as Hajji Abdallah—and its spokesman in May trumpeted recent attacks in Iraq and Syria and promised additional operations around the world. The group has conducted a steady rate of assassinations, and IED and mortar attacks in mostly rural parts of northern and central Iraq and

eastern Syria, including a series of assaults in May that killed and wounded dozens of Iraqi soldiers. These operations are celebrated in graphic propaganda videos that showcase the group's battlefield prowess. ISIS is also working to release thousands of terror group members and their families currently detained in prisons and living in camps in northeastern Syria, where our foreign partners face growing security and humanitarian challenges.

(U) Outside of Iraq and Syria, ISIS continues to prioritize the expansion and reinforcement of its global enterprise, which now encompasses approximately 20 branches and networks. In January, the group's chief spokesman heralded the group's growth and pledged to expand its attacks including against Israel, echoing earlier statements made by Abu Bakr al-Baghdadi prior to his death. Since last year, ISIS leaders have touted the strength of the group's transnational network by launching five global campaigns that incorporate attack claims and propaganda videos from its branches and networks. Individually, these ISIS branches and networks have made uneven progress in advancing the group's agenda. In several parts of Africa, ISIS groups conduct frequent attacks against local security forces and have expanded their safe havens, while coalition operations and attacks from local rivals have stunted the group's growth in Afghanistan, Libya, Somalia, and Yemen.

(U) ISIS continues to seek out avenues for external operations against the West, although CT pressure has diminished the group's ability to execute operations on the scale of previous attacks in Paris and Brussels. ISIS leaders have repeatedly called on supporters in the West to conduct attacks, including attacks using toxic substances, and reiterated these calls in July in its first English-language video in 18 months since the death of the group's last official English translator. ISIS-inspired attacks in the West have declined significantly since 2015 in part because authorities around the world continue to detain local ISIS adherents some of whom were planning terrorist attacks or attempting to join the group.

Al-Qa'ida

(U) CT pressure against al-Qa'ida has diminished its cadre of veteran leaders and ability to strike the West, but the group's global network still poses a significant threat to U.S. and allied interests. Al-Qa'ida's significant leadership losses include AQIM leader Abdelmalek Droukdal in June 2020, AQAP leader Qasim al-Rimi in January 2020, the leader of AQIS in September 2019, and several senior Syria-based leaders, including deputy amir Khalid al-Aruri and Sari Shihab. However, several of the group's remaining senior leaders continue to find safe haven in Iran, and will likely play a key role in the group's efforts to reconstitute its leadership.

(U) Leadership losses have not diminished the group's determination to strike American and Western targets. Through its propaganda, al-Qa'ida leaders continue to exhort their adherents to strike U.S. persons and installations: in February, AQAP media hailed the Pensacola attack and issued a call for supporters to attack U.S. and Israeli interests around the world. Earlier propaganda lauded al-Shabaab's attacks against U.S. military personnel in Kenya and Somalia, linking those operations to al-Qa'ida's global response to the movement of the U.S. embassy

from Tel Aviv to Jerusalem. Al-Qa'ida has also attempted to capitalize on global unrest and the COVID-19 pandemic in its media products and messaging.

(U) Al-Qa'ida's reach is sustained through its affiliate groups in Asia, Africa, and the Middle East, which continue to launch attacks against local governments, expand their territory, and look for opportunities to advance the group's transnational agenda by striking U.S. or Western targets. In Somalia, al-Shabaab controls large parts of the country despite significant CT pressure, using these safe havens to sustain a relentless insurgent campaign against the Somali government and African Union Mission to Somalia (AMISOM) forces. Earlier this year, the group launched an attack on a joint U.S. and Kenyan military base at Manda Bay airfield and killed three Americans, highlighting the group's external reach and determination to strike U.S. interests. Al-Shabaab also linked its attack against a hotel in Kenya in January 2019—which killed one American—to al-Qa'ida's global campaign targeting the U.S. and Israel.

(U) As noted previously, AQAP continues to threaten U.S. interests, underscored by its communication with the Pensacola attacker and its subsequent claim of responsibility. In Yemen, continued fighting amongst warring factions and the withdrawal of some CT forces have helped the group sustain some operations and territory despite continued CT pressure. However, the group's ability to exploit these opportunities and expand its safe havens has been undermined by the loss of Rimi and other prominent operatives, internal tensions, and battles with other local factions, including the Huthis. In Syria, Hurras al-Din—a group made up of several al-Qa'ida veterans—has suffered successive losses of key leaders and operatives, which, along with conflicts with other violent extremist factions and the erosion of its safe haven in Idlib Province, has stunted the group's growth. As of late June, battlefield conflicts between Hurras al-din and the Nusrah Front continued to escalate prompting al-Qa'ida to issue a public statement condemning the fighting.

(U) In North Africa, the loss of Al-Qa'ida in the Islamic Maghreb (AQIM) leader Abdulmalek Droukdal is the latest setback suffered by the group since 2018, but it will probably continue to provide guidance to other al-Qa'ida elements in the region despite its own lack of attacks. In West Africa, al-Qa'ida-affiliated group Jama'at Nusrat al-Islam wal-Muslimin (JNIM) has exploited growing instability to expand its operations and carry out attacks—including a complex VBIED and indirect fire attack that killed one and wounded two French soldiers at a French military camp in Mali on 23 July—against local and Western government and security targets in the region and rivals aligned with ISIS.

(U) In South Asia, al-Qa'ida in the Indian Subcontinent (AQIS) has struggled to rebound from the death of its leader, Asim Umar, in a U.S. military raid in Afghanistan in September 2019 and is probably only capable of small-scale regional attacks. Additionally, in mid-March, AQIS published a special issue of Nawai Afghan Jihad praising the U.S.-Taliban agreement, which mirrored al-Qa'ida's leaders' statements on the deal. Finally, al-Qa'ida's presence in Afghanistan has been reduced to a few dozen fighters who are primarily focused on their survival, and are probably incapable of conducting attacks outside the country under sustained CT pressure.

Iran, Lebanese Hizballah, and other Terrorist Groups

(U) In addition to the global jihadist challenge, the U.S. faces a confrontation with Iran, which remains the world's foremost state sponsor of terrorism. Tehran views terrorism as a key tool to counter U.S. influence and uses the Iranian Islamic Revolutionary Guard Corps-Quds Force (IRGC-QF)—which is a component of a designated foreign terrorist organization—to provide weapons, funding, and training to a range of terrorist and militant partners and proxies throughout the Middle East. Following the U.S. military operation that targeted IRGC-QF chief Qasem Soleimani in January, Iranian leaders promised to take revenge and accelerate their efforts to eject the U.S. from the region.

(U) In Iraq, Tehran supports several Shi'a terrorist groups including U.S. designated FTOs Kata'ib Hizballah (KH) and Asa'ib Ahl al-Haqq (AAH), which in the past two years have conducted an increasing number of indirect fire attacks against U.S. diplomatic installations, including the U.S. embassy in Baghdad, and military installations in Iraq, killing three Americans. These groups—which continue to receive advanced weaponry and training from their Iranian backers—have pledged to exact revenge for the death of a senior militia leader in the same U.S. military operation that killed Soleimani and have pledged to force the U.S. military to withdraw from Iraq. In the Palestinian territories, Iran backs terrorist groups including HAMAS and the Palestine Islamic Jihad, which regularly targets Israel. Tehran also works with militants in the Arabian Peninsula to counter U.S. allies including Saudi Arabia and Bahrain.

(U) Iran also continues to support Lebanese Hizballah, which uses its sophisticated terrorist apparatus to advance Tehran's regional strategy. Following the death of Soleimani, Hizballah leader Hassan Nasrallah called for retaliation including against U.S. military personnel in the Middle East, and has blamed the U.S. for the German Government's recent ban of the group's operations. We are closely monitoring for indications of how political and economic fallout from the Beirut explosion could impact the group's position in Lebanon. Within Lebanon and the broader region, the group has expanded its stocks of advanced weapons systems including Unmanned Aerial Systems (UAS) and long-range rockets while deploying trainers to Yemen to train the Houthis, threatening U.S. allies. Finally, Hizballah's global terrorist operations arm—the Islamic Jihad Organization (IJO)—has in recent years deployed operatives to almost every continent and extended its reach into the United States: since 2019, two U.S.-based individuals have been jailed for scouting potential targets on the group's behalf.

(U) Finally, Iran continues to employ and support terrorism outside the region, potentially including the United States. In 2018, two Iranians were arrested in the U.S. for surveilling Iranian oppositionists and Jewish and Israeli groups and passing the information to Iran. In Europe, Iranian operatives since 2018 have been implicated in two unsuccessful terrorist plots in Denmark and Belgium.

Challenges

(U) I'd like to highlight and briefly discuss three broader trends that will increasingly influence the U.S. CT campaign in the coming years.

(U) **COVID-19 and Heightened Instability** – The COVID-19 pandemic may fuel greater instability and degrade humanitarian conditions in several parts of the developing world, providing terrorists with opportunities to undermine local governments and expand their safe havens. Prior to the outbreak, terrorist groups were already enjoying success exploiting endemic instability to entrench and expand in parts of Africa and the Middle East. In these regions, local authorities often lack the capability or will to mitigate the terrorist threat, while intractable conflicts and economic instability render society vulnerable to violent extremist encroachment. The spread of COVID-19 may worsen these conditions by sapping governments' CT and security resources and depressing local economies. Meanwhile, terrorists have recognized the potential opportunities of the COVID-19 pandemic and have accelerated attacks against over-extended security forces, used propaganda to blame the outbreak on their enemies or characterize the disease as divine punishment, and moved to undermine civilian confidence in the ability of local governments to care for civilians.

(U) **Great Power Competition** – Sustaining pressure against key terrorist threats amidst the intensifying contest for influence amongst major global powers will pose a growing challenge for the U.S. Increasingly, U.S. adversaries like China and Russia are expanding their military footprint and security partnerships in regions where the U.S. has critical CT equities, including Africa, Asia, and the Middle East. Both powers regularly use their overseas presence to secure new influence, attempt to diminish U.S. power, and showcase their own CT capabilities, efforts that can complicate U.S. efforts against ISIS and al-Qa'ida. In addition, the U.S. Government's reapportionment of resources to better meet the challenge of heightened global competition will place pressure on the CT community to prioritize high-impact strategies targeting those groups that pose the most severe threats to U.S. interests.

(U) **Emergent Technologies** – The CT community is moving aggressively to keep pace with the rapid development of pertinent technologies including advances in dual-use technology, UAS, 3D printing, ubiquitous end-to-end encryption, cryptocurrency, and new social media platforms, a complex challenge that demands a whole-of-government response and partnership with private industry. Terrorists have historically proven adept at harnessing these and other emergent technologies to disseminate their propaganda, attract new members, advance their weapons capabilities, and support operations, including the development of chemical, biological, radiological, or nuclear (CBRN) capabilities. Regarding social media, terrorist groups are increasingly transitioning to smaller, less-visible platforms to share content following intensified voluntary efforts by prominent companies to restrict violent and extremist material consistent with their terms of service. Terrorists are also looking to exploit the move towards greater encryption to safeguard their communications. For its part, in coordination with State, FBI and DHS, NCTC has worked with U.S. technology companies, including several members of the Global Internet Forum to Counter Terrorism (GIFCT), a private industry initiative and now a

non-governmental organization, to provide technology companies with information about how terrorists use the internet, including specific key words and logos. The Center has also worked with members of the GIFCT to help identify terrorist content.

Closing

Since the Global War on Terror began nearly two decades ago, we've significantly degraded our terrorist adversaries and made the United States a considerably harder target for them to reach; today's terrorism threat to the U.S. and our allies is less acute but more diffuse—emanating from more groups in more places than it did in 2001. Technological innovation, great power competition, and instability resulting from a global pandemic are only a few of the factors that will make this landscape increasingly complex in the coming year. These challenges necessitate a dynamic response that evolves along with our adversaries and applies lessons learned to adapt for the future. At NCTC, we are committed to combatting this adversary and are innovating new ways of doing business to ensure that we are best aligned to connect the dots amidst a flood of ever-changing information. What remains constant is our commitment to the mission and to supporting our partners in their unrelenting efforts to sustain pressure against terrorists and violent extremists spanning an ideological spectrum around the globe.



TESTIMONY OF

The Honorable Ken Cuccinelli
Senior Official Performing the Duties of the Deputy Secretary
U.S. Department of Homeland Security

BEFORE

United States Senate
Committee on Homeland Security and Government Affairs

ON

“Threats to the Homeland”

Thursday, September 24, 2020
Washington, DC

Good morning Chairman Johnson, Ranking Member Peters, and distinguished members of the Committee. Thank you for the opportunity to testify before you on behalf of the Department of Homeland Security (DHS) regarding today's threats to the Homeland. Born out of the ashes of 9/11, the American people tasked DHS with one purpose: to protect this great Nation and keep our citizens safe.

As Acting Secretary Wolf said in his recent State of the Homeland remarks, "the Department of Homeland Security is bound by one mission, one creed. Answering the call, often times in the most arduous of environments and difficult of circumstances, to safeguard the American people, our homeland, and our values from all threats, all the time—both today, tomorrow, and in the months and years to come."

Although the threats facing our nation 17 years ago when DHS was founded have evolved significantly, DHS continues to be motivated to adapt in order to address these new and emerging threats.

DHS addresses these emerging threats with a clear mandate from President Trump: the safety, security and prosperity of the American people comes first. DHS, using our unique authorities, and in collaboration with our federal, state and local partners, will continue to make good on this promise.

Indeed, under the leadership of President Trump, the 240,000 men and women of the DHS family have been empowered to overcome new and challenging threats, as well as accomplish our enduring no-fail missions. Specifically:

- We are combating crises at the Southern Border—such as human trafficking, drug smuggling, and unprecedented illegal migration flows—while restoring integrity to the immigration system;
- We are maintaining vigilance against terrorist threats, foreign and domestic, within the bounds of our authorities;
- DHS has been a part of the Whole-of-America response to COVID-19, leveraging every aspect of our federal government through a locally-executed, state managed, and federally-supported strategy;
- We are protecting federal buildings and federal workforce, including federal law enforcement officers, from an emerging threat of violent rioters;
- We are preparing for and responding to natural disasters;
- We are identifying and preventing malign foreign actors and nation states from interfering in our elections and protecting our election infrastructure, as part of our broader mission to safeguard and secure cyberspace; and
- We are aggressively responding to the threat posed by China—now and in the future.

Border Security

Nearly four years ago, the American people elected President Trump with a mandate to secure our borders and enact an America First immigration policy.

To stem the tide of human smuggling, drug smuggling, and criminal gangs flooding across our border and into our country, the Trump Administration has constructed more than 300 miles of the border wall system. Our work is not finished. We are on track to complete 450 miles by the end of 2020.

We have interdicted more than 4 million pounds of illegal drugs on the Southern Border, including methamphetamine, cocaine, as well as fentanyl and drug analogues originating from China. Most of these drugs are supplied by transnational crime organizations making billions in profits while tens of thousands of Americans die due to overdoses. With these efforts, the Trump Administration has inhibited the ability of these transnational criminal organizations to further devastate our communities—including every congressional district in America.

Restoring Integrity to the Immigration System

Building the wall system is not a stand-alone solution to these problems. The wall fits into a greater, holistic approach to secure the border.

Through President Trump's diplomatic agreements and arrangements with our neighbors to the south, our allies have taken steps to secure their own borders. These include historic border security arrangements with Guatemala, Honduras, and El Salvador. A secure Mexico means a secure United States. A secure Honduras means a secure United States. A secure El Salvador and a secure Guatemala means a secure United States.

Under President Trump, we have made regulatory changes to enforce our immigration laws as Congress originally intended. We also have been able to enact a common-sense approach that not only supports our national security requirements but also protects the American worker. We have done so by terminating the dangerous "catch and release policy" and closing loopholes that led to asylum fraud and employment authorization abuse.

Our immigration system is not only designed to support national security requirements, but also protect American workers. Tightening our immigration system also fortifies economic security. The days are over of looking the other direction while allowing unfettered illegal foreign labor to flood our domestic labor markets, depress American wages, and strain our municipalities.

Terrorism

The nation continues to face threats from foreign and domestic terrorists inside our borders—the threats that animated the Department's founding.

I'm proud to stand with the Acting Secretary and say that DHS has taken unprecedented actions to address all forms of violent extremism.

Last year, the Department released a comprehensive strategy that contextualizes the threats from violent extremists and lays out the DHS mission in preventing such violence. We secured—with help from Congress – additional funding in FY 2020 for these initiatives. And the President

requested a 300% increase in funding for DHS-wide efforts in this area in his FY 2021 Budget Request.

We recently released a Public Action Plan that outlines dozens of separate actions across the DHS enterprise designed to combat domestic terrorism, and just yesterday announced our FY20 Terrorism Prevention grant recipients.

Let me be clear: DHS stands in absolute opposition to any form of violent extremism. We will continue our daily efforts to combat all forms of domestic terror.

COVID-19 Response

Of all the threats DHS has confronted in the last year, the COVID-19 pandemic has posed one of the most formidable, rapidly evolving, and uniquely challenging.

President Trump's decisive and rapid action led our federal government to pursue a Whole-of-America response, which continues to deliver results through a locally-executed, state-managed, and federally-supported strategy.

Early on, President Trump acted swiftly, banning travel from hot spots like China, to mitigate the impact of COVID-19. Despite criticism from certain politicians, the President's action saved lives. Our efforts to secure the border also directly correspond to DHS' unique authorities and mission to combat the spread of COVID-19.

CBP and FEMA play a particularly important role in serving the American people during this crisis.

On the domestic front, FEMA has marshalled all available resources to support President Trump's strategy to combat the pandemic and safely reopen America. FEMA processed the first ever nationwide emergency declaration under the Stafford Act. This was in addition to simultaneous major disaster declarations granted to all 50 states, 5 territories, and the District of Columbia.

Following the emergency declaration, the Centers for Disease Control and Prevention (CDC) requested DHS assistance in enforcing the Director's order issued under Title 42, which suspended the introduction into the United States of certain persons from countries where a communicable disease exists. To date, CBP has halted and expelled over 90 percent of aliens crossing the Southern Border within two hours of encountering them—an incredible feat and of critical importance to the public health and the protection of our workforce in response to COVID.

Under President Trump's direction, we utilized the Defense Production Act to procure more than 220 million respirators from the 3M Company, saving American lives. By taking historic action to better collaborate with the private sector, we have helped deliver and allocate billions of pieces of scarce PPE to our frontline healthcare workers and first responders.

FEMA has delivered millions of units of personal protective equipment (PPE) to our federal, state, territorial, and tribal government partners, allocated billions of dollars in public and individual assistance, and provided tremendous guidance to local officials.

In August, in the absence of Congressional action, President Trump authorized FEMA to use \$44 billion from the Disaster Relief Fund to alleviate the effects of lost wages due to COVID-19, allowing states to make supplemental payments to those receiving unemployment insurance compensation. FEMA acted in short order. As of September 8, FEMA has already provided more than \$29 billion to 47 states for Lost Wages Assistance to support American workers.

Civil Unrest/Riots

While responding to the pandemic, we have simultaneously worked to combat the violence that has erupted in several metropolitan areas across the country.

In cities like Portland, Oregon, arsonists, looters, and agitators attacked federal property, law enforcement officers, and local small businesses.

For more than 60 days, DHS law enforcement personnel in Portland were under siege by a violent mob intent on destroying a federal courthouse. Federal law requires DHS to protect buildings, grounds, and property that are owned, occupied, or secured by the Federal government and the people on that property. Despite hundreds of injuries, our officers courageously held the line and fulfilled their statutory duty to defend federal property.

President Trump has offered federal assistance to every community that has suffered from this type of violence. DHS is proud to support our Department of Justice counterparts as they execute their Constitutional mandate to keep order in American cities when requested by our local partners and governments.

DHS is ready to assist in restoring peace should the communities request our support.

Natural Disasters

The Department continues our role overseeing natural disaster response efforts during these unprecedented times.

DHS recognized early on that we would likely have to respond to the 2020 hurricane season while also continuing our efforts to counter COVID-19.

As Hurricane Laura was about to make landfall just last month, President Trump immediately authorized emergency disaster declarations for Texas, Louisiana, and Arkansas. And DHS personnel are responding to Hurricane Sally as we speak.

The President's decisive action and FEMA's prevention and preparedness measures continue to enable DHS to rapidly respond to that hurricane and any future natural disasters.

Election security

DHS is committed to ensuring that our election system functions free from interference, both foreign and domestic. In that vein, the Administration has continually called out malign actors, such as China, Russia, and Iran, which seek to interfere in our elections and threaten our democracy.

DHS, through our Cybersecurity and Infrastructure Security Agency (CISA), continues to make progress securing the election systems and our nation's critical infrastructure. The 2018 midterm elections were the most secure in modern history, and DHS is working diligently with state and local election officials to make the 2020 elections even more secure.

As such, CISA is currently working with representatives from all 50 states, thousands of local jurisdictions, and our election technology partners to make sure they have the resources they need to keep our elections secure and resilient.

Securing Cyberspace and Emerging Threats

Cyber threats to the homeland, from both state affiliated actors and cyber criminals have been and will remain one of the most prominent threats facing our nation. All levels of government and entities across the private sector, to include the vast array of critical infrastructure upon which we rely, are facing a constant barrage of multifaceted cyber-enabled threats. These threats are designed to access and collect sensitive information, to hold operational technology at risk, and interrupt the accessibility of vital networks.

DHS, including through the operations of CISA, the United States Secret Service, the U.S. Coast Guard, ICE-Homeland Security Investigations, and the Transportation Security Administration, is, leveraging its full suite of authorities to mitigate this cyber threat, increase the resilience of those systems upon which our critical infrastructure sectors rely and impose costs on malicious cyber actors looking to leverage vulnerabilities for financial or other gain.

In addition, DHS, through its Science and Technology Directorate, works in collaboration with CISA and our federal partners to characterize and better understand emerging technological and science-based threats facing our nation's critical infrastructure.

China

Surveying the threat landscape, one menacing actor is ever-present—China.

In the midst of our complex challenges, DHS must also confront an aggressive nation-state. The Chinese Communist Party (CCP) seeks to assert its influence in both overt and covert ways to achieve a variety of geopolitical and domestic goals. The Peoples Republic of China's (PRC) increasingly aggressive and bold actions—from undermining long-standing Hong Kong autonomy to attempting to build a data collection network that spans the globe—imperils the United States and the international rules-based order that DHS has helped to sustain and enforce since its inception.

Across a wide range of policy spheres, from threatening U.S. economic security and prosperity, to undermining the core notion of a secure representative democratic process, DHS is on the frontline of growing tensions with the PRC.

President Trump has taken unprecedented action issuing a presidential proclamation restricting travel of certain Chinese graduate students and researchers with ties to entities in China supporting China's military-civil fusion strategy to prevent them from stealing and otherwise appropriating sensitive research. DHS is working closely with the Department of State to enforce that presidential proclamation.

We are targeting illicit Chinese manufacturers who have exploited the COVID-19 pandemic by producing fraudulent or prohibited PPE and medical supplies that especially endanger our front-line workers.

We are preventing goods produced by forced labor from entering our markets and demanding that China respect the inherent dignity of each human being. CBP continued that effort just this week with the announcement of five Withhold Release Orders.

At our borders and our ports of entry, we are leveraging technology and innovation to target and interdict deadly Chinese-made fentanyl and fentanyl-like substances before they can destroy American communities and take American lives.

DHS is working with our interagency and industry colleagues to protect our information and communications infrastructure from intellectual property theft and nefarious data collection by China.

China's relentless barrage of attacks aimed at undermining American workers, American economic dominance, and the American way of life cannot be allowed to stand—and under President Trump, it won't. A policy of appeasement is not an option; it is a proven road to failure.

The power dynamic DHS is witnessing between the United States and China will be a focus for many years to come. In the near-term, DHS will continue to relentlessly respond to the threat posed by Beijing, consistent with the National Security Strategy and the Strategic Approach to the People's Republic of China.

Conclusion

DHS continues to demonstrate its ability to take on and overcome wide ranging and diverse threats.

As we seek to fulfill our mission, the men and women of DHS look forward to continued cooperation with Congress so that together we can keep our citizens safe and secure.

**Post-Hearing Questions for the Record
Submitted to Hon. Christopher Wray
From Senator Gary C. Peters**

“Threats to the Homeland”

September 24, 2020

*****Due to the change-over in Administration, responses were not received to these questions for the record.*****

1. You recently noted that the Russians were more interested in information operations than in actual hacking of election infrastructure. In the event that attacks were to occur, do you have the partnerships in place to identify when it happens?
 - a. Generally, are these operations we expect to be able to identify in real time or close to it?
2. In your recent testimony before the House, you noted that the greatest threat to the homeland is not one ideology or organization, but “lone actors largely self-radicalized online who pursue soft targets using readily accessible weapons.” The FBI has briefed HSGAC staff that the majority of domestic terrorism attacks have come from “racially motivated” attacks. Can you please tell us the breakdown in that racial motivation – what percentage are due to white supremacist attacks, versus other racial motivations?
 - a. What specific steps have you ordered the FBI take to respond to the threat of white supremacist violence?
 - b. How exactly is the FBI allocating limited counterterrorism resources to address this threat?
3. You noted in recent testimony that the FBI has been working more closely with social media companies to help address the threat of disinformation related to the election, but said that you would “like to see more progress” from these companies. What more do you want to see from these companies? How can they be more effective at addressing this threat?
 - a. How can Congress help provide oversight of these companies and combat disinformation?
4. One of the threats identified after the 2016 election was an extensive Russian hacking effort of election systems including voter registration databases. While an Election Day attack on these databases could have incredible impacts on voting – absentee voting may help mitigate this risk. Would you agree that early and absentee voting could mitigate the potential impact of an Election Day hacking operation by ensuring a significant percentage of voters are already validated and have received ballots?

**Post-Hearing Questions for the Record
Submitted to Hon. Christopher Wray
From Senator Kyrsten Sinema**

“Threats to the Homeland”

September 24, 2020

*****Due to the change-over in Administration, responses were not received
to these questions for the record.*****

1. Director Wray, in your opening statement at the hearing, you stated that hostile foreign actors and opportunistic criminal elements have seized upon this moment in time when the United States faces unprecedented challenges because of the COVID-19 pandemic. I also think it's fair to say the pandemic itself has served as a hostile actor, disrupting our economy and workforce, and killing over 210,000 Americans. What additional steps does the FBI need to take from a law enforcement perspective to respond to these hostile actors that are using COVID-19 to advance their agendas?
2. The Cyberspace Solarium Commission report was presented to the public in March of 2020 and recommended the creation of a National Cyber Director who would sit in the Executive Office of the President and oversee activities across the government for cybersecurity. Do you agree with this recommendation? Why or why not?
3. During this hearing, a number of different critical threats were discussed, all of which are important. What threats should Congress be examining that are currently flying under the radar or did not receive enough attention during the hearing?

*****Due to the change-over in Administration, responses were not received
to these questions for the record.*****

**Post-Hearing Questions for the Record
Submitted to Hon. Christopher Wray
From Senator Jacky Rosen**

“Threats to the Homeland”

September 24, 2020

*****Due to the change-over in Administration, responses were not received
to these questions for the record.*****

1. In the last fiscal year, the FBI has arrested over 100 domestic violent extremists. Statistics show that racially and ethnically motivated violent extremism were the primary source of all lethal domestic terrorism incidents in the last two years. From Pittsburgh to El Paso, in recent years we all have tragically witnessed the deadly effects of hate and bigotry.
 - a. Why doesn't the FBI Counterterrorism Division maintain a section to specifically investigate domestic terrorism?
 - b. Does the FBI collect data specifically on the white supremacist threat, including violent acts of anti-Semitism, which have increased in recent years?
 - c. What does the FBI need from Congress to ensure law enforcement agencies have the resources to protect Americans from the growing threat of racially and ethnically motivated violent extremists?
2. Domestic terrorists are increasingly harnessing existing and emerging technologies to disseminate their propaganda, recruit new members, and evade law enforcement. Terrorists are using encryption to safeguard their communications, and social media is being exploited to spread hate and bigotry, and encourage violence. Social media is also enabling domestic terrorists to create transnational ties by coordinating with groups abroad.
 - a. How is the FBI working to keep pace with the rapid development of emerging technologies and their use by violent extremists, both at home and abroad?
 - b. How can Congress better empower federal law enforcement to combat online hate? What can we learn from examples in other countries, including in Europe?

*****Due to the change-over in Administration, responses were not received
to these questions for the record.*****

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20510

JAN 19 2021

The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20510

Chairman Johnson and Ranking Member Peters:

(U) The enclosed document responds to Questions for the Record following the "Threats to the Homeland" open hearing on 24 September 2020.

(U) If you have any questions, you may contact Legislative Affairs at (703) 275-2474.

Sincerely,



Robert L. Cooper
Acting Assistant Director for
Legislative Affairs

Enclosures:

1. (U) Responses to Questions for the Record from 24 September 2020 Hearing before the Committee on Homeland Security (U)

UNCLASSIFIED

UNCLASSIFIED

**Post-Hearing Questions for the Record
Submitted to Hon. Christopher Miller
From Senator Jacky Rosen**

“Threats to the Homeland”

September 24, 2020

1. QFR: Domestic terrorists are increasingly harnessing existing and emerging technologies to disseminate their propaganda, recruit new members, and evade law enforcement. Terrorists are using encryption to safeguard their communications, and social media is being exploited to spread hate and bigotry, and encourage violence. Social media is also enabling domestic terrorists to create transnational ties by coordinating with groups abroad. How is the National Counterterrorism Center working to keep pace with the rapid development of emerging technologies and their use by violent extremists, both at home and abroad?

NCTC RESPONSE: NCTC has teams throughout its four directorates that use all-source data derived from partners across the USG and open source information to produce insights and analysis on terrorists' current and aspirational use of technology. These analysts closely monitor terrorists' use of encryption, social media, artificial intelligence, unmanned systems, additive manufacturing, cybercrime and attacks, technical security measures, as well as online payment technologies including cryptocurrencies. They are in almost daily contact with operational, analytic, and technical partners throughout the IC, the Department of Defense, and other government organizations to help drive collection and identify new trends related to terrorists' use of emerging technology. Analysts use their findings to support policymakers, warfighters, state and local law enforcement, foreign partners, and, as appropriate, the private sector by identifying tailored opportunities to prevent terrorists' use of emerging technologies to plan, recruit, or otherwise further terrorism.

- NCTC's Tech-Sector Outreach and Research (TOR) Cell engages with U.S. tech-sector companies and provides timely and value-added strategic information to assist companies' identification of terrorist content online –including terrorist tactics and tradecraft – which companies may determine should be deleted under their Terms of Service or other user agreements or policies.
- NCTC's team responsible for threat finance analysis engages with its interagency partners, including the Departments of Treasury and Justice, as well as with the U.S. financial sector to closely track emerging financial trends and assist with the identification and disruption of financial facilitation activities
- NCTC data scientists and a center-wide data strategy group focus on improving the technology available to the IC CT enterprise – through information sharing, discovery and correlation, identity and knowledge management, and big data integration – to better integrate USG CT data.

UNCLASSIFIED

UNCLASSIFIED

**Questions for Record from Committee on Homeland Security
Submitted to Hon. Christopher Miller**

"Worldwide Threats to the Homeland II"

17 September 2020

1. QFR: Last year, reporting by media discussed NCTC's expansion of "its focus on domestic terrorism." Please provide the Committee with an update as to what work NCTC is doing today on domestic terrorism, including violent white supremacist extremist violence. To what extent has NCTC staffed and funded its work on domestic terrorism?

NCTC RESPONSE: On 16 January 2020, the Office of the Director of National Intelligence (ODNI) issued a Congressional Notification (CN): Enhancing NCTC Support on Racially and Ethnically Motivated Violent Extremist Threats, including Domestic Terrorism and Overseas Linkages. The CN noted the inclusion in the October 2018 National Strategy for Counterterrorism of the persistent domestic terrorism (DT) threat and its corresponding direction to departments and agencies, where lawful and appropriate, to investigate ties between domestic terrorists and their overseas counterparts to better integrate DT information into analysis of homeland threats and related information sharing efforts. The CN described, at a classified level, NCTC's measured steps to enhance DT support to operating agencies of the CT community, principally the Federal Bureau of Investigation (FBI) as the lead federal agency responsible for countering DT. Since that time, NCTC has continued its support as described in the CN. NCTC has also instituted mandatory training for personnel who will work on DT related assignments to ensure the workforce understands NCTC's authorities in its supporting role, privacy and civil liberties safeguards, as well as other applicable requirements. NCTC prioritizes its key lines of effort commensurate with the most acute threats to national security, as identified by the President and the DNI, including through the National Intelligence Priority Framework and the National Strategy for Counterterrorism.

2. QFR: Al-Shabaab recently claimed responsibility for numerous attacks in East Africa, including an attack on a U.S. base as recently as September 2020 that injured a U.S. service member. Please describe the current threat posed by Al Shabaab to U.S. interests and U.S. service members and law enforcement agents posted overseas.

NCTC RESPONSE: The IC assesses that al-Shabaab poses a persistent threat to USG, military and civilian persons, as well as facilities throughout Somalia and Kenya. The IC bases its assessment on al-Shabaab's public statements vowing revenge on U.S. interests, previous attacks directed at U.S. personnel in retaliation for U.S. drone strikes and attacks on and threats to attack public places that USPERs would patronize.

3. QFR: According to analysis by the Congressional Research Service, Al-Qaeda has welcomed the U.S.-Taliban agreement, "celebrating it as a victory for the Taliban's cause and thus for

UNCLASSIFIED

UNCLASSIFIED

global militancy." Recent reporting states that "two senior Trump Administration officials indicated... that the Taliban has yet to fully cut ties with Al-Qaida." Given that the U.S.-Taliban agreement requires the Taliban to prevent any group, including Al Qaeda, from using Afghan soil to threaten the security of the U.S. or its allies, what mechanisms are in place or need to be in place to verify the Taliban's compliance with the February 2020 U.S. - Taliban agreement?

NCTC RESPONSE: The U.S. is leveraging diplomatic engagement and intelligence reporting—along with reporting from our Coalition partners and allies—to monitor developments relevant to CT assurances made by the Taliban in the February 2020 U.S.-Taliban Agreement. Although the U.S. commitment to decrease our military presence in Afghanistan will probably result in a reduction in our ability to verify Taliban compliance with the agreement, NCTC is deeply engaged in exploring options to mitigate such losses and preserve insight into a range of issues and threats in the Afghanistan-Pakistan region.

4a. QFR: Politico recently reported that your predecessor, Former Director Travers, stated that NCTC's "information technology system is woefully underfunded." Is NCTC's information technology system underfunded?

NCTC RESPONSE: In 2019 and 2020, the DNI approved the addition of funding to the NCTC budget for the TIDAL initiative. TIDAL is a multi-year development program as part of the Identity Intelligence (I2) Enterprise, extending from FY 2020 through FY 2025, designed to modernize the information technology (IT) used to manage the nation's repository of Known and Suspected Terrorists; speed the process by which the CT community nominates and enhances terrorist identities; significantly increase NCTC's screening and vetting capabilities to accommodate expected growth in the volume and variety of national security vetting requests; and, greatly improve data discovery and sharing across NCTC and with our CT mission partners through the creation of the NCTC Data Lake and ancillary services. In addition, NCTC has prioritized the execution of its base IT budget to address a number of chronic infrastructure deficiencies, ensure the protection of our data, and transition systems into the cloud environment to be part the I2 Enterprise architecture sharing identity information as appropriate and improve performance and resiliency. Sustainment of these efforts will further enable NCTC to execute its mission into the foreseeable future.

4b. QFR: What does the agency need to do its job, and do its job well in this increasingly diverse and fluid threat environment?

NCTC RESPONSE: As we look towards the future, NCTC is evaluating avenues to incorporate transformative technologies, such as Artificial Intelligence/ Machine Learning, natural language processing, and expanded biometrics. We are collaborating closely within ODNI to examine ways to increase the amount of development work that can be done within the unclassified environment, which will expand the talent pool, as well as to reduce the time required for security clearances and system accreditations.

UNCLASSIFIED

UNCLASSIFIED

5. QFR: Earlier this year, the State and Treasury Department labeled the Russian Imperial Movement (RIM) a Specially Designated Global Terrorist group. Since this designation, have you seen an increase in Watch list nominations of individuals with links to White Supremacist Extremists? Please provide details and explain.

NCTC RESPONSE: Since the terrorist group designation of the RIM on 06 April 2020, by the State Department, NCTC saw approximately 150% increase in new identities nominated to TIDE who are related to RIM. This review also resulted in the addition of first time biometrics for the leaders, along with enhancements for the remaining existing RIM members. While researching RIM leadership, new RIM members were discovered and added to TIDE, resulting in enhancements, including first time biometrics, and a Selectee upgrade. The majority of new RIM subjects nominated to TIDE since April 2020 have been from the Defense Intelligence Agency's Defense Combatting Terrorism Center.

6. QFR: The Chief of U.S. Central Command has said that displaced persons in camps in the Middle East may be radicalized and susceptible to influence later by ISIS. He went on to say that dealing with refugees and displaced persons is one of very highest priorities, while noting that victory against ISIS has not yet been achieved. How are you working with the Department of Defense to achieve these objectives in contributing to the defeat of ISIS?

NCTC RESPONSE: NCTC closely monitors and publishes finished intelligence products on ISIS recruitment and radicalization and mobilization to violence in displaced persons camps in Syria as part of ongoing efforts to track ISIS-linked foreigners in the camps and analyze the group's organizational health and operational strategy. These products are shared with Department of Defense (DOD) entities to inform their engagements with local partners and their planning on the ground, including efforts to biometrically enroll foreign residents of the camp. NCTC also participates and briefs in interagency policy meetings led by the State Department and DOD on this topic to create a common intelligence picture. We would defer to colleagues in both departments for additional information.

We share General McKenzie's concern about the risk of ISIS recruitment and radicalization and mobilization to violence in displaced persons camps. There are two camps in Northeastern Syria that house ISIS family members that fled the group's last stronghold in Baghuz in March 2019. Al-Hawl is the largest of these camps and houses nearly 70,000 mostly women and children, including approximately 10,000 foreigners from 60 countries. The IC believes that most of the camp residents either have no affiliation to ISIS or are disillusioned with the group to which they are linked by circumstance; however, a small subset—many of whom are foreigners—are deeply committed to ISIS ideology and enforce and spread it among camp residents. This subset of residents has raised ISIS flags, indoctrinated children, and perpetrated violence to coerce others to adhere to ISIS ideology.

UNCLASSIFIED

UNCLASSIFIED

7. QFR: According to recent reporting, an August 17, 2020, DHS and National Counterterrorism Center intelligence product warned of possible election-related attacks both before and after the election. The report went on to voice grave concern about the threat from lone offender white supremacist extremists. How does NCTC view the threat from right-wing, including white supremacist, extremists surrounding the election?

NCTC RESPONSE: We are monitoring developing threats by violent extremists related to the 2020 election and aftermath. We defer to the FBI to discuss details of ongoing investigations.

8. QFR: We know that foreign actors, mainly from Russia but others as well, took advantage of our open society by sowing dissent and misinformation via social media platforms like Facebook in the lead up to the 2016 election. To what extent and with what level of success have nations like Russia and others engaged in disinformation campaigns that target domestic extremist movements vulnerable to exploitation?

NCTC RESPONSE: Russian influence campaigns probably include topics that would resonate with domestic violent extremists—particularly RMVEs and militia violent extremists—including COVID-19 restrictions, gun legislation, and racial justice issues.

9. QFR: Law enforcement targeted various members of the accelerationist, neo-Nazi group, The Base, earlier this year. Reporting has suggested that the group's leader, Rinaldo Nazario, is living in Russia. Is there any indication of whether or not his actions and leadership of this violent white supremacist group are approved of, supported by, or otherwise given safe haven by the Russian government?

NCTC RESPONSE: NCTC defers to FBI.

10. QFR: In the course of their investigations, what similarities do your agents or analysts find between international violent white supremacists and Salafist-jihadi extremists like those in Al Qaeda or ISIS?

NCTC RESPONSE: While Western Sunni extremists and RMVEs are inspired by disparate ideologies, propaganda, and grievances, we see some commonalities in their social media use and radicalization pathways.

Sunni extremists and RMVEs typically are influenced by an array of violent extremist material online and use online platforms to share propaganda and connect with like-minded sympathizers at home and abroad. Both sets of violent extremist actors utilize mainstream social media platforms to radicalize to violence and recruit new members. Some also take advantage of interest-specific websites and microblogging and gaming platforms to connect with other violent extremists. In recent years, HVEs and RMVEs have increasingly turned to

UNCLASSIFIED

UNCLASSIFIED

encrypted mobile messaging applications, such as Telegram, to conceal their communications.

Both Sunni extremists and RMVEs also generate and share online vivid, graphic imagery—including videos of executions and live-streamed attacks—to engage and recruit sympathizers. Both groupings also regularly seek to exploit major events or trends through their respective online messaging, including the COVID-19 pandemic, social unrest in the U.S., or migration to Europe to advance their agendas.

While every violent extremist's radicalization pathway is unique, the radicalization process and drivers for Sunni extremists and RMVEs typically are dependent on a combination of personal, group, community, sociopolitical, and ideological factors. In particular, common factors across ideologies include a desire for a sense of identity and a search for a greater cause to fight for; to appeal to such individuals, radicalizers link their calls for violence to the broader defense of their respective global communities. Individuals may also be influenced by destabilizing factors that can make them more susceptible to violent extremist narratives such as a personal crisis or lack of meaningful relationships.

The vast majority of both Western Sunni extremists and RMVEs mobilize without individual connections to or direction from violent extremist organizations. Identifying potential Sunni extremists and RMVE attackers who avoid sharing plans with other violent extremists and engage in operational security practices is a persistent law enforcement challenge.

11a. QFR: Women “immigrants” to the Islamic State have been fleeing the Caliphate by the hundreds, eventually returning to their native countries. Some appear to have embraced the group’s ideology and remain committed to its goals.

How is the U.S. addressing what may be a growing threat of attempted radicalization of women by ISIS and other terrorist organizations?

NCTC RESPONSE: NCTC defers to the State Department, U.S. Agency for International Development (USAID), and Department of Homeland Security (DHS).

11b. QFR: Are there any programs or strategies targeting this specific concern?

NCTC RESPONSE: NCTC defers to the State Department, USAID, and DHS.

12a. QFR: In February 2020, the U.N. Secretary-General reported that “foreign terrorist fighters and adherents of ISIS will continue to pose short-, medium- and long-term terrorist threats on a scale many times greater than was the case with [AQ] from 2002 onwards, based on the

UNCLASSIFIED

UNCLASSIFIED

much greater numbers involved." Moreover, U.N. member states report that "as many as 1,000 foreign terrorist fighters imprisoned on return to Europe prior to 2015 are expected to be released in Europe in 2020," and many are assessed "as still dangerous." How are FBI and NCTC coordinating with our partners overseas to prepare for the threat posed by those that are still assessed to be dangerous?

NCTC RESPONSE: NCTC shares information and best practices with foreign partners to identify the foreign fighters who pose the highest priority threats, including some of those who soon will be released from prisons in Europe.

We worked with our interagency partners to develop a method for reviewing returned foreign fighters to identify individuals who are more likely to pose a threat based on various individual and environmental factors. We shared a more detailed description of the process with many European countries, which may inform their resource allocation decisions for monitoring these individuals.

Established information sharing agreements with our European partners regarding terrorism related data enables the watch listing of individuals convicted on terrorism charges, which prohibits their travel to the U.S., including after their custodial sentences have been served.

12b. QFR: What does the future look like for the release of convicted Islamic State supporters in the U.S. and are we equipped to deal with individuals that are assessed to still be dangerous here at home?

NCTC RESPONSE: As of August 2020, 157 individuals in the U.S. have pled or been found guilty of offenses related to the Islamic State since the establishment of ISIS's self-proclaimed caliphate in 2014. The average age of those individuals was 28 with an average sentencing length of 13.2 years; many of these are scheduled to be released by 2022. Multiple federal government partners work collaboratively during the custodial and post-release monitoring phases of an inmate's sentence to assess the remaining threat and develop management strategies.

12c. QFR: How are your agencies coordinating with the Bureau of Prisons and other federal, state, local, tribal, and territorial partners on this matter?

NCTC RESPONSE: NCTC convenes a quarterly Extremist Recidivism Community of Interest, which brings together key stakeholders from the corrections, probation, intelligence, policy, and research spaces to increase their connectivity and share lessons learned and threat information. NCTC works closely with our Bureau of Prisons partners who serve on the National Joint Terrorism Task Force in order to exchange intelligence on federal inmates who have a history of or nexus to international terrorism while they are in custody. NCTC, in coordination with FBI and DHS, has delivered multiple in-person and virtual trainings to federal probation officers about the homegrown violent extremists (HVE) and domestic

UNCLASSIFIED

UNCLASSIFIED

terrorism threat. NCTC also provides finished intelligence products to our federal, state, and local correctional partners as part of our Joint Counterterrorism Assessment Team, and organizes briefings and outreach through our Domestic Representatives program. Bureau of Prisons and Probation frequently attend NCTC's Terrorism Prevention Practitioner Conference—where practitioners from around the country come together once a year to collaborate and network on a variety of issues concerning terrorism and prevention—and have presented in the past.

- 12d. QFR: Furthermore, what new or emerging trends have you observed in homegrown violent extremists (HVEs) seeking to travel overseas and how have your respective agencies adapted?

NCTC RESPONSE: Despite the ongoing heightened CT pressure against terrorist groups overseas, during the past couple of years the IC has continued to observe HVEs persistently aspiring to travel abroad to join terrorist groups such as ISIS and Al-Qa'ida. Even throughout the COVID-19 pandemic and the associated travel restrictions established to reduce the spread of the virus, the IC has observed some HVEs continuing to desire to travel abroad and attempting to adapt their travel plans to these new restrictions.

- 13a. QFR: What controls are in place at FBI and NCTC to ensure objective and timely releases of intelligence assessments of threats to the homeland?

NCTC RESPONSE: NCTC and FBI work closely together to regularly review reporting and determine the nature and status of terrorism threats to the Homeland. We carefully coordinate on each other's analyses and work together to produce intelligence assessments warning of Homeland threats. All products go through an extensive coordination and review process across the IC to ensure assessments are supported and objectivity is maintained.

- 13b. QFR: What, if any, challenges do FBI and NCTC face in producing these assessments and what specific actions are planned to mitigate such challenges?

NCTC RESPONSE: Classification restrictions on some reporting can be a challenge in reaching all audiences, but we have a number of options for product lines that can handle all classifications. This enables assessments to be published in a timely manner, and we can follow up with downgraded products to reach a broader audience if necessary.

- 13c. QFR: Has anyone in the Executive Office of the President or the Office of the Director of National Intelligence requested that you edit, block, or change a piece of intelligence or limit the production of intelligence on particular topics?

NCTC RESPONSE: While some exchanges with NCTC's customer are necessary to ensure the delivery of timely, objective, accurate, and relevant intelligence that meets customer needs, we have not received any inappropriate requests from the Executive Office of the President

UNCLASSIFIED

UNCLASSIFIED

or the ODNI to edit, block, or change any piece of intelligence or to limit production on any topics. All NCTC production is published in accordance with the IC Analytic Standards, which require that intelligence not be distorted by, nor shaped for, advocacy of a particular audience, agenda, or policy viewpoint.

UNCLASSIFIED

**Post-Hearing Questions for the Record
Submitted to Mr. Kenneth Cuccinelli
From Senator Gary C. Peters**

“Threats to the Homeland”

September 24, 2020

*****Due to the change-over in Administration, responses were not received
to these questions for the record.*****

1. In March, you provided testimony before HSGAC on the various actions that DHS was taking to prevent the spread of COVID-19 in the U.S. It is now clear that those actions were not enough, and the U.S. death toll now exceeds 200,000. The U.S. failed to contain the virus, experienced shortages of critical testing supplies for months, and ineffectively distributed needed PPE to states. What specific changes has the Department made or recommended that will mitigate the impact of the next wave or another pandemic?
2. In March, you endorsed Ranking Member Peters’ idea for a centralized website with reliable Coronavirus information. Despite the establishment of that website, mis- and disinformation continues to undermine response efforts – including through conflicting statements from senior administration officials. Do you believe Americans are most likely to follow public health recommendations if the federal government speaks with one voice?
 - a. If a family hears one thing from the Centers for Disease Control and Prevention, and something else entirely from the President, who should they listen to?
3. The Administration continues to suggest that shortages of personal protective equipment (PPE) are a thing of the past. However, the American Nurses Association and the American Hospital Association continue to report shortages, leaving our nation’s frontline workers to reuse masks for days. Why do DHS and the Administration assert there are no shortages when nurses are telling us that there are? How is DHS addressing them?
 - a. Why do PPE shortages persist, nearly seven months into this national emergency?
4. Why has DHS not utilized the authorities from the Defense Production Act (DPA) to incentivize more companies to produce N95s?
 - a. What should we do next if DPA usage is not filling the nation’s persistent gaps?
5. What modeling has DHS completed to project PPE demand over the next six months?
 - a. What information do you have about supply over the same window?
 - b. How many cases of influenza do you project?

- c. Can you provide the Committee with this information?
6. Due to the continued threat of COVID-19, many schools across the country are utilizing distance-learning. This creates a new cybersecurity challenge for schools, which maintain a significant amount of sensitive data for students and staff. Has CISA evaluated this threat?
 - a. What has CISA done to help protect students who are primarily attending school online this fall?
 - b. Do you support Ranking Member Peters' legislation, the *K-12 Cybersecurity Act*, which would help us better understand the unique risks schools face and provide recommendations and an online toolkit for schools to use when implementing their own solutions?
7. Increasingly severe storms and natural disasters, flooding, high water levels and other impacts of climate change present a constant threat to communities across the country. DHS faces these threats not only as the department tasked with emergency management, but also ensuring the operational capability of components also experiencing these adverse impacts. How does DHS mitigate these threats to ensure the safety of the DHS workforce, while also fulfilling their operational missions?
8. Data from the U.S. Army Corps of Engineers notes that the Great Lakes are experiencing record-high water levels, resulting in shoreline erosion and damage to public and private property. How have water levels impacted operations for DHS components like the U.S. Coast Guard and CBP in the Great Lakes?
9. DHS should provide clear information about the criteria for continued border restrictions. Border communities and individuals, including many Michiganders, have been separated from family and property due to restrictions. What criteria or benchmarks is the Department using in formulating border crossing restrictions?
 - a. What is the current status of development and promulgation of publicly shared materials on border restriction criteria?
10. Land ports of entry in Michigan and across our borders have experienced significant changes in traffic due to COVID-19 related border restrictions. Despite reductions, reports indicate that drug seizures have been up, with CBP's Detroit Field Office seizing 12 pounds of fentanyl between March 21 and May 16. The Buffalo Field Office also reported a record year in drug seizures for Fiscal Year 2020, to date. What do you attribute these increases to?
 - a. How has COVID-19 affected detection efforts?
11. Port and cargo security are critical to addressing security threats in commerce. HSGAC is aware that CBP has recently conducted a review of its cargo processing policies at sea ports of entry, including in Michigan. Can you provide the committee with an update on the results of this review?

12. *On Behalf of Sen. Menendez*: On June 9, 2020, Malachy McAllister, a law-abiding, tax-paying resident of the United States for over two decades, was deported by the Department of Homeland Security. Mr. McAllister fled Belfast in 1988 after narrowly escaping an assassination attempt by pro-British Loyalist paramilitaries, who fired 26 shots into his house while his mother-in-law and children were at home. This attack compelled him to seek safety in the United States where he applied for political asylum. Unfortunately Mr. McAllister's application for asylum was denied. President Trump's sister, Judge Maryanne Trump Barry, expressed in her opinion that current law did not anticipate the circumstances of the McAllister family and urged discretion in his case.

In recognition of the danger Mr. McAllister would face at home, no criminal record in the U.S., U.S. citizen family members and his positive contributions to U.S. society, he had been granted deferred action from deportation for years. Congressional leaders wrote to Acting DHS Secretary Chad Wolf on June 3, 2020 and June 7, 2020, requesting the exercise of discretion and to stop Mr. McAllister's deportation until his case received legislative consideration. In fact, Acting DHS Secretary Chad Wolf was informed, before Mr. McAllister was deported, that he had recently broken his collar bone and travel was against medical advice. Despite this information, DHS chartered an Air Ambulance and crew to deport Mr. McAllister.

Why did Acting DHS Secretary Chad Wolf and DHS leadership fail to exercise prosecutorial discretion and waste considerable taxpayer dollars to unnecessarily expedite the removal of Malachy McAllister? Who specifically signed off on Mr. McAllister's deportation from DHS leadership? How much did chartering an Air Ambulance cost taxpayers? Please provide the number of times and detail the occasions in which DHS has chartered an Air Ambulance to deport an individual who has received strong bipartisan congressional support for deferred action.

*****Due to the change-over in Administration, responses were not received to these questions for the record.*****

**Post-Hearing Questions for the Record
Submitted to Mr. Kenneth Cuccinelli
From Senator Maggie Hassan**

“Threats to the Homeland”

September 24, 2020

Question#:	1
Topic:	Binsar Siahaan
Hearing:	Threats to the Homeland
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

Question: As reported by the Washington Post, on the early morning of September 10th, six ICE agents entered the grounds of Glenmont United Methodist Church in Silver Spring, Maryland, and in violation of ICE's own sensitive locations policy, lured Binsar Siahaan out of his home there on false pretenses and then arrested him in front of his wife. Siahaan has since been moved 800 miles to the Stewart Detention Facility in Georgia. ICE's sensitive locations policy ensures enforcement actions are not undertaken on locations such as churches or schools unless (1) exigent circumstances exist, (2) other law enforcement activities led officers to the location, or (3) prior approval to the arrest was granted. Please explain which of these exceptions was applied to Siahaan's case, an Indonesian immigrant who has lived in the United States for three decades and works and lives at the church with his family and who had been released in February from ICE custody while his legal appeals were pending. If prior approval was granted, please provide the name of the official who granted that approval and the justification for that approval. Please also provide a list of incidents where exceptions to the sensitive locations policy were made during your tenure at DHS and whether the Department intends to continue the sensitive locations policy going forward.

Response: U.S. Immigration and Customs Enforcement (ICE) officers arrested Binsar Rionald Siahaan, an unlawfully present Indonesian national, at his residence in Silver Spring, Maryland on September 10, 2020. An immigration judge ordered Mr. Siahaan's removal in 2005, which has been upheld through multiple appeals. Mr. Siahaan filed an emergency stay of removal after his most recent arrest, which is currently pending, and he is currently detained at Stewart Detention Center in Georgia.

Please note that ICE is unable to disclose any further information specific to this case without signed, written consent from the alien in question.

Question#:	1
Topic:	Binsar Siahaan
Hearing:	Threats to the Homeland
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

Question#:	2
Topic:	Chinese Theft of Intellectual Property
Hearing:	Threats to the Homeland
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

Question: What is the Department of Homeland Security (DHS) going to do to prevent Chinese theft of intellectual property from U.S. companies both from an insider threat perspective and through cyber-attacks?

Response: The U.S. Department of Homeland Security (DHS) takes the threat of government-sponsored malicious cyber activity against the homeland, including intellectual property theft, very seriously. DHS recently established the DHS China Working Group, made up of senior representatives of all DHS components, with the goal of developing an action plan to protect and defend the nation against threats from People's Republic of China (PRC)-sponsored online activities. The Working Group is overseen by the Senior Official Performing the Duties of Under Secretary for Strategy, Policy, and Plans (PLCY) and has already compiled a preliminary round of actions. These actions are currently undergoing internal review.

The Working Group is sub-divided into five workstreams, which are operated at the staff level and managed by Component representatives. The Cybersecurity and Infrastructure Security Agency (CISA), manages the cybersecurity and critical infrastructure workstream. Participation includes staff from ICE, U.S. Secret Service, the DHS Science and Technology Directorate, and the DHS Office of Intelligence and Analysis, in addition to a number of CISA divisions. This workstream leads the development of action items related to the prevention of intellectual property theft. To date, generated actions have included increasing public and private sector engagement through awareness, training, and exercises; facilitation of the protection of cloud service providers, which have been used as a vector for PRC government-sponsored offensive attacks; augmenting support for the US academic sector, which is a key target based on the significant intellectual property data managed; studying the effect of emerging technologies, including Unmanned Aerial Systems manufactured in China, on the vulnerability of intellectual property and developing deterrence strategies; and developing a strategy to protect and defend U.S. intellectual property from Chinese government-sponsored cyber espionage and data theft.

In addition, the National Intellectual Property Rights Coordination Center, within the Immigration and Customs Enforcement's Global Trade Investigations Division, continues to combat intellectual property theft through investigations, interdictions, and outreach and training for domestic and international law enforcement organizations.

Question#:	3
Topic:	Insecure Technology
Hearing:	Threats to the Homeland
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

Question: How is the U.S. dealing with insecure technology being introduced into our critical infrastructures, such as the nationwide expansion of 5G networks and recently uncovered security flaws in Supermicro servers?

Response: CISA is working, in partnership with other agencies such as the Department of Commerce's National Telecommunications and Information Administration, to implement the National Strategy to Secure 5G. As part of its analytic and partnership efforts to strengthen the resilience of the critical infrastructure community, CISA is actively maturing its capability to more holistically understand the criticality of connected systems and the underpinning technology, hardware, software, and services. Not surprisingly, 5G (and broader ICT supply chain) security considerations have been front and center as part of this activity.

As part of the wider effort of Federal agencies investing in 5G security efforts, CISA is helping to coordinate and shape the deployment of secure and resilient 5G technologies and networks across the Nation.¹ Through its core capabilities of stakeholder engagement, risk management, and technical assistance, CISA's 5G Strategy establishes five strategic initiatives for DHS:

- Strategic Initiative 1: Support 5G policy and standards development by emphasizing security and resilience: Developing 5G policy, best practices, and standards that emphasize security and resilience to prevent attempts by threat actors to influence the design and architecture of 5G networks;
- Strategic Initiative 2: Expand situational awareness of 5G supply chain risks and promote security measures: Educating stakeholders on 5G supply chain risk, particularly around vendors, equipment, and networks to promote leading security practices within the public and private sector;
- Strategic Initiative 3: Partner with stakeholders to strengthen and secure existing infrastructure to support future 5G deployments: Strengthening and securing existing infrastructure to support future 5G deployments by recommending improvements for existing 4G Long-Term Evolution (LTE) infrastructure and core networks;
- Strategic Initiative 4: Encourage innovation in the 5G marketplace to foster trusted 5G vendors: Catalyzing innovation in the 5G marketplace to foster trusted 5G vendors; and
- Strategic Initiative 5: Analyze potential 5G use cases and share information on risk management strategies: Assessing risk mitigation techniques on 5G use cases in order to share and popularize strategies that continue to secure the NCFs.

¹ CISA is working within the US Government Interagency process as other Departments and Agencies are engaged in similar and sometimes overlapping efforts in 5G.

Question#:	3
Topic:	Insecure Technology
Hearing:	Threats to the Homeland
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

These initiatives include associated objectives to ensure there are policy, legal, security, and safety frameworks in place to fully leverage 5G technology while managing its significant risks. In line with these initiatives, CISA is developing written analytical products that enable risk mitigation efforts within the federal government, critical infrastructure, and state, local, tribal, and territorial government. The federal government and our partners benefit from all the advantages that emerging technologies promise to bring, all while mitigating their significant risks. CISA works with government and industry partners to ensure there are policy, legal, security, and safety frameworks in place to secure the development and deployment of 5G technologies while also managing risks. We also promote security best practices and standards and communicating risks – to include supply chain risks – to 5G infrastructure stakeholders.

CISA also works with partners across the Federal interagency, private sector industry partners, and internationally to help shape adoption of emerging technologies for the purposes of reducing national security risk and increasing resilience. One such public-private partnership is the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force. The ICT SCRM Task Force is the United States' main public-private partnership body devoted to identifying and managing risks to the ICT supply chain. The task force is made up of members from the U.S. government and the private sector owners and operators of the Communications and Information Technology critical infrastructure sectors. The ICT SCRM Task Force's purpose is to develop operational and strategic recommendations that will help all organizations build supply chain risk resilience, such as developing and releasing a threat scenarios report or lessons learned during the COVID-19 pandemic. The task force collaborates and shares these strategic and operational recommendations with other federal organizations and bodies like the Federal Acquisition Security Council, as the council has a vested interest in these recommendations.

Congress created the Federal Acquisition Security Council (FASC) under the SECURE Technology Act of 2018 to develop criteria to assist departments and agencies in determining risks to the ICT supply chain; disseminate supply chain risk information; and decide what actions to take to mitigate the supply chain risk. The FASC released the Interim Final Rule in September 2020 documenting its operations and describing how the FASC will facilitate risk information sharing with federal and non-federal entities. DHS is a member of the FASC and has been identified as the FASC's Information Sharing Agency under 41 CFR § 201.201.

Internal to the Department, the Deputy Under Secretary for Management directed the Office of the Chief Information Officer to lead an internal team of stakeholders. This team will discuss pending items and issues within the FASC in anticipation of the Department performing its statutory duty of issuing exclusion and removal orders to protect the supply chain of the civilian side of the Federal government.

Question#:	3
Topic:	Insecure Technology
Hearing:	Threats to the Homeland
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

Additionally, CISA provides a yearly response to Executive Order (EO) 13873: Securing the Information and Communications Technology and Services Supply Chain. This EO addresses the threat posed by the unrestricted acquisition or use of ICT and services “designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries,” and declares a national emergency with respect to this threat.

The EO requires the Secretary of DHS to produce a written assessment within 80 days and annually thereafter that “assess[es] and identify[es] entities, hardware, software, and services that present vulnerabilities in the United States and that pose the greatest potential consequences to the national security of the United States.” The assessment “shall include an evaluation of hardware, software, or services relied upon by multiple information and communications technology or service providers, including the communications services relied upon by critical infrastructure entities identified pursuant to Section 9 of Executive Order 13636.”

Question#:	4
Topic:	Information Security
Hearing:	Threats to the Homeland
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

Question: DHS is responsible for the information security of the entire civilian federal government, including providing mandated security services to other agencies and handling incident responses. A September 2019 Inspector General report suggests that DHS does not have the cybersecurity talent it needs to reach related objectives. There are several technical systems and areas that lack the right technical expertise at DHS. What is your strategy for developing good tech talent and securing the nation's cyberspace?

Response: CISA, the agency charged with supporting the security of the Federal civilian executive branch agencies' networks, is focused on the cybersecurity workforce gap within the civilian federal government. CISA recognizes the intricacies of the various recruitment and hiring phases, and that the operating environment and hiring process is not transactional, but cumulative. CISA leverages a multi-pronged approach to attract and develop tech talent to secure the nation's cyberspace. Currently CISA uses the following to attract, identify, recruit and hire qualified and quality cyber talent:

CISA uses a multi-faceted approach for job announcements to broaden the applicant pool and increase diversity of applicants. CISA uses two types of postings to announce and advertise its positions. The first type is an open and continuous announcement, which is a job opportunity announcement on www.usajobs.gov and is consistently open and attracting candidates for application. These positions are designed to attract information technology and cybersecurity professionals, typically at the GS-09 to GS-13 levels for the GS-2210 occupational series. Every 60 days, CISA refreshes and extends the open and continuous announcements. The second type of posting is a short-term individual job opportunity announcement that is aligned specifically with one or more position descriptions. Although our organization experiences many roles where direct hiring authority is eligible, we find that the use of announcements increases the diversity of the applicants and affirms the motivation of the candidate in joining CISA.

CISA uses student programs and internships to grow talent and the agency's pipeline. CISA has many paths for students and recent graduates to pursue an opportunity with CISA to help protect the homeland from cyber and physical threats. CISA's internships provide hands-on opportunities to challenge and build technical skills of the workforce of the future, and in Fiscal Year (FY) 2020 onboarded more than 58 individuals through these programs- the largest class to-date – with plans to continue to build upon this success in FY 2021.

CISA uses a recruitment event schedule to drive talent into our vacancies, yielding consistent new hires each month. In FY 2020, CISA moved away from in-person events to virtual hiring events, yielding much success. Past recruitment events yielded between 15 to 35 Tentative Job Offers (TJOs) extended, and that success has created a schedule for FY 2021 that includes using

Question#:	4
Topic:	Information Security
Hearing:	Threats to the Homeland
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

vendors like ClearanceJobs and DICE to execute over a dozen events for 2021. Each event will have a focus for recruiting, such as “Women in STEM” or a specific work role of critical need, with the intention of offering TJOs to candidates shortly after the event.

CISA is aggressively marketing its value as an employer in the cybersecurity and Federal space using various employment marketing and branding techniques.

A combination of public affairs and event managers, as well as recruitment communication specialists, work to market CISA hiring events and opportunities across its five social media platforms, and through its event vendor networks. In FY 2020, CISA established a web presence and maintains a steady stream of relevant content on its career’s webpage and social pages, driving continued traffic to its event and job announcements. The FY 2021 recruitment program is listed on the CISA careers website, and metrics indicate continued inbound messaging increases the number of registrants CISA has had for its events over the past the year.

In addition to the initiatives above to enhance federal cybersecurity recruitment and hiring, CISA must continuously identify, attract, and cultivate candidates from diverse backgrounds who are positively predisposed to CISA and its mission. While not a direct objective of recruitment, CISA recognizes these programs and initiatives represent opportunities to cultivate and strengthen relationships with non-traditional talent pools, while projecting a strong and identifiable agency brand within cyber communities. As such, CISA is working to foster non-traditional avenues that will both strengthen our current workforce and create and sustain a talent pipeline, as outlined below.

CISA will utilize the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) as the basis for all CISA-sponsored education and training programs. CISA and other federal partners are promoting and fostering an educational ecosystem to elevate and advance cybersecurity education. Government and industry need cybersecurity professionals that possess robust technical capabilities to meet the challenges of the future. The NICE Framework, now mandated throughout the Federal Government, is a big step toward identifying and ensuring that a cybersecurity professional has the necessary expertise throughout their career.

Additionally, CISA has education and training initiatives to help develop technical talent, including:

The President’s Cup Cybersecurity Competition - a federal competition that recognizes and rewards elite cybersecurity talent in the Federal Government. The President’s Cup Cybersecurity Competition is preparing to complete its second iteration in February of 2021 after a brief postponement due to COVID-19. CISA is pursuing both remote and in-person delivery options

Question#:	4
Topic:	Information Security
Hearing:	Threats to the Homeland
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

and will make an informed decision in January on the delivery method of the final round of competition. The team believes that the in-person event provides immense value beyond just the competition as an event to bring together the nation's best and brightest cyber professionals, but will defer to health guidelines of local, state, and federal governments on the efficacy of an in-person gathering at that time. In the FY 2021 Appropriations bill, CISA was granted the authority to use Operations and Support funding may be used to deliver awards (both monetary and non-monetary) to any Federal civilian employee or member of the uniformed services. This is a tremendous advancement for the competition to centralize the award structure and ensure uniformity across federal government for the achievement of winning the competition. The 2020 competition saw a marked improvement in registration and participation, indicating that the competition is reaching its audience. The feedback provided by the competitors has improved as well, indicating an overall improvement in the quality of the competition commensurate with the time allotted to design and run the President's Cup 2020. 2020 also saw larger Federal civilian representation, with two Department of Justice employees and a member of an independent government agency qualifying for the final round in February. In addition to providing the competition, the platform used to run the President's Cup has been released as open-source to allow any government department or agency to run their own competitions using the same technology as the President's Cup.

The Federal Reskilling Academy - Progress on the Federal Reskilling Academy continues. The team is currently working on securing contract support to deliver quality training for the Academy students. We anticipate a contract award towards the end of Q2 FY 2021 and will begin training cohorts early in Q3. CISA plans to begin three (3) cohorts of students in FY 2021. As these new CISA programs mature, we look forward to providing more details on our plan to execute our mission within our current budget, authorities, and scope.

Federal Cybersecurity Training Partnership with FEI - In FY 2020, CISA piloted a new course offering, targeted at non-cyber executives in Federal service. The course covered basic cybersecurity subject areas, as well as exercises such as how to handle a breach. The course received positive feedback from the first cohort of students, and CISA plans to expand the partnership with FEI in the future to deliver additional cohorts through the training, and is currently working with FEI to establish the number of courses that can be offered this fiscal year. As these new CISA programs mature, we look forward to providing more details on our plan to execute our mission within our current budget, authorities, and scope.

Question#:	5
Topic:	Federal Employee Viewpoint Survey
Hearing:	Threats to the Homeland
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

Question: According to the Best Places to Work in the Federal Government rankings compiled by the Partnership for Public Service and based on OPM's annual Federal Employee Viewpoint Survey, DHS ranks 17 out of 17 large federal agencies in overall employee engagement. What is your overall plan for improving federal employee engagement?

Response: In addressing the Department's progress on improving engagement and morale, it is important to understand the context in which our employees operate. As you know, DHS is an agency with diverse and demanding mission sets. The COVID-19 pandemic crisis is a good example of a unique challenge our workforce encountered in carrying out their duties. As the Federal Government moves forward with reintegration and return-to-work, it is important to remember that many DHS employees never stopped reporting to their job locations in order to ensure mission execution.

DHS is making progress. Our results on the Federal Employee Viewpoint Survey (FEVS) have improved steadily since 2015. Our Employee Engagement Index, for example, has increased by nine percentage points. The governmentwide score has increased only four percentage points in that same period. The Government Accountability Office and Office of Personnel Management have recognized DHS for this progress.

Improving employee morale and engagement is a sustained effort. A couple of years ago, DHS Headquarters brought a Chief Learning and Engagement Officer on board to support agency-wide and Component efforts. Headquarters has worked with its Component partners to continue to strengthen their action plans and ensure leadership accountability. DHS is in the process of creating written guidance and training that will further improve Component plans and enhance the Department's capacity to respond to employee needs. For example, the Department has instituted new initiatives including DHS Leadership Year, the DHS Leadership Survey, and Employee and Family Readiness. DHS will continue to adapt its employee engagement strategy based on data and feedback from its workforce and leadership.

Question#:	6
Topic:	Effective Leadership
Hearing:	Threats to the Homeland
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

Question: According to the same survey, DHS's "effective leadership" score has risen in each of the last four years, but is still just 49.3 out of 100, ranking last among all large agencies. What is your plan to improve DHS leadership at all levels - from the department's senior leaders down to its front-line supervisors?

Response: Since FY 2010, DHS has invested heavily in ensuring meaningful, results-based development for new and seasoned leaders at all levels (from Team Member through Executive). The purpose of this strategic initiative is to ensure that leaders at each level receive consistent development initially and annually, regardless of Component or discipline.

Through the collaborative efforts of all DHS Components, leaders are receiving the development they need to increase their ability to manage people and programs for results. Using a combination of classroom, online, virtual, and experiential learning, DHS has built an infrastructure to support application of development far beyond the training experience. DHS leaders have access to a robust and flexible slate of development that can be managed as part of their demanding workday, including a wide variety of required and optional development incorporating rotations, mentoring, shadowing, reading, and micro-learning. In fact, the DHS Leader Development Program was highlighted as a federal best practice in a recent IBM report on the Business of Government. DHS was recognized for its focus on preparing leaders now and into the future through succession-focused cohort programs and innovative virtual and peer-focused learning.

Components have implemented all required leader development in competencies that improve skills in leading people, creating an engaged culture, and workplace dynamics; and ongoing data collection highlights the increase over the years in both completions and impact. For example, despite the challenges that faced the men and women of this Department in FY 2020, 90 percent of Transportation Security Administration supervisory employees, 77 percent of U.S. Customs and Border Protection supervisory employees, and 73 percent of U.S. Citizenship and Immigration Services supervisory employees completed their requirements—all among the highest completion rates the Department has seen. When asked recently what single intervention has the most impact on their leader effectiveness, supervisory leaders overwhelmingly responded that development is the most valuable factor in supporting their effectiveness. These responses highlight that leadership skills development is more than an initiative at DHS – our workforce recognizes and embraces the critical role that development plays in helping them serve as successful leaders of an engaged and proficient workforce.

While FEVS is an important measure of federal workforce engagement, we know that lasting change takes time to sustain – and to notice. DHS leadership has taken a results-focused

Question#:	6
Topic:	Effective Leadership
Hearing:	Threats to the Homeland
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

approach at the Department with the understanding that improved leader performance will continue to bear fruit in employee morale and satisfaction. For instance, DHS released a study illustrating that organizations whose supervisors complete more of their required leader development requirements have higher FEVS scores, beginning two years later, than organizations whose supervisors complete fewer requirements. DHS has also definitively found that graduates of its Senior Executive Service Candidate Development Program and Capstone Executive Development Program are rated as higher performers by their supervisors than their non-graduate peers. These leaders are making change throughout the Department, and the increase in DHS FEVS scores is the beginning of what we believe will be lasting improvement.

However, the Department is also focused on ensuring that it does more than develop current leaders – it is changing the dynamic of how it cultivates a pipeline of leaders who are selected for leadership potential and developed in advance of their initial first-line supervisory position, rather than waiting until they start leading people. One of the Department’s newest elements is the Leadership Bridges strategy, which promotes the development of essential supervisor skills well before selection into supervisory positions – this will not only impact the next generation of DHS supervisory success, but introduce individuals into the overall leadership pipeline who will bring a greater capability and skill to each leadership level that they pursue.

DHS is also investing heavily in its senior executive development. For example, in FY 2021 DHS will be providing interested employees the opportunity to engage in micro-learning and multi-rater activities that will accommodate their schedules and deliver relevant, timely content on-demand. This approach of developing leadership skills from the top-down and from the bottom-up will help DHS supervisory leaders at all levels increase their leadership performance, and hopefully continue our forward progress.

The DHS Leader Development Program goes beyond extensive development in transformational leadership and supervisory acumen – it drives a culture and practice of people-oriented, mission-focused leadership excellence supported through integrated efforts across performance management, engagement, strategic planning and business operations in order to create both a context and a platform for success now and into the future.

**Post-Hearing Questions for the Record
Submitted to Mr. Kenneth Cuccinelli
From Senator Kyrsten Sinema**

“Threats to the Homeland”

September 24, 2020

*****Due to the change-over in Administration, responses were not received
to these questions for the record.*****

1. Using Title 42 authority, CBP is quickly expelling almost every person who crosses the border. I understand the need to adapt policies and procedures to protect the public health and also support strong border security. However, the sheer volume of overlapping restrictions and policies seems to have effectively closed our southern border to those who have a legal right to seek asylum. The lack of information DHS officials are providing to migrants regarding what legal rights they may have is concerning. DHS has stated previously that individuals are still screened for potential claims under the Convention Against Torture (CAT) and Customs and Border Protection (CBP). Commissioner Morgan previously testified in front of this committee that CBP is screening all unaccompanied children who arrive to the United States for relief under the Trafficking Victims Protection Reauthorization Act (TVPRA). However, there is a lot of evidence, including the situation regarding children being held in Phoenix hotels, which indicates these protections are not being applied consistently or fairly.
 - Does policy guidance provided by DHS to CBP and Border Patrol agents in the field address Title 42’s interaction with the Trafficking Victims Protection Reauthorization Act (TVPRA), Convention Against Torture (CAT), and other potential asylum claims made by migrants? If DHS feels that TVPRA and CAT protections do not apply under Title 42 authority, please indicate how your interpretation of federal law justifies that stance?
 - What specific policy guidance is provided for the handling of unaccompanied children under Title 42? How many unaccompanied children have been screened by CBP for TVPRA protections since March 2020?
 - Please provide my office with any and all policy and implementation documents issued by DHS that outline the use of Title 42 authority to expel migrants and how Title 42 procedures interact with traditional asylum claims, including claims under TVPRA or CAT.
 - Please provide copies of any agreements between the U.S. and Latin America and Caribbean countries regarding the return of unaccompanied children under the CDC order. In what ways, if any is DHS tracking information on the children you are expelling? Do these agreements provide any provisions for information sharing?
 - Of the unaccompanied children who have been expelled under Title 42 since March 2020, how many children are in each age category, less than 1 year, 1 to less than 2

- years, 2 to less than 3 years... etc to 17 but less than 18 years? Who keeps track of this data?
- How does DHS handle migrants that they are seeking to expel under Title 42 who Mexico will not accept, specifically Cuban nationals?
 - DHS has stated that it only conducts cursory health screening for migrants apprehended in the field before they are expelled. What health issues does DHS consider serious enough when observed during this cursory review to halt a Title 42 expulsion? Is pregnancy alone considered a health condition that would exclude someone from a Title 42 expulsion?
2. Travel restrictions on the southwest border were put in place in March and have been extended on a monthly basis through October 21st. These incremental extensions coupled with DHS' efforts to limit non-essential travel by U.S. citizens has caused uncertainty and confusion for border communities. During this pandemic, we must be smart and stay safe, but it is also important that local communities understand DHS plans and benchmarks for resumption of regular operations.
 - Is DHS developing a plan to return to normal operations at the border, and how is DHS communicating these plans and benchmarks to border communities and getting their feedback on how this prolonged shutdown has impacted them?
 3. The Cyberspace Solarium Commission report that was issued in March of 2020 recommended the creation of a National Cyber Director who would sit in the Executive Office of the President and oversee activities across the government for cybersecurity. Do you agree with this recommendation? Why or why not?
 4. The discussion during the hearing covered a number of critical threats, all of which are important. What other threats should Congress be examining that were not covered during the hearing or are flying under the radar?
 5. Currently, there are individuals in Mexico who fall under the Migrant Protection Protocols (MPP) and Remain in Mexico (RIM) program who have had their hearings suspended and there is no indication of when the hearings will resume. Some of these individuals who have approached a port of entry to seek asylum protection have been denied an opportunity to have a non-refoulement interview. When does CBP plan to resume providing non-refoulement interviews to those in MPP who express fear for their lives at the border? If DHS is considering reinstating non-refoulement interviews, what other initiatives is DHS considering to ensure Department compliance with the Convention Against Torture?

*****Due to the change-over in Administration, responses were not received to these questions for the record.*****

**Post-Hearing Questions for the Record
Submitted to Mr. Kenneth Cuccinelli
From Senator Jacky Rosen**

“Threats to the Homeland”

September 24, 2020

*****Due to the change-over in Administration, responses were not received
to these questions for the record.*****

1. In August, Senator Harris and I sent a letter to Acting CBP Commissioner Mark Morgan asking him to clarify his testimony at a June 25th CBP oversight hearing, in which he told the committee under oath, in response to one of my questions, that ALL unaccompanied children that CBP encounters at the U.S. southern border – and in fact ALL children subject to the agency’s new policies in implementing the CDC’s March 20th order – are screened for trafficking and other protection concerns. While Mr. Morgan has not responded to our letter, his claims are inconsistent with reports that CBP continues to deport unaccompanied children into potentially dangerous conditions WITHOUT properly screening them as required by anti-trafficking law.

In fact, as recently as *last month* during a press conference, Acting Commissioner Morgan said: “What we’re trying to do, the best we can, is remove all individuals, regardless of whether they’re minors or adults... We’re trying to remove them as fast as we can to not put them into our system, to not have them remain in the United States for a long period of time...”

The latest reports indicate that the number of unaccompanied children expelled since the implementation of the CDC order is at least 8,800, and we need to know how many of these children DHS sent back into harm’s way without proper screening.

- a. Of the more than 8,800 unaccompanied children who have been expelled since the March 20th CDC order, did DHS screen ALL children consistent with the Trafficking Victims Protection Reauthorization Act (TVPRA) and other protection concerns?
 - i. If not, why not?
 - ii. Can you briefly explain CBP’s screening process? Please provide documentation of the screenings that are taking place and the forms used for these screenings.
- b. Of the unaccompanied children whom CBP has expelled, how many were from Mexico and Canada? How many were from *non-contiguous* countries?

- c. Of the unaccompanied children who were expelled, how many were placed into immigration court proceedings before being expelled?
- d. How many unaccompanied children were transferred to the Office of Refugee Resettlement before being expelled?
- e. How many unaccompanied children who are not Mexican nationals have been expelled to Mexico?
- f. Is DHS tracking information on unaccompanied children the Department has expelled?
- g. Prior to the CDC order, did DHS officials or other government officials urge HHS or CDC officials to issue an order barring entry for unaccompanied children or asylum seekers?

Please provide copies of all correspondence from you and other DHS officials to HHS, CDC, and the White House relating to CDC order extensions and amendments.

- 2. Last month, we were all shocked when we learned about the whistleblower complaint alleging that personnel at ICE facilities performed hysterectomies on immigrant women without their consent. While I understand that the DHS Inspector General will be conducting an immediate and thorough investigation, it is clear that there needs to be additional oversight at facilities that with which ICE contracts.
 - a. Aside from DHS requesting an expedited investigation from the DHS OIG, what additional actions has DHS taken?
 - b. Does ICE still have a contract with the medical provider(s) involved in the complaint?
 - i. If so, has ICE taken *any* action against the facility or the medical provider contactors?
 - c. Are DHS officials aware of any other ICE facilities that are performing or have performed medical procedures without the consent of detainees?
 - i. If so, will those cases be part of this investigation?
 - d. How does ICE screen contracted medical providers? Is ICE currently reviewing its medical contracting procedures? If so, what plans does the agency plan to implement?
 - e. Will DHS commit to making the results of any investigation public?

3. On October 6, 2020, the Department shared with Congress the Homeland Threat Assessment 2020, which concludes that “racially and ethnically motivated violent extremists—specifically white supremacist extremists (WSEs)—will remain the most persistent and lethal threat in the Homeland.”

A whistleblower complaint from former head of intelligence and analysis at DHS Brian Murphy alleged that DHS leadership ordered him to downplay the threat from white supremacists to “ensure [the assessments] matched up with the public comments by President Trump.” Previous drafts of the Homeland Threat Assessment, which contained language on the white supremacist threat that was softened relative to earlier drafts, confirmed Mr. Murphy’s complaint.

- a. As we approach the 2020 election, does DHS take the position that politicizing threat intelligence undermines the core mission of the Department to keep Americans safe and secure?
 - b. Was the order to water down language describing the white supremacist threat done to benefit the political interests of the White House?
 - c. The Homeland Threat Assessment’s conclusion that white supremacists will pose the most lethal and persistent threat to the homeland is deeply troubling. Given this assessment, how does the Department plan to allocate resources to protect Americans from white supremacist extremists?
4. In the last fiscal year, the FBI has arrested over 100 domestic violent extremists. Statistics show that racially and ethnically motivated violent extremism were the primary source of all lethal domestic terrorism incidents in the last two years. From Pittsburgh to El Paso, in recent years we all have tragically witnessed the deadly effects of hate and bigotry. Yet last year, the Department of Homeland Security reportedly disbanded a group of intelligence analysts in the Office of Intelligence and Analysis who focused on domestic terrorism, leading to a decreasing number of analytic reports produced about this growing threat. At the same time, the Department’s office to prevent domestic terrorism has faced major cuts in personnel and funding.
 - a. Why is the Department of Homeland Security gutting its own tools to measure, prevent and combat racially and ethnically motivated violent extremism?
 5. Over the past few years, we have seen a dangerous increase in threats and attacks on all types of houses of worship, including the deadliest attack against the Jewish community in modern American history at the Tree of Life Synagogue in Pittsburgh.

The Nonprofit Security Grant Program makes FEMA grants to eligible nonprofit organizations for target hardening and other security enhancements to protect against terrorist attacks. In the Fiscal Year 2021 DHS budget, DHS failed to request a specific funding amount for the program.

- a. What DHS officials recommended that the Nonprofit Security Grant Program be funded at zero dollars?
 - b. How does DHS plan to keep houses of worship safe and secure without a specific allocation for the Nonprofit Security Grant Program?
 - c. With anti-Semitism and domestic terrorism on the rise here in the United States, and given the growing need for the Nonprofit Security Grant Program, as demonstrated by an increase in the number of grant applicants last year and lack of resources to fund these applications, how does DHS plan to fill that gap?
6. I'm particularly concerned about the Inspector General's capacity to investigate the disturbing whistleblower complaint regarding forced hysterectomies on ICE detainees, based on the low number of IG investigations completed and released in FY2020, the slowest pace of any year since 2003.
- a. Can DHS comment on the drastically reduced number of investigations the OIG has issued this year?
 - b. Can you understand how the slowdown of IG investigations, at a time when whistleblower reports at DHS are particularly shocking, creates the impression that under your leadership and that of Acting Secretary Wolf, DHS and this Administration are suppressing independent investigations that we need to get the truth?
 - c. Did you or other DHS officials influence or attempt to influence the Inspector General's decision not to investigate your serving as Acting Deputy Secretary after the GAO released its findings that you do not lawfully hold the office? Did you or other DHS or White House officials communicate with him at all about this decision?
7. Domestic terrorists are increasingly harnessing existing and emerging technologies to disseminate their propaganda, recruit new members, and evade law enforcement. Terrorists are using encryption to safeguard their communications, and social media is being exploited to spread hate and bigotry, and encourage violence. Social media is also enabling domestic terrorists to create transnational ties by coordinating with groups abroad.
- a. How is DHS working to keep pace with the rapid development of emerging technologies and their use by violent extremists, both at home and abroad?

*****Due to the change-over in Administration, responses were not received to these questions for the record.*****