

THREATS TO THE HOMELAND

HEARING

BEFORE THE

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

FIRST SESSION

NOVEMBER 5, 2019

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

42-868 PDF

WASHINGTON : 2021

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*

NICHOLAS RAMIREZ, *U.S. Coast Guard Detailee*

DAVID M. WEINBERG, *Minority Staff Director*

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

LAURA W. KILBRIDE, *Chief Clerk*

THOMAS J. SPINO, *Hearing Clerk*

CONTENTS

Opening statements:	Page
Senator Johnson	1
Senator Peters	2
Senator Hassan	14
Senator Harris	17
Senator Scott	20
Senator Carper	23
Senator Portman	26
Senator Lankford	28
Senator Romney	31
Senator Hawley	33
Senator Sinema	37
Prepared statements:	
Senator Johnson	47
Senator Peters	48

WITNESSES

TUESDAY, NOVEMBER 5, 2019

Hon. David J. Glawe, Under Secretary, Office of Intelligence and Analysis, U.S. Department of Homeland Security	4
Hon. Christopher A. Wray, Director, Federal Bureau of Investigation, U.S. Department of Justice	6
Russell Travers, Acting Director, National Counterterrorism Center, Office of the Director of National Intelligence	8

ALPHABETICAL LIST OF WITNESSES

Glawe, Hon. David J.:	
Testimony	4
Prepared statement	50
Travers, Russell:	
Testimony	8
Prepared statement	70
Wray, Hon. Christopher A.:	
Testimony	6
Prepared statement	63

APPENDIX

Senator Scott's letter to FBI	79
Get Back response to Senator Lankford	81
Get Back response to Senator Sinema	82
Get Back response to Senator Peters	83
Get Back response to Senator Hawley	85
Responses to post-hearing questions for the Record:	
Mr. Glawe	87
Mr. Wray	123
Mr. Travers	138

THREATS TO THE HOMELAND

TUESDAY, NOVEMBER 5, 2019

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

The Committee met, pursuant to notice, at 2:33 p.m., in room SH-216, Hart Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

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

OPENING STATEMENT OF CHAIRMAN JOHNSON

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

I want to, first and foremost, thank our witnesses for your service to our country. I want to thank you, obviously, for taking the time and for your testimony and the answers to our questions but, again, first and foremost, your service to our country. This was not planned this way, but this does mark the 10-year—I hate to even call it an “anniversary”—of the shooting at Fort Hood. Thirteen people lost their lives; 30 people were injured. But it kind of underscores what we are dealing with here in terms of a threat environment.

This is my ninth annual threat hearing that I have either chaired or participated in. I oftentimes say I am not the most uplifting character. I wish I could say that in those 9 years I have seen tremendous progress being made and we have reduced these threats and all is well.

Unfortunately, we face the same threats. If anything, the threats are growing. I do not think 9 years ago we were talking about the modern use of drones. We were not talking about encrypted and the use of social media to the extent it is being used right now. So, we face the same threats. They are evolving. Terrorist groups are metastasizing; they are spreading around the world. And if anything, what has happened is just trying to deal with and counter those threats has grown more complex and far more difficult.

You have tremendous responsibilities on your shoulders, and I truly do appreciate the fact that you are willing to bear those responsibilities.

I would ask that my written statement be entered into the record.¹

Rather than just kind of repeat what you are going to be talking about, rather than depress people further, I will turn it over to my Ranking Member, and then we will get into witness testimony.

OPENING STATEMENT OF SENATOR PETERS²

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

As we all know, the Department of Homeland Security (DHS) was created to defend the United States from any and all threats to the safety of our Nation. The Department and its leaders are critical to our national security efforts, and we rely on them to effectively coordinate with both the National Counterterrorism Center (NCTC) and the Federal Bureau of Investigation (FBI) to provide a unified effort to defend the homeland.

When DHS was first created in the aftermath of September 11, 2001 (9/11), the agency's mission was very clear: combat the scourge of international terrorism and ensure that we could say with confidence, "Never again."

But over time, the narrow focus has expanded, and as the threats to our homeland have grown, they have become more dynamic as well.

New terrorist groups devoted to striking America and our allies have emerged.

Foreign adversaries and cyber criminals seek to infiltrate and disrupt the Nation's cyber networks, posing an asymmetric threat that could cripple our economy with simply the click of a button.

Foreign interference in our domestic affairs has presented a complicated new challenge that we are still scrambling to adequately address.

A rise in domestic terrorism, specifically acts of violence carried out by white supremacist extremists, has targeted racial and religious minority communities all across our country.

Every year, we hold these hearings to examine these and other threats facing our country and to hear from the heads of the agencies responsible for keeping America safe.

The safety of Americans is built on partnership—partnership between our security agencies here today, partnership between agency leadership and their staff, and partnership between Congress and the Administration.

As we convene this hearing without a Secretary of Homeland Security, acting or otherwise, I am deeply concerned that these partnerships are starting to unravel. The absence of steady leadership at the Department of Homeland Security is a driving force for the institutional breakdowns that risk making us less safe.

The Department needs and the American people certainly deserve qualified, consistent, and stable leadership that will empower the brave men and women at DHS to protect the homeland, re-

¹ The prepared statement of Senator Johnson appears in the Appendix on page 47.

² The prepared statement of Senator Peters appear in the Appendix on page 48.

spond to natural disasters, and allow our Nation to grow and to prosper.

This Committee will continue to exercise thorough oversight of the Department's efforts to ensure that communities are protected from these threats, but that requires cooperation from your agencies and your compliance with constitutionally mandated requests.

I am extremely disappointed in your agencies' failures to provide a sufficient or, in the case of the FBI, any response to bipartisan requests from this Committee about the growing threat of domestic terrorism and white supremacist violence.

No one should live in fear of being attacked in their neighborhoods or in their houses of worship. This is a serious and growing threat, one we must address in order to save lives and to protect the very core of what makes us a free, a diverse, and a vibrant people.

I am grateful that your departments have taken the important step of presenting a framework for addressing this threat, but we cannot stop with a simple acknowledgment or a strategy put onto paper. This threat is not theoretical, and neither should our response be.

I insist that you comply with our outstanding requests—bipartisan requests, I may say—immediately as Congress works to combat the very real threat of domestic terrorism.

This Committee and your agencies must work together to review the policies and actions needed to keep Americans safe and ensure that they are successful.

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 these threats, and how this Committee and your agencies can continue working together to protect our national security.

Again, thank you for being here. I look forward to your testimony.

Chairman JOHNSON. It is the tradition of this Committee to swear in witnesses, so if you will all stand and raise your right hand. Do you 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. GLAWE. I do.

Mr. WRAY. I do.

Mr. TRAVERS. I do.

Chairman JOHNSON. Please be seated.

In light of Secretary Kevin McAleenan's announced retirement, representing the Department of Homeland Security is the Honorable David Glawe. Mr. Glawe is the Under Secretary for Intelligence and Analysis (I&A) at the Department of Homeland Security. Mr. Glawe was confirmed by the Senate on August 3, 2017. Prior to serving in this capacity, he served as Special Assistant to the President and Senior Director for Homeland Security. He has over 26 years of intelligence community (IC) and law enforcement experience, including serving in senior positions within the Office of the Director of National Intelligence (ODNI) and the Federal Bureau of Investigation. Mr. Glawe.

**TESTIMONY OF THE HONORABLE DAVID J. GLAWE,¹ UNDER
SECRETARY, OFFICE OF INTELLIGENCE AND ANALYSIS, U.S.
DEPARTMENT OF HOMELAND SECURITY**

Mr. GLAWE. Chairman Johnson, Ranking Member Peters, and distinguished members of the Committee, it is my honor and privilege to testify on behalf of the Department of Homeland Security to address today's emerging worldwide threats.

First, let me briefly touch upon my role. I currently serve as the Chief Intelligence Officer and Under Secretary at the Department of Homeland Security. I am responsible for ensuring the Secretary, our 22 DHS components, and our homeland security partners have access to the intelligence they need to keep the country safe. My focus is to ensure the unique tactical intelligence from the DHS intelligence enterprise is shared with operators and decisionmakers across all levels of government so they can more effectively mitigate threats to the homeland. My office generates intelligence that is unbiased and based on sound analytic judgments that meet the U.S. intelligence community standards.

I will speak today about the major shifts in the threat landscape. Specifically, I would like to speak about the threats we face from foreign terrorist organizations, domestic terrorism, cyber, foreign influence, and transnational organized crime (TOC).

Underpinning these threats is increasing adversarial engagement from nation-states such as China, Russia, Iran, and North Korea.

Domestic terrorism and targeted violence. I want to address one of the most pervasive threats we face in the homeland, which is the threat of targeted violence and mass attack, regardless if it is considered domestic terrorism or a hate crime. There is no moral ambiguity. These extremists are often motivated by violent ideologies or perceived grievances, often targeting race, ethnicity, national origin, religion, sexual orientation, gender, or gender identity. Lone attackers generally perpetrate these attacks and subscribe to an ideology that advocates hate and violence. They have adopted an increasingly transnational outlook in recent years, largely driven by technological advances through the use of social media and encrypted communication to connect with like-minded individuals online.

We are focused on identifying the behaviors and indicators of an individual at risk of carrying out targeted violence attacks so that we can appropriately identify and mitigate any violent act before it is carried out.

As a former police officer in rural Colorado and part of the 1999 Denver Metropolitan Police's areas response to the horrific attack at Columbine High School in Littleton, Colorado, I have firsthand experience, and it has shaped my approach to dealing with this type of violence.

At the Federal level, the Federal Bureau of Investigation and the Department of Justice (DOJ) lead the investigations and prosecuting of these crimes, while DHS informs, equips, and trains our homeland security partners to enhance their prevention and protection capability.

¹ The prepared statement of Mr. Glawe appears in the Appendix on page 50.

Foreign terrorist organizations remain a core priority of DHS' counterterrorism mission. We continue to make substantial progress in our ability to detect and mitigate the threats that these groups pose. However, foreign terrorist organizations remain intent on striking the country through directed attacks or by radicalizing the most vulnerable and disaffected Americans. These groups seek to inspire violence, encouraging individuals to strike at the heart of our Nation and attack the unity of our vibrant and diverse society. The Islamic State of Iraq and Syria (ISIS), al-Qaeda, and returning foreign fighters represent significant, persistent, and long-term national security threats.

Regarding cyber threats and emerging technologies, cyber threats remain a significant strategic risk for the United States, threatening our national security, economic prosperity, and safety. Nation-states' cyber criminals are increasing the frequency and sophistication of their attacks and malicious activity. China, Russia, Iran, and North Korea are developing and using advanced cyber capabilities and intend to target critical infrastructure, steal our national security and trade secrets, and threaten our democratic institutions.

The foreign intelligence threat has quickly evolved into one of the most significant threats our country has seen in decades. U.S. adversaries, including Russia, China, Iran, and North Korea, and other strategic competitors will use online influence operations to try to weaken democratic institutions, undermine U.S. alliances, threaten our economic security, and shape policy outcomes. We expect our adversaries and strategic competitors to refine their capabilities and add new tactics as they learn from their current experience, suggesting the threat landscape could look very different in the future.

Transnational organized crime. Transnational criminal organizations have a destabilizing effect on the Western Hemisphere by corrupting governments and government officials, eroding institutions, and perpetuating violence. They profit from a range of illicit activity, including human smuggling and trafficking, extortion and kidnapping, and narcotics trafficking. Their activity has led to record levels of crime and murder in Mexico, with a direct impact on the safety and security of our citizens.

I want to address the horrific events in Mexico from the last 24 hours. The reprehensible killings in northern Mexico of American citizens, including women, children, and infants, is a stark example of how these brutal organizations operate on a daily basis. The violence and disregard for human life displayed by these criminal organizations is as barbaric and gruesome as any terrorist organization we see around the globe. Transnational criminal organizations are motivated by money and power. They continually adjust their operations and supply chain to avoid detection and interdiction by law enforcement. Like legitimate businesses, they are quick to take advantage of improved technology, cheaper transportation, and better distribution methods. In many ways, cartels operate with the same sophistication of a foreign intelligence service.

In conclusion, I am very proud to oversee the Department's intelligence efforts to ensure the safety and security of all Americans. I want to thank you for the Committee's support of the Depart-

ment. It is a privilege to represent the men and women of the Department of Homeland Security, and I look forward to your questions this afternoon.

Thank you.

Chairman JOHNSON. Thank you, Mr. Secretary.

Our next witness is the Honorable Christopher Wray. Mr. 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 (AG) at the Department of Justice for Criminal Division. Director Wray.

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

Mr. WRAY. Thank you. Good afternoon, Chairman Johnson, Ranking Member Peters, Members of the Committee. I am honored to be here today representing the roughly 37,000 men and women of the FBI. It has been just over 2 years, as you noted, Mr. Chairman, since I became FBI Director, and I have now had the opportunity to visit all 56 of our field offices, many of them more than once, all across the country and met with State and local partners from every State represented by this Committee. I have also had the opportunity to meet with every headquarters division, scores of our foreign partners, business and community leaders, and crime victims and their families, and I think I have a much better sense now of what we are all up against.

Frankly, the threats that we face today are very different from over a decade ago. They are evolving in scale, in complexity, in impact, in agility, and the FBI is moving forward to meet those threats head-on.

Preventing terrorist attacks remains the FBI's top priority. Even as we recognize our country's important achievements with the death of al-Baghdadi and our fight against ISIS in the Middle East, we know that we have to stay vigilant against that threat, both overseas and here at home, and that includes people bent on joining terrorist organizations where they flourish abroad, folks like the two Milwaukee men sentenced earlier this year who were swearing allegiance to Baghdadi and trying to travel overseas to Syria to join the fight with ISIS.

We are also laser-focused on preventing terrorist attacks by people who are already here in the United States inspired by foreign terrorists, the people we refer to as the "homegrown violent extremists (HVE)." Often lone actors, these folks are inspired by foreign ideologies, but self-radicalize and operate through websites and encrypted messaging platforms rather than in some remote training camp or cave.

We are also keenly focused on threat of domestic terrorism, attacks carried out by a wide variety of violent extremist ideologies. That is everything from anarchist groups to racially motivated violent extremists.

To confront these threats, we are working closely with our Federal, State, and local law enforcement partners and reaching out to

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

all the communities we serve. And our efforts are paying off. We are being proactive, like in the case of the man our Miami Joint Terrorism Task Force (JTTF) arrested in August for threatening, among other things, to kill every Hispanic American in Miami; or the Las Vegas man our JTTF arrested the same month, who had been discussing a potential synagogue attack and had already purchased bomb-making materials; or the man we arrested just this past Friday who also planned to attack a synagogue, this one in Colorado, using pipe bombs and dynamite.

But these cases present unique challenges in part because in this country we do not investigate a person just because of his or her beliefs. And these people, like the homegrown violent extremists I was describing earlier, tend to work online and move quickly, at the speed of social media, leaving dangerously little warning time from espousing radical views to attack. I can tell you, after having personally walked through the crime scene at the Tree of Life synagogue and having personally visited with the teams at the scenes both in El Paso and in Dayton, that this threat is never far from our minds and is a focus all across the FBI.

Now, we do not have time to talk through, certainly in my opening but probably even in this hearing, all the top threats that we are dealing with, but I hope we can touch on more of them as I respond to your questions this afternoon. In particular, on the counterintelligence front, where the Chinese Government is now targeting our innovation through a wider than ever range of actors. Not just Chinese intelligence officers conducting both traditional and cyber espionage, but people they enlist to help them like contract hackers, certain graduate students and researchers, insider threats within U.S. businesses, and a whole variety of other actors working on behalf of China.

We see the Chinese Government encouraging and even assisting the abuse of incentive plans like the so-called Thousand Talents Program, plans that offer cash and other enticements to bring American information back to China, information that is often actually trade secrets and other innovations stolen from American companies and universities. We are seeing Chinese companies then using that stolen technology to compete against the very American companies it belongs to.

We are seeing intellectual property and data theft from companies and academic institutions of just about every size in just about every sector. This is a threat to our economic security and in many respects a threat to our national security. It is also a threat to American jobs, American businesses, American consumers, and it is in small towns and big cities alike.

Even as we speak, even as I sit here testifying before this Committee, the FBI has around 1,000 investigations involving attempted theft of U.S.-based technology that lead back to China, and that is involving nearly all of the FBI's 56 field offices. I can tell you that number is representing a significant uptick from a few years ago, and it is growing.

The men and women of the FBI dedicate themselves every day to keeping the American people safe. I want to thank this Committee for your support for our FBI workforce. I can tell you it makes all the difference in the world to our hardworking agents,

analysts, and professional staff all across this country and, frankly, around the world.

So thank you again for the opportunity to appear before you today.

Chairman JOHNSON. Thank you, Director Wray.

Our third witness is Russell Travers. Mr. Travers is the Acting Director of the National Counterterrorism Center. Acting Director Travers has been in this position since August 16, 2019, although he also served as the Acting Director from December 2017 to December 2018. His previous service includes Deputy Director of NCTC and Special Assistant to the President and Senior Director for Transnational Threat Integration and Information Sharing on the National Security Council (NSC). Mr. Travers.

TESTIMONY OF RUSSELL TRAVERS,¹ ACTING DIRECTOR, NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. TRAVERS. Thank you and good afternoon. Chairman Johnson, Ranking Member Peters, Members of the Committee, it is a privilege to be here to represent the men and women of the National Counterterrorism Center.

In the years since 9/11, the U.S. counterterrorism community and its many partners have achieved significant successes against terrorist groups around the world. As we saw just 2 weekends ago with the raid against Abu Bakr al-Baghdadi, the U.S. continues to remove terrorist leaders around the globe. And over the past year, coalition operations against ISIS in Iraq and Syria has deprived the group of its so-called caliphate.

Moreover, ongoing CT efforts across Africa, the Middle East, and South Asia continue to diminish the ranks of both al-Qaeda and ISIS, removing experienced leaders and operatives on a regular basis. And interagency efforts to enhance our defenses at home have resulted in continued progress in safeguarding the homeland from terrorist attacks.

There is indeed a lot of good news, but we need to be cautious because challenges remain. I will highlight and summarize just three.

First, military operations have indeed bought us time and space as we address a global terrorist threat. But the diverse, diffuse, and expanding nature of that threat remains a significant concern.

After 9/11, we were primarily focused on an externally directed attack capability emanating from a single piece of real estate along the Afghanistan-Pakistan border. Eighteen years later, as my colleagues have noted, we face a homegrown violent extremist threat, almost 20 ISIS branches and networks that range from tens to hundreds to thousands of people, al-Qaeda and its branches and affiliates, foreign fighters that flock to Iraq and Syria from well over 100 countries, Iran and its proxies, and there is a growing terrorist threat from racially and ethnically motivated extremists around the globe.

¹ The prepared statement of Mr. Travers appear in the Appendix on page 70.

By any calculation, there are far more radicalized individuals now than there were at 9/11, and this highlights the importance of terrorism prevention.

While some aspects of the threat can only be dealt with through kinetic operations, the resonance of the ideology will not be dealt with by military or law enforcement operations alone. The world has a lot of work to do in the nonkinetic realm to deal with radicalization underlying causes.

The second challenge stems from terrorists' ability to exploit technology and attributes of globalization. They are good at it, and they are very innovative, as the Chairman suggested. We have seen the use of encrypted communications for operational planning; the use of social media to spread propaganda and transfer knowledge between and amongst individuals and networks; the use of drones and unmanned aircraft systems (UASs) for swarm attacks, explosive delivery means, and even assassination attempts.

High-quality fraudulent travel documents will increasingly undermine a names-based screening and vetting system and threaten border security. We will see greater use of cryptocurrencies to fund operations, and the potential terrorist use of chemical and biological weapons has moved from a low-probability eventuality to something that is considered much more likely.

In many cases, terrorist exploitation of technology has outpaced the associated legal and policy framework needed to deal with the threat. Looking out 5 years, we are particularly concerned with the growing adverse impact encryption will have on our counterterrorism efforts.

The third challenge I would highlight relates to a concern about potential complacency. Our whole-of-government approach to counterterrorism over the past 18 years has kept the country pretty safe. In our view, the near-term potential for large-scale, externally directed attacks against the homeland has at least temporarily declined as a result of U.S. and allied actions around the globe. But as noted earlier, the threat itself does continue to metastasize and will require very close attention in the years ahead.

In a crowded national security environment, it is completely understandable that terrorism may no longer be viewed as the number one threat to the country, but that begs a host of questions.

First, what does the national risk equation look like as the country confronts a very complex national security environment?

Second, how do we optimize CT resources in the best interests of the country when departments and agencies may have somewhat differing priorities?

Third, if we are going to reduce efforts against terrorism, how do we do so in a manner that does not inadvertently reverse the gains of the past 18 years?

These are all complicated questions that will require significant conversation, sophisticated conversation going forward, in both the Executive and Legislative branches.

Thank you, Mr. Chairman. I look forward to your questions.

Chairman JOHNSON. Thank you, Mr. Travers.

I was not expecting an infusion of optimism here, and I did not get it. These are serious threats, and they are becoming more and more complex.

One thing I noticed was lacking in all of your written testimony as well as your oral testimony, except for Under Secretary Glawe did reference the murder of the Mormon family, we did not talk about the really incredible events surrounding the capture of El Chapo's son and how the drug cartels completely took over and overwhelmed the law enforcement there. And we did not talk about—and this is the thing that was really missing. We did not talk about MS-13 and some of those gangs that are infusing our inner cities and are incredibly brutal.

I guess I would just like to ask all three of you, either the reality, the potential for spillover of the drug cartel activities we saw with El Chapo's son, as we saw with the Mormon tragedy, but also just the gangs that we already know exist, and really the current situation. Is it growing? How much of a handle do we have on these gangs? I will start with you, Mr. Glawe.

Mr. GLAWE. Chairman Johnson, thank you for the opportunity to speak about this. I would say in regard to Mexico, there are areas in Mexico which I would characterize as "lawless"—"lawless" being that the drug cartels run the infrastructure, the services, and their businesses, which is drug trafficking.

Chairman JOHNSON. I have heard—and I do not want to name the figure, but I have heard a pretty high percentage of the number of communities are completely controlled by the drug cartels.

Mr. GLAWE. We have done an evaluation with other U.S. intelligence community partners, and I would be happy to come back in a closed session. I believe that is classified, and we can go through that. But we did do an evaluation similar to a counter-insurgency model that we have looked at in the war zones, and it is devastating right now. The drug interdiction numbers on the Southwest Border have increased statistically over the last 3 years, methamphetamine, fentanyl-based narcotics, opium-based narcotics, and cocaine. Their networks are sophisticated. They operate as a sophisticated business and enterprise with a supply chain, with covert and overt operatives. They are able to use extortion and assassinations at will. It is all based on money and moving people and goods to the Southwest Border and over the border into the United States. Those supply lanes and drug-trafficking routes are defined, and where they are not, there is war and fighting going on.

Chairman JOHNSON. We held a hearing, and MS-13 was not motivated by drugs. It was something else.

Director Wray, can you kind of speak to gangs in our inner cities?

Mr. WRAY. Certainly the FBI is spending a lot of our effort on gangs in the inner cities, not just MS-13, 18th Street, gangs like that that have a more national footprint, but also neighborhood gangs. If you talk to police chiefs around this country, you will find that in a lot of cities it is neighborhood gangs that are really terrorizing the communities. We view it as a threat that is unfortunately alive and well, and we are tackling it through a variety of different kinds of task forces, capacity building with State and locals.

Chairman JOHNSON. What has been the trend over the last 10 years?

Mr. WRAY. I think part of it is this trend toward the neighborhood gangs. MS-13 has continued to become a major factor, but we also, like I said, are increasingly worried about neighborhood gangs. We have found that when you in a coordinated way are strategic and prioritized in going after the threats, in a lot of communities what you will find is that if you prioritize, you will find that there, in effect, a tail wagging the dog, and it varies from city to city. But in one city it will be a particular neighborhood. In another city it might even be a six-block radius. In another place it might be a particular corridor or on a highway. In another place it might be a particular group, 20 or 30 people who are really driving the threat. But almost always, with good intelligence analysis, working together with our partners, you will find, again, that tail wagging the dog. If you are disciplined in going after it, you can have a dramatic impact, sometimes quite quickly, that lasts.

Chairman JOHNSON. But are the number of gang members growing? Are the actions becoming more brutal? I read about things that are just horrific.

Mr. WRAY. Certainly MS-13 takes brutality to a whole other level. Violence there, as you know, Mr. Chairman, is essentially part of the rite of passage to join and move up the ranks. So there is a degree to which there is really almost violence for violence's sake on the part of some of these gangs.

Chairman JOHNSON. But, again, are the numbers growing or is it flat? I am just trying to get a feel for the trend here.

Mr. WRAY. I am not sure I can give you the numbers of gang membership per se, but I would be happy to have someone follow up with and give you a more detailed briefing on that. I know the violent crime rate has gone down some in the last year or two; even though not dramatically, it has gone in the right direction.

Chairman JOHNSON. In your testimony, your oral testimony, Director Wray, you were talking about the cyber theft, which is, I have heard, hundreds of millions of dollars. Primarily the big culprit there is China. I cannot personally envision a trade deal reigning that in. I think we are going to have to use law enforcement, and I think we are going to have to use law enforcement from the standpoint of having global partners, for example, deny entry from management of these companies that we know are stealing our intellectual property.

Can you just kind of speak to that reality?

Mr. WRAY. I think you are exactly right, that there is no one remedy that is going to deal with a threat that is this broad, this deep, this diverse, this vexing. What I would say is that there is a role for trade, there is a role for law enforcement, there is a role for diplomacy, there is a role for, in particular, as I think you and I have discussed in the past, building resilience in this country by working with the private sector and the academic sector.

A lot of times, the most effective defense against the Chinese counterintelligence threat can be done by companies and universities, and other institutions in this country being smarter and more sophisticated about protecting themselves. So we are putting a lot of effort into that, being a little more forward-leaning than we might have been 5 or 6 years ago in terms of providing detailed in-

formation to try to help them, as I said, be part of the common defense that I think we all need.

Chairman JOHNSON. Canada arrested the Chief Financial Officer (CFO) of Huawei on charges related to violation of sanctions. Is there a concerted effort to try and, again, deny entry, potentially arrest people from these companies that are stealing our intellectual property? Is there an organized effort globally with other Western democracies to do that?

Mr. WRAY. We are doing things with other Western countries and, frankly, non-Western countries because this is a threat that is being confronted by a lot of our allies.

I will say that in some instances there are abuses of the visa process that we are trying to help address. That is obviously a State Department issue, but they are an important part of this fight as well.

In other cases, there may be people who are engaged in intellectual property theft in a way that violates the terms of their contract, either an employment contract in a company or a research contract with a university, and they can be essentially kicked out on that basis. Sometimes that is a lot better solution than traditional law enforcement.

Chairman JOHNSON. OK. Senator Peters.

Senator PETERS. Thank you, Mr. Chairman.

There is no question the three of you have very difficult jobs and big responsibilities. Mr. Glawe, I want to discuss one of those very difficult jobs that the Department of Homeland Security has, which is, of course, what all three of you do: first and foremost, keep us safe. That is the fundamental objective, is to make sure that Americans are safe. But you have an added responsibility, and that is to move trade and commerce as efficiently as possible across the borders, and those two are often at odds with each other. Certainly in Michigan, it is something that we look at a lot, given the fact that we have two of the three busiest land crossings, border crossings, in the country. And so the facilitation of secure trade and travel is absolutely essential to my State, as well as many others. In order to support that mission, it is crucial that the DHS has a clear picture of the threats facing the Northern Border and between the ports of entry (POE) as well.

So my question to you is: Could you briefly speak to I&A's work to assess the threats on the Northern Border to support the Department's Northern Border strategy as it exists today?

Mr. GLAWE. Sure. Ranking Member Peters, thank you for the question. I am a relatively unique witness for you; I was the head of intelligence for U.S. Customs and Border Protection (CBP) prior to assuming this role, and I occupied that position for almost 3 years. In that role with U.S. Customs and Border Protection, I led a team that did an assessment of the Northern Border threat, which I will be happy to share with the Committee. I have traveled to the Northern Border. I have been to Detroit. I have been to those land border crossings, and I have been to our intelligence center, which we stood up there.

There is a vulnerability in the marine environment and the land environment. It is a porous border, and the terrain is tough, as it is in the Southwest Border, but different. We are looking at how

we deploy our assets, which are primarily law enforcement, with the air and sensor capability to see individuals that may be crossing unlawfully. A lot of our relationship revolves around a partnership with the Canadians, the Canadian Border Service, and the Royal Canadian Mounted Police and their intelligence services, which are outstanding. We are very much relying on that partnership with each other, backed up by the good intelligence collection by our partners that goes on 24 hours a day.

I would like to highlight the National Vetting Center, which is our global capability to identify at-risk individuals, which is also being expanded to cargo, that pose a threat to the United States, and that is in full operational capacity now through our National Targeting Center at U.S. Customs and Border Protection.

But we are constantly evaluating the threat to the Northern Border by transnational criminal organizations (TCOs), terrorist organizations, and foreign intelligence officers.

Senator PETERS. Thank you.

Mr. Wray, I mentioned this briefly in my opening comments, but your agency has not provided a single document in almost 6 months now to a letter that Chairman Johnson and I authored dealing with domestic terrorism. This is a bipartisan letter. I think we were very careful in terms of the scope of it, that it is not overly broad but hopefully allowed us to have the kind of information necessary for us to provide the kind of oversight, particularly on something as serious as domestic terrorism and white supremacist action in particular, which you have highlighted as something that is growing.

To me—and I think I speak for my Chairman as well—that is unacceptable when you have a joint letter from a Ranking Member and the Chairman, bipartisan. My question to you is: Do you require a subpoena to respond to routine document requests from this Committee?

Mr. WRAY. No. Second, I would tell you, Ranking Member Peters, that we have tried very hard to be responsive to this Committee. I will say that I know that the Department, of which we are, of course, a part, provided a long written response. I know that we sat down with your staff, Committee staff, and provided a verbal briefing, which was very helpful on our end in understanding better the purpose and the scope and the intent of the request. I also know that we have been providing monthly domestic terrorism reports to the Committee staff, among others.

But having said that, the most important thing to me is to make sure that we are being responsive, and I will direct my staff to drill in and figure out how we can be more responsive and more forthcoming in response to your requests.

Senator PETERS. So you will be more responsive than not responding at all?

Mr. WRAY. As I said, Senator, I think we have been responsive.

Senator PETERS. You talked about the Committee response. We actually talked about this last week. What we got from DHS were basically publicly available documents. I will tell you our staffs are pretty good at looking at publicly available documents, so that is not real helpful in our oversight role. These were very specific questions that we would expect a response. We believe that we

should probably have as a Committee—and that is my question. Do you think the Committee should have less access to documents than just a general FOIA request? That is basically what we are seeing here.

Mr. WRAY. Senator, I cannot speak for DHS' response—

Senator PETERS. No. This is for the FBI.

Mr. WRAY. But from the FBI, as I said, I do not think providing verbal briefing, the written response from the Department, and the monthly reports is no response at all.

The point, though, from my perspective, is that I want to make sure we are addressing your concerns, so I do not want you to take any of my responses suggesting that I am not going to direct my staff to drill back down and make sure that we are doing everything we can to be cooperative.

Senator PETERS. I appreciate that. Could we get a commitment by the end of the week that we would have that?

Mr. WRAY. We will get some kind of response by the end of the week. I need to get more information about what is missing and what is still needed.

Senator PETERS. I appreciate that, and I hope you will have prompt attention to that.

According to the FBI, domestic terrorists killed 39 people in fiscal year (FY) 2019, making it the most deadly year for domestic terrorism since the 1995 Oklahoma City bombing. My question to you, Mr. Wray, is: How would you characterize the domestic terrorist threat posed by White supremacists?

Mr. WRAY. So first I would say that domestic terrorism generally, in particular, self-radicalized typically lone actors here, represents a serious, persistent threat. I think we had about 107 domestic terrorism arrests in fiscal year 2019, which is close to the same number that we had on the international terrorism front.

Within the domestic terrorism group, we have about—at any given time, the number fluctuates, but at any given time, we have about 1,000—sometimes it is closer to 900, sometimes it is above 1,000—domestic terrorism investigations. A huge chunk of those domestic terrorism investigations involve racially—motivated violent extremist-motivated terrorist attacks, and the majority of those, of the racially—motivated violent extremist attacks, are fueled by some kind of White supremacy. I would say that the most lethal activity over the last few years has been committed by those type of attackers.

Senator PETERS. I am out of time, but I will follow this in the second round. Thank you.

Chairman JOHNSON. Senator Hassan.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you very much, Mr. Chairman. Thanks to you and Ranking Member Peters for convening this hearing on threats to our homeland. Thank you to all three of our witnesses not only for being here today but for your service to our country, and I hope you will carry back with you to the men and women you lead our sincere thanks from a grateful country for all they do to keep us safe.

Director Travers, I wanted to start with a question to you. Last month, I traveled to Afghanistan and Pakistan and heard firsthand the concerns of our military and embassy personnel about the growing and very real threat of ISIS-K, the ISIS affiliate in Afghanistan. I heard clearly that ISIS-K threatens not only U.S. forces in Afghanistan, but also has designs on striking the U.S. homeland.

You said last week that there are more than 20 ISIS branches globally, some of which are using sophisticated technologies such as drones to conduct operations. Despite our key victories against ISIS in Syria and Iraq, ISIS as a global terrorist organization remains a deadly threat to the United States.

Director Travers, we know that ISIS-K and other affiliates of ISIS want to strike the U.S. homeland. Please tell us more about their ability to do this and what we are doing to mitigate this threat.

Mr. TRAVERS. Thanks for the question, Senator. Yes, so of all of the branches and networks of ISIS, ISIS-K is certainly one of those of most concern, probably in the neighborhood of 4,000 individuals or so. We certainly share the concerns of both the U.S. military and the embassy in theater. They have attempted to certainly inspire attacks outside of Afghanistan. They attempted last year to conduct a suicide attack in India. It failed. They have actually tried, a couple years ago, I think, to inspire an attack against New York that the FBI interrupted. There was an attack in Stockholm in 2017, I believe, that killed five people. So they certainly have a desire and the propaganda would indicate that they want to conduct attacks outside of Afghanistan, thus far relatively limited.

I would say that we saw attack claims by ISIS-K ramping up throughout 2016, 2017, and 2018, somewhat lower the beginning of this year, although now I think we are looking at about an attack a day or so. Interestingly, only about an hour and a half ago, they were the latest ISIS branch to declare allegiance to the new head of ISIS.

Senator HASSAN. Thank you for that.

Director Wray, I have a question for you about ransomware, but just before I do, I want to thank your team in New Hampshire. We recently had a field hearing about the threats to our houses of worship, in particular from domestic terrorism, and supervisory senior resident agent Michael Gibley was very helpful, and I think our faith leaders have been very encouraged by his work with them. So thank you and him for that.

As to ransomware, we are seeing the impact of it across the country, including an attack in my home State of New Hampshire. Threat actors target every aspect of our communities from health care providers to our small businesses and even to State and local governments themselves, as they did in New Hampshire.

Last week, I talked with Cybersecurity and Infrastructure Security Agency (CISA) Director Krebs about what the Department of Homeland Security is doing to assist State and local entities facing ransomware attacks. Director Wray, what is the FBI doing to address the threat of ransomware attacks on our communities? Is it tracking the number of ransomware attacks on our country? How

is the FBI coordinating with the Department of Homeland Security in these efforts?

Mr. WRAY. So, first off, Senator, I appreciate the feedback on the meeting up in New Hampshire. On ransomware specifically, I think what we are seeing is a shift to more and more targeted ransomware attacks, more and more targeting, for example, municipalities, and there are a variety of reasons why municipalities are particularly vulnerable victims to ransomware attacks.

We are also seeing more enterprise-level ransomware attacks where it essentially affects every computer in the organization.

Senator HASSAN. Right.

Mr. WRAY. One of the things that we are trying to do whatever we can is figure out through our unique role as both a law enforcement agency and an intelligence agency. There have been times where, for example, we are able to reverse-engineer a decryption key. So I can take, for example, we had a case in the Northwest, for example, a small business, 600 people, crippling ransomware attack, potentially all those people about to lose their jobs, the company to go under. But because of our investigative work, we were able to reverse-engineer a decryption key. They did not have to pay the ransom. They got their systems back online, and a lot of nice thank you notes from those 600 employees.

Senator HASSAN. I bet.

Mr. WRAY. As far as working with DHS, the basic lanes in the road, if you will, we work very closely together. The FBI is the lead on the threat, and DHS is the lead on the asset. And essentially we work together in that respect.

Senator HASSAN. It is something that I think in a lot of the work we have done as a Committee we are hearing more and more concern from our local stakeholders about it and also really want to help all of the various agencies coordinate and share information as effectively as possible.

Director Travers, I wanted to go back to the issue of domestic terrorism. In the aftermath of 9/11, the Federal Government built a robust and capable counterterrorism architecture, establishing new departments, centers, and counterterrorism information-sharing mechanisms to support State and local partners and address a foreign terrorist threat unlike any we had seen before.

Today, 18 years later, we face a surge in domestic terrorism—and you will hear it from everybody on this Committee; you have heard it already in some of the questions—including rising threats against houses of worship. If we are to prevent domestic terrorist attacks, we have to start treating these incidences as seriously as we did when al-Qaeda and other foreign terrorist organizations have threatened or attacked us after 9/11.

Director Travers, the National Counterterrorism Center was created after 9/11 to respond to threats from al-Qaeda. The center is responsible for ensuring that we effectively integrate and share terrorist-related information in order to prevent attacks. Can you share your thoughts on the current State of domestic terrorism information sharing? What does the U.S. Government need to do amid this rising threat to ensure that intelligence is not missed and that it gets to the people who need to know it?

Mr. TRAVERS. I will start, but I think probably pass it to Director Wray. The Intelligence Reform and Terrorism Prevention Act that created NCTC, written by this Committee, gave a number of statutory responsibilities to NCTC in the realm of international terrorism. There are references in the legislation to domestic terrorism, but quite clearly, the Bureau would have the lead, and I view NCTC as being in support. So we have, I think, a lot of things we can do, and our staffs are working on sort of laying out the parameters, but things like addressing issues of radicalization and mobilization, kind of left of boom kinds of questions, that NCTC has done a lot of work with our partners on the international terrorism side. I think it is pretty clear that the processes look a lot alike in terms of using social media and the Internet and so forth. We are broadening our aperture there, and collectively writing at the unclassified and For Official Use Only (FOUO) so we can get that kind of information to our State and local partners.

Where I think NCTC has particular value-add is in some senses “domestic terrorism” is a bit of a misnomer because of the international connections, and so we work a great deal with our partners around the globe because everyone is struggling with this problem right now and trying to figure out how to deal with it. And so we can bring a lot of analytic horsepower and potentially collection to the international problem set and then in regard help the Bureau.

Senator HASSAN. Thank you. I see that I am over time. I do not know if the Chair would like Director Wray to comment now or take it up another time.

Chairman JOHNSON. Briefly.

Mr. WRAY. I guess the short version would be that, in addition to everything that Director Travers has said, we are looking very hard at some trend of, for example, White supremacists or neo-Nazis here connecting through social media online with like-minded individuals overseas, and in some cases actually traveling overseas to train. As Director Travers said, we are engaging a lot with our five Immigration and Customs Enforcement (ICE) partners and others like that as we are comparing notes on this threat.

Senator HASSAN. All right. Thank you.

Thank you, Mr. Chair.

Chairman JOHNSON. Senator Harris.

OPENING STATEMENT OF SENATOR HARRIS

Senator HARRIS. Thank you. Good afternoon. As you know, our country is facing many threats, so I thank all of the witnesses for being here today.

Director Wray, I want to start by asking you about Rudy Giuliani, a close outside adviser and counsel to the President. Have you communicated with Mr. Giuliani since you were nominated as the FBI Director?

Mr. WRAY. No.

Senator HARRIS. And do you know if Mr. Giuliani holds any security clearance of any kind?

Mr. WRAY. I do not know the answer to that.

Senator HARRIS. Has Mr. Giuliani made any formal representations at least to the Justice Department or the FBI regarding his foreign relationships, business dealings, or conflicts of interest?

Mr. WRAY. I am not sure there is anything I could say on that here.

Senator HARRIS. Is that because this is a confidential matter or because you do not know or because they do not exist?

Mr. WRAY. That is in part because I do not know the answer for the whole FBI.

Senator HARRIS. What is the other part?

Mr. WRAY. If there were something that was shared with some other part of the FBI that I am not aware of, it might well run afoul of some of the other Issues that you mentioned.

Senator HARRIS. OK. Given the close relationship between the President and Mr. Giuliani, has the FBI told the President whether his counsel is a potential counterintelligence threat?

Mr. WRAY. I do not think there is anything that I can say on that subject.

Senator HARRIS. I recall that you have testified in the past that you have taken an oath to defend the Constitution, and I admire the way that you have said that, and I do believe that to be true. Do you believe that your first oath is to the Constitution or to the President?

Mr. WRAY. My loyalty is to the Constitution and to the people of this country.

Senator HARRIS. If an American acting on behalf of a foreign person was seeking to influence or interfere with an American election, would the FBI want to know about that?

Mr. WRAY. Again, I do not want to be misunderstood as wading in and commenting on specific recent events, but just as a general matter, any information about potential interference with our elections by a foreign government or by anybody else is something the FBI would want to know about.

Senator HARRIS. In sworn testimony before the Senate Appropriations Subcommittee in June, you said that you "could not think of an instance where the President has directly or indirectly asked you to open an investigation of anyone." As of today, can you confirm or deny whether the President has ever asked you to open an investigation as to anyone?

Mr. WRAY. Again, I cannot think of an instance in which that has happened. We have certainly had discussions about, for example, domestic terrorism threats, foreign intelligence threats, nation-states, things like that, but those have tended to be more about a threat in the aggregate as opposed to a specific individual or anything like that.

Senator HARRIS. Has the President or anyone on his behalf suggested that the FBI start, stop, or limit the scope of any investigation?

Mr. WRAY. Not that I can think of.

Senator HARRIS. In your view, would it be improper for the FBI to launch, limit, or stop a criminal investigation at the request of the President or anyone at the White House?

Mr. WRAY. Again, I am not going to wade into specific people's conversations, but what I will say is that the FBI's obligation and

my obligation and the obligation that I expect of all 37,000 men and women of the FBI is that we are going to conduct properly predicated investigations, continue properly predicated investigations, and complete properly predicated investigations.

Senator HARRIS. So without referring to any specific investigation, in your view, would it be improper for the FBI to launch, limit, or stop a criminal investigation at the request of the President or at the request of anyone at the White House?

Mr. WRAY. I think we should conduct our investigations based only on the facts and the law and the rules that govern us and nothing else.

Senator HARRIS. OK. I am going to take “nothing else” as meaning that you believe it would be improper to be asked by the White House or the President to engage in such conduct. Is that correct?

Mr. WRAY. Again, I am not going to wade into hypotheticals, but I think we are saying the same thing in the sense that I do not think—

Senator HARRIS. We are talking about rules and ethics.

Mr. WRAY. I do not think that the FBI should be concluding or closing an investigation for any improper purpose.

Senator HARRIS. OK. I am going to ask you one more time, and you will either answer it or you will not, clearly. But I am asking you about what is ethically appropriate. Would it be ethically appropriate to launch, limit, or stop a criminal investigation at the request of the President or anyone at the White House?

Mr. WRAY. I think there should be no opening of an investigation based on anything other than the facts and the law. That is my answer.

Senator HARRIS. Thank you. To your knowledge, has the White House or any member of the Administration ever directed or suggested that Attorney General Barr or any other member of the Justice Department start, stop, or limit the scope of a criminal investigation?

Mr. WRAY. I cannot speak to Attorney General Barr’s communications with others.

Senator HARRIS. During your time at the Justice Department and given your extensive and noble career, have you ever encountered suspects or defendants who tried to intimidate witnesses?

Mr. WRAY. Absolutely, and prosecuted some.

Senator HARRIS. Why is witness intimidation a threat to the pursuit of justice?

Mr. WRAY. Why isn’t witness—

Senator HARRIS. Why is it?

Mr. WRAY. Oh, why is it. I was going to say I happen to believe that witness intimidation is a threat to—because investigations and prosecutions should be about the truth and pursuit of the truth, and if witnesses who have firsthand information cannot and do not come forward, then that pursuit of the truth is frustrated and impeded.

Senator HARRIS. In June 2019, it was reported that hundreds of law enforcement officers around the country are in active members-only extremist Facebook groups. These groups include White Lives Matter, Ban the NAACP, Death to Islam Undercover. Can you tell

me what work your agency has done to investigate any of these cases and to what degree of success?

Mr. WRAY. I am not aware of the specific report that you are referring to. As I think I mentioned in response to one of the earlier questions, we do have about 900, say, give or take at the moment, domestic terrorism type investigations. That is, of course, not counting our hate crimes investigations. And a huge chunk of those involve some degree of what one might call "White supremacist ideology" as the extremist ideology that is motivating the crime that we are investigating.

Senator HARRIS. Thank you, Director.

Mr. WRAY. Thank you.

Senator HARRIS. Thank you for your service.

Chairman JOHNSON. Senator Scott.

OPENING STATEMENT OF SENATOR SCOTT

Senator SCOTT. I want to thank each of you for being here today. I want to thank Chairman Johnson and Ranking Member Peters for putting this together.

My focus today is on the FBI's ability to share domestic terrorism information and other violent information with local FBI offices and State and local law enforcement.

Let me start by saying that the men and women of the FBI are dedicated public servants. They serve this country selflessly with no desire for praise or public recognition. I understand that the FBI gets very little credit for their success, nor do they seek credit. I understand it is only the few instances of failure that get public attention and scrutiny.

The FBI deserves praise for the work that they do every day to keep us safe, but I also have concerns with the failures that occurred before a series of shootings in Florida and the lack of after-action transparency on the part of the FBI.

In the days following the senseless attack at Marjory Stoneman Douglas High School in Parkland, Florida, I learned of repeated failures by the FBI to properly investigate and act on specific tips received about the shooter in the months leading up to the attack. Weeks before the shooting, a detailed warning about the shooter was received by the FBI National Call Center. The warning was never passed on to the South Florida field office for an investigation or to any State or local law enforcement.

Months before that, the FBI was warned about the shooter through a comment on a YouTube video in which someone with the shooter's name stated, "I am going to be a professional school shooter." I understand the FBI gets a high volume of tips, but it appears the FBI did nothing with this detailed information of an imminent threat.

We are also aware of similar instances of pre-attack notifications received by the FBI regarding other attacks in Florida, including at the Fort Lauderdale airport, the Pulse nightclub in Orlando, and a Tallahassee yoga studio.

Since that time, I have repeatedly sought information from you, Director Wray, regarding the steps you have taken to hold accountable those within your agency responsible for those failures. I asked for two things: First, has anyone been held accountable? Sec-

ond, what changes have been made to prevent this from happening again? So far, I have gotten very little information. As Governor when this happened, I asked for an explanation, and I was told nothing. I got no information back. As a U.S. Senator, I put together a letter and asked for information on accountability and what changes have been made. Again, I got little information.

Mr. Chairman, I want to enter in the record the correspondence I sent and received.¹

Chairman JOHNSON. Without objection.

Senator SCOTT. The Parkland families have also told me that they have not gotten answers. So I am asking today: Has anyone from the FBI been held accountable for the failures that followed the attack at Marjory Stoneman Douglas? How have they been held accountable? And what changes have been made?

The attack was 100 percent the fault of an evil person. It is not the responsibility of the FBI, and people make mistakes. But the failure to act on specific information given to the FBI that could have stopped this evil person requires action to correct the errors.

I recently introduced the TIPS Act, which will require the FBI to be more proactive with sharing information with local and State officials. I would also like your feedback on that proposal, but, first, if you could talk about Parkland.

Mr. WRAY. Thank you, Senator. First let me say that there is no issue that tears up inside more than a threat to kids in this country, whether it is the kind of example that you are describing or any number of others. And that was a heartbreaking day for everybody in the FBI, and I hope you know that, and I mean that personally.

Second, we have made extensive changes. I immediately after the Parkland shooting dispatched a large special inspection team into CJIS, which is where our public call center is. As a result of that, a number of changes have been made, and without going into all the detail, let me just give you a few of the key points.

First, we have increased staffing significantly, both at the line level and the supervisor level.

Second, we have enhanced the training significantly.

Third, we have enhanced the technology significantly.

Fourth, we have added more oversight.

Fifth—and this goes to parts of your question—we put in place an entirely new leadership team with a wealth of experience, and we have made other personnel changes, some of them disciplinary in nature. Partly because of pending litigation against us and because of privacy implications, there is a limit to how much detail I can really go into on the personnel front, but there are significant changes that have been made.

I actually have personally gone out there not once but twice, first to see what it was like before, and second, now to see how it has changed since then. I have actually sat in the midst of the call operators, put on the headset, and listened as they dealt with the calls and watched how it happens. I can tell you that there is an incredible amount of really good work going on down there.

¹ The letter submitted by Senator Scott appears in the Appendix on page 79.

You mentioned the volume issue. I think it is important for people to understand that on any given day our call center up there gets more than 3,000 tips. Of those 3,000 tips, about 60 a day—that is 60 tips a day—are potential threats to life. So that is a huge amount of wheat having to get separated from the chaff there. Of the 60, probably about 80 percent of them have no Federal nexus whatsoever, and so we are looking at ways—and I know that that is the goal now coming around to your legislation. That is a goal that I think we share, which is how can we get the right information—that is the key word, the “right” actionable information, that wheat and not the chaff, to our State and local partners as far as possible. And there is something that we have in place that I would love to talk to you more about called “eGuardian,” which is a system that has been in place for a while that we have significantly enhanced, and the key takeaway from that, Senator, is that it would dual-route, so simultaneously go straight from the call center not just to local field office but also the State Fusion Center or the equivalent.

We have already had a number of instances—and I could go through a number of them here—where some threat comes in, and within hours, using that approach, within hours we have had an arrest.

I think we are very encouraged by the direction it takes, but make no mistake, this is one of the hardest things law enforcement has to deal with today, and we are doing our best, and we are going to keep working at it.

Senator SCOTT. So can you explain—so here is why I never get a response, OK? First off, I do not think you have an easy job. I know it is hard, and you get lots of tips. I get all that. But I have never heard that—and I do not get why somebody cannot say, “A person was disciplined,” “They were held accountable,” something. I am a business guy. In business, you have to hold people accountable if somebody made a mistake.

If somebody said, the person’s name, “I am going to be a professional school shooter,” that is pretty actionable, you would think, right? When somebody calls just a few weeks before a school shooting and they give detailed information, I mean, you have to believe somebody got held accountable. And to this point, I mean, the Parkland families have never been told that anybody was held accountable, and it is always this amorphous, “Well, we cannot,” it is privacy or something like that. There has to be something, a better answer than that, because it just seems, if you take their side, you would say nothing happened to them. Nobody got held accountable.

Mr. WRAY. Like I said, to me the privacy act issues and the pending litigation are things that I do have to take seriously in responding to your question, and I am trying to lean in in answering your question. I can tell you that there were two individuals principally involved with the call. We have had one individual that has been reassigned as a result of that inspection report and one who is, I guess the best way to put it is, no longer with the FBI. I really cannot go into more detail than that. But I would tell you that the more important thing is it should not be anybody’s impression, I can assure you, that nothing has been done. We have made mas-

sive changes out there, and I know we have invited you and your staff to come out and see it, and I would welcome that. I think you would be encouraged by what you have seen out there.

Senator SCOTT. All right. Thank you.

Chairman JOHNSON. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Let me just say thank you all for your testimony. I thought you gave excellent testimonies, and we appreciate that. Thank you for being here today and for the work that you do.

I passed Senator Sheldon Whitehouse. He was leaving as I was coming in. He is not on the Committee, so he did not get to ask questions, but he was going to ask if he could. He wanted to ask you about responding to the questions for the record (QFRs), Mr. Wray. I would just ask you to check with your team, just make sure that you are being responsive there, OK? He asked me to mention that, so I did on his behalf. I know you probably get a lot of those.

I was privileged to be the Chairman of this Committee a few years ago. Tom Coburn of Oklahoma was our Ranking Member, and it was during the Obama Administration, and we had a hearing or two with folks essentially from Homeland Security, Mr. Glawe, and the issue was Swiss cheese. You might say, "Why would it have been Swiss cheese?" Because the top leadership in Homeland Security kind of looked like Swiss cheese. We had a number of positions that were vacant, leadership positions. We had many others that were filled by people in acting capacity and had never been Senate-confirmed. We are happy that you are here and others that are filling in, but if he were here, he would probably say he had the same concern with all these people in acting positions.

I asked my staff to give me a number, and they said—

[phone rings]. That is Coburn right now. He is everywhere. I understand that when Acting Secretary McAleenan leaves—and I think he has been terrific. I hate to see him go. But I understand that 11 of the 18 positions requiring Senate confirmation will be vacant.

I will say that again: 11 of the 18 positions requiring Senate confirmation will be vacant. One of the reasons that Tom Coburn and I worked hard, along with the people on our Committee in those days, was because the Department of Homeland Security had the worst morale—it is measured about every 2 years. It had the worst morale of all the departments, major departments of government. One of the reasons why was because of that. And the last 2 years, when they finished up and that administration left, I remember talking to Jeh Johnson, and he told me that the last measurement—we have this measurement every 2 years where an independent entity measures the morale of the major departments, and the Department that made the most improvement in that 2-year period was Homeland Security. So it really does make a difference in more ways than we might expect.

But I would ask each of you—and I will just start with you, David—could you speak to how the lack of Senate-confirmed leadership at the highest levels of DHS affects the interagency work

that you all do to keep our homeland secure? This would be just for you, Secretary Glawe. How can we in Congress push the President to nominate qualified individuals in order to ensure the Department is able to carry out its vital mission? Please.

Mr. GLAWE. Senator, thank you for bringing that up. With 27 years in law enforcement and a career official, starting as a Houston police officer, it is an honor and a privilege to serve with the men and women of the Department of Homeland Security. They do an incredible mission. The career service members have carried on this mission with an incredible professionalism, and I am happy to say our employee viewpoint survey continues the upward trajectory. Even though some of these Senate-confirmed positions are not filled, we continue our upward trajectory, as well as in my office which has seen some of the biggest increases in morale this year, and your staff will have access to that.

I would say that we have two officials that are pending confirmation: our Under Secretary of Policy and our Chief Financial Officer. We would appreciate their speedy confirmation.

As one of the longest-serving Senate-confirmed—and you unanimously confirmed me—I appreciate that by the Senate and this Committee as well.

Senator CARPER. All right. Would either of the other witnesses care to comment on this? Please.

Mr. WRAY. Senator, I would just say, without speaking to DHS' leadership vacancies, that we work very closely with the men and women of DHS across all their different sub-agencies every day on our task forces. They are fantastic public servants and great partners, and we are proud to stand with them.

Senator CARPER. All right. Thank you.

Mr. TRAVERS. The same would be true of NCTC. I have many people embedded at DHS, and I have many I&A officers that work for me, and it is a very strong partnership.

Senator CARPER. All right. I was out of the room for a little bit. I do not know if this has already been raised, but I want to talk a bit about our withdrawal of U.S. troops from northeastern Syria. Something that troubles me deeply. I gave a speech on the floor, I think it was last Thursday, close of business, and I mentioned it. It was something like 11,000 Kurdish lives had been lost in the battle against ISIS. I have a friend, you ask him how he was doing. He says, "Compared to what?" Eleven thousand of their lives and a relative handful of ours. Every one of those is dear and precious, but I just want to ask, and we will start—let us see. I guess I am going to ask each of you this. We will start with you, Mr. Travers. But can you just please speak about the effects that pulling U.S. troops out from northeastern Syria will have on our Kurdish allies, please?

Mr. TRAVERS. I believe it is true that General Maxloun and the Syrian Democratic Forces (SDF) have been very close allies. They have been incredibly important in terms of providing intelligence over the years. We were heartened by both the President's and the Secretary of Defense's statement that the U.S. forces that will remain in Syria will have a continuing counterterrorism mission as well as the oil, and that there will be continued engagement with the SDF.

This remains a very important counterterrorism objective to us because they are guarding many different prisons with both foreign fighter and Iraqi and Syrian ISIS fighters. And so that relationship really needs to continue.

Senator CARPER. All right. And just a simple yes or no. Were you all consulted on this matter by the White House?

Mr. TRAVERS. I was not, but it would not necessarily be the case that I would be.

Senator CARPER. All right. Thanks.

Same question, if you could, Mr. Wray. Could you just talk a little bit about the effects that pulling out U.S. troops from northeastern Syria will have on our Kurdish allies? I know this is a little bit out of your wheelhouse, but take a shot.

Mr. WRAY. Well, parts of it are in our wheelhouse. In particular, we are obviously concerned about potential resurgence of ISIS if certain fighters in particular were to escape or be released. We will say that the biggest threat to the homeland, that is, the biggest ISIS-related threat here, in many ways in the online inspired threat, in effect the virtual caliphate. So that threat is something that we have been all over with or without the presence in Syria.

One of the things that we have done, we, FBI, along with others, working with our partners, anticipating the day where we might not be there, is biometric enrollment on the battlefield in effect, in order to put us in a position where fingerprints, DNA, et cetera, are available and can be shared with our allies and others so that in the event that fighters end up spreading out for one reason or another, we have a better chance of intercepting them before they do harm.

Senator CARPER. All right. Mr. Secretary, same two questions, if I could, and then I will be done. The same two questions, if you could, Mr. Secretary. Were you consulted on this matter by the White House? Just a yes or no is fine.

Mr. GLAWE. Sure, Senator, and no, I was not, and I would not be in my current role. But what I would say is as a follow-on to what Director Wray said, our partnership with obtaining the biometrics from the ISIS fighters, al-Qaeda fighters, any terrorist organization, is critical for our vetting program and our relationships with the intelligence services, our law enforcement services abroad, and our foreign partners. But the disbursement of terrorism is global. Southeast Asia, northwest/East Africa, Middle East are all threats from ISIS, al-Qaeda, Al-Shabaab and others, and affiliates. It is how we get that information and we vet them. So if the refugees or migration flows out of Yemen or Syria are large, we have to have the biometrics to collect to make sure they do not come here, to run them against systems to make sure they are not terrorists, criminals, or foreign intelligence officers.

So it is really critical, that information sharing and that vetting process we have to make sure bad things or bad people are not coming to the United States.

Senator CARPER. Thanks so much, and thank you all for your service, your leadership, and the people you lead.

Thank you.

Chairman JOHNSON. Senator Portman.

OPENING STATEMENT OF SENATOR PORTMAN

Senator PORTMAN. Thanks to the three of you for some great testimony today and, most importantly, for what you and the men and women who are in your organizations do every day to help keep us safe.

I noticed in your opening statement, Director Wray, you talked about the Thousand Talents Program, and as you may know, the Permanent Subcommittee on Investigations (PSI) with Senator Carper and others, we are in the process of looking into that issue and have done a series of hearings on related items, including on the Confucius Institutes. In fact, we did a Confucius Institute report that indicates that there are limitations that China places on the activities here, including censorship, as an example, not allowing the academic community here to discuss topics they believe are politically sensitive, such as, the Tiananmen Square uprising or something like that.

But as you say, it goes well beyond Confucius Institutes. You said that China is abusing the Thousand Talents program, I wrote. You also said that the FBI has about 1,000 cases, coincidentally, investigating technology transfer. And you said that universities should be smarter about defending themselves.

I guess my question would be: What efforts has the FBI taken to inform the higher education community about this threat? And what has your response been?

Mr. WRAY. I think you have put your finger on an important issue. The role of academia in our country, especially given the amount of taxpayer-funded research there is in particular, is a key component to this counterintelligence threat. So in addition to investigations—and I cannot give you the number out of the 1,000 that involve universities and, in particular, graduate students and researchers, but certainly it is a significant number. But in addition to the investigations, we are much more actively engaged with major universities in encouraging them and informing them so that they can take appropriate action voluntarily but robustly to guard against the threat.

As far as the reaction we have gotten, it varies. But I have been actually quite encouraged by quite a number of universities, which a few years ago would not have wanted to meet with the FBI under any circumstances, much less in the kind of partnership way that is occurring now, including very good responsiveness from Ohio State. I have met with them. We had an academic summit in FBI headquarters just about a month ago where we brought in chancellors and others from universities all across the country, a whole bunch of our SACs, and kind of briefed them on some of the threats and had engagement about how we can work more constructively together to help them defend themselves.

Senator PORTMAN. Our information is that Ohio State certainly, and some other schools, have expressed their interest in working even more with you and appreciate what has been done. They also, I think, are not providing us the transparency we need to know whether there is a problem. Would you agree with that?

Mr. WRAY. I would probably let Ohio State speak for itself in terms of its own transparency, but—

Senator PORTMAN. I am not talking about Ohio State. I am talking about just in general. We found out, as you may know, in our investigation as an example that about 70 percent of the schools were not properly reporting the foreign government payments that they were receiving with regard to the Confucius Institutes. So the transparency, although some of it is in law already and not being followed, is not adequate in our view. Is that your view?

Mr. WRAY. I think it is fair to say there is a lot of room for improvement, but we are seeing improvement.

Senator PORTMAN. Let me talk about another issue that is a national security threat for our entire country, but Ohio is particularly hard-hit, and that is the drug crisis and the epidemic of overdoses and deaths. We know that the Southern Border has lots of challenges. One is certainly the drug issue. We know that crystal meth, which is the new drug that is causing havoc in our communities in Ohio, but also heroin and cocaine, comes almost exclusively across that Southern Border. And my question to you is really about what is happening. You see a significant reduction in terms of crossings. I am looking at some data here that compares last month to the month of May as an example, almost a one-third reduction in crossings, or at least in apprehensions, which would indicate crossings.

So the number of people coming over has slowed considerably, still a significant issue but not like it was. And yet from all indications we have, the drug flow has not been reduced, even though many have linked some of the same traffickers who bring people across as bringing drugs across.

Can you speak to that and talk about how these drugs are coming over? Secretary Glawe, if you would like to speak to that, that would be helpful to this issue. But what more can we do, of course, on the border? But, also, what is the relationship between people crossing and drugs crossing?

Mr. GLAWE. Senator, thank you for the question. Just to give you the numbers from 2017 to 2019 so you know what we are dealing with on the narcotic flows, we have seen a 40-percent increase in cocaine from seizures at the Southwest Border. We have seen a 20-percent increase in fentanyl. We have seen a 30-percent increase in heroin. And to your point, we have seen a 200-percent increase in methamphetamine, and that is in addition to the emergency on the border we have with the migrant flows and Border Patrol and Office of Air and Marine and our Office of Field Operations being taken offline for just detention.

So we have a crisis at the Southwest Border, and it is all based on moving people and goods illicitly across the border. Cartels are about moving goods and people across the Southwest Border.

Senator PORTMAN. So with almost a third fewer people, have you seen any reduction in the drug flow? Because we certainly have not experienced that on the other end.

Mr. GLAWE. No. We have seen an increase. We have seen an increase, and that is what we are apprehending. So those numbers are probably low. That is what we are catching. That is what else is going in. So we have seen those increases in the last 2 years. The cartels are a sophisticated business about moving supplies to the United States. They are as good as any major business. There

are profits in it. It ranges largely, but they are a Fortune 500 company, and it is all about moving illicit goods across the border. And it is a sophisticated network—and I am sure you have heard the names—of plaza bosses which run and control what moves across the Southwest Border. And they are trafficking supply chains and their relationships with China, which is now—the fentanyl production that is moving into Mexico. It is very sophisticated, very robust, and constantly changing in dynamic.

Senator PORTMAN. I would love to follow up with you on that and maybe a QFR here on the fentanyl issue. My sense is there is not a lot of production of fentanyl in Mexico, but there is processing. They are getting it, just as we were getting it, through the mail system—and still do, by the way. But they are getting it to Mexico, often converting it into a pill form, and then sending it over. Again, a huge increase compared to even a few years ago, so a new threat on the border.

But, look, I think the demand side is key here. We have done a lot of work on that. We will continue to, on prevention, recovery programs, and treatment. But we have to do something to deal with the flow, too, because this crystal meth, I will tell you, on the streets of Columbus, Ohio, I am told it is less expensive than marijuana, and deadly. So we would appreciate any input you have as to how we can do a better job to reduce that supply, at a minimum not just reducing the poison coming into our communities, but reducing the impact because it will increase the cost.

Mr. GLAWE. Senator, I would just follow up. As far as actioning this, it is a sophisticated approach that goes beyond just law enforcement. It is a partnership with our U.S. intelligence community partners, our Mexican intelligence community partners, the Mexican military as well as our military. That partnership is robust, and we have a very good relationship with our Mexican partners. But it is really upping the game and a strategy to impact these groups. That is going to have to go city by city, State by State. As I mentioned to Chairman Johnson earlier, there are some areas that are primarily controlled by the cartels and that supply chain, it is very sophisticated and will require a real strategic approach to how we are doing business.

Chairman JOHNSON. Senator Lankford.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Mr. Chairman, thank you.

Let me first say to all of you thank you for the work that you are doing. You do not hear that enough. There are a lot of threats, and you face a lot of things, and you go through a lot of information each and every day for the sake of our Nation and for the people in my State in Oklahoma. And we appreciate that very much.

Yesterday we had an event in Oklahoma city that we just called “Day One.” It was an event that is 168 days away from the 25th anniversary of the Murrah Building bombing in 1995. Twenty-five years ago, we lost 168 Oklahomans, many of them Federal employees, and their families, many of them children. We remember distinctly well what domestic terrorism looks like in Oklahoma City, and we have not forgotten about that.

So from all of us and for the families and the people that I live around, we want to say thank you that you are staying vigilant in this, because we do not take domestic terrorism lightly.

So, with that, let me ask you an unfair question. As you look at your time that you have to spend and the threats that you face right now, give me a percentage of threats that you face based on domestic terrorism and acts and international terrorism that are coming. Is that 60/40? Is it 50/50? Is it 70/30? Again, it is an unfair question, but give me your best guess of what you are tracking right now.

Mr. WRAY. Are you asking specifically about within the terrorism threats or about all threats, writ large?

Senator LANKFORD. Within terrorism threats.

Mr. WRAY. I would think we are probably roughly half and half, international/domestic, on the terrorism front right now. Certainly the number of arrests that we had in fiscal year 2019 was, I think, 107 domestic terrorism arrests, 121 international terrorism arrests. The investigations of domestic terrorism, probably about 900 right now, say; about 1,000 HVEs.

Now, we do have other foreign terrorist organization investigations, so it is probably more investigations on the international terrorism side, but that gives you a little bit of a sense.

Senator LANKFORD. Right, that helps. When you identify the different types of international terrorism threats that are coming into the United States or that have a threat that you can identify coming toward the United States, is there a certain ideology that seems to be more typical for international foreign threats coming at the United States?

Mr. WRAY. Of course, we are looking at both Sunni and Shia threats, but I think in terms of the most immediate lethality, it is the Sunni threats that are the ones that are more concerning. I am sure Director Travers may have a few things to add to that, but, in particular, the ISIS-inspired attackers here, these are people who are not necessarily—did not get up in the morning true believers, but kind of spent time online, radicalize, and essentially have latched onto an ideology as an excuse to commit crude but very lethal attacks against often soft targets using easily accessible weapons. That is probably the biggest threat to the homeland.

Senator LANKFORD. Right. Senator Rosen and I have worked on an anti-Semitism task force and continue to be able to bring up some of the issues of domestic terrorism and threats, as has been already named, the threat that was just confronted this past weekend in Colorado toward one of the synagogues there. There is a growing sense of ideology in multiple different areas, and we are grateful that you are continuing to be able to engage foreign as well as domestic.

Let me shift topics just slightly on that because I wanted to get a feel for where we were on that. Let me shift to election security. This has been an ongoing issue that Congress continues to be able to address. We have talked about multiple times with the Department of Homeland Security and their responsibility to be able to address election security.

This Congress allocated \$380 million in election security funding in 2018 to States, but the last time that I tracked those numbers,

not even half of that money has been spent by the States yet. Do you have a good estimate at this point what the States have spent from the \$380 million that Congress allocated to deal with election security? How do you evaluate the status of preparation for election security right now?

Mr. GLAWE. Senator, as the head of intelligence, I will have to get back to you¹ on the States' allocation of those resources that we sent them. I will take that question for the record to come back with you.

Regarding the execution of what we are doing within the Department, you are very aware that the Cybersecurity and Infrastructure Security Agency that is run by Director Chris Krebs has had an aggressive partnership with all 50 State election officials and territories. In the lead-up to the 2018 election, we conducted over 1,400 field interviews and engagements directly with State officials.

Just to give you an idea of our production as far as intelligence sharing directly with the States, classified and unclassified, in the lead-up to the 2016 election, we did 24 intelligence reports. In the lead-up to the 2018 election, through my office we had 313, and we are going to do quite a bit more in the lead-up to 2020. We are looking at attacks on the critical infrastructure of the election systems, but then also, as Director Wray has mentioned as well, we are really looking at that foreign influence campaign, that covert influence, the use of social media, the amplifying effect to try to affect elections, but any range of things that could be used by threat actors at the State and local level, not just the Federal level.

Senator LANKFORD. Do you have what you need at this point to be able to help secure the elections?

Mr. GLAWE. Senator, I welcome a discussion and going back with my colleagues in the Department to have an answer for that, but at the Department we are aggressively posturing our resources in partnership with the FBI, in partner with all the other U.S. intelligence community assets as well, and specific collection requirements they have regarding what our vulnerabilities are. And then I would just like to highlight that we are in over 80 Fusion Centers, as we mentioned earlier, as an information touch point—and I created the information-sharing enterprise, the backbone of the technical infrastructure, which is the Homeland Security Information Network, which I have to thank—and I know you are not Appropriations, but you guys have funded and authorized us to use that, and that has been a fantastic information tool.

Senator LANKFORD. Thank you.

Director Wray, I need to ask you a question that I do not need a specific answer for, but we can get it in a classified setting and go through in greater depth on this. When American individuals travel to Russia or China, there seems to be ample number of individuals to be able to track them and to be able to follow them and to be able to make sure that they are aware of all of their movements. I have yet to be able to talk to an American yet that has traveled to China or Russia and said, "Yes, they ran out of people to be able to trail me."

¹ The get back response from Mr. Glawe appears in the Appendix on page 81.

Do you have the resources that you need for individuals that you have suspicion on that are Chinese nationals or Russian nationals currently in the United States to be able to make sure that we have coverage of the level that is needed for individuals that there is highest suspicion?

Mr. WRAY. I can tell you that our counterintelligence program is an area where we are in need of growth and resources, not just agents and analysts but linguists, and we need more data analytics. All of these issues, including on the one that you are mentioning, in today's world involve terabytes and terabytes of data. In order to be able to be agile to exploit that quickly and effectively, we need to have the right tools to be able to get through that information.

And so I know the President's budget request has requests in that category, but I can assure you that that is the kind of thing that would be put to great use quickly.

Senator LANKFORD. That is great. Thank you.

Chairman JOHNSON. Senator Romney.

OPENING STATEMENT OF SENATOR ROMNEY

Senator ROMNEY. Thank you, Mr. Chairman. One thing I have noted in each of the questions that have been answered so far is the questioners have begun by expressing appreciation to your respective agents for the work that they do. I think I certainly speak for myself and I believe I speak for all the members of the Senate that I have spoken with, and it probably includes almost all, which is there is a very profound appreciation for the sacrifice and the extraordinary professionalism of the men and women who serve in your respective agencies, and I hope that that is expressed to your members time and time again.

Mr. Glawe, you spoke about foreign nations in particular that try and interfere with our sense of unity in the country, our political process, our elections—Russia, China, North Korea, and Iran. Can any one of you give me, if you will, kind of a rough sense of is this an ad hoc process that goes on within the country, or is it organized by their governments and staffed by a certain number of people with a budget associated with it? If it is organized, do we have a sense of the scale of the enterprise that is undertaken by each of these countries to interfere with our election process to sow disunity through social media and the like?

Mr. WRAY. I think there might be more that we could say, in a classified setting on that, but what I would say is that all of those countries have designs in engaging in malign foreign influence in this country. Of them, the Russians are the ones who have most advanced this idea of sowing divisiveness and discord, the pervasive messaging campaigns, false personas, things like that. But certainly Iran we know is taking very careful note of what the Russians have done and has its own malign foreign influence efforts, some of which have a cyber dimension to them, and that is something we are tracking very carefully.

Of course, the Chinese, that is a whole other kettle of fish, as it were, and they have a very robust foreign influence effort here, but it is a different—they all have their own shapes and sizes to the problem.

Senator ROMNEY. But it is highly organized by each of their respective governments; it is not just something that is done on an ad hoc basis?

Mr. WRAY. I think that is a fair statement.

Senator ROMNEY. Yes, as you spoke, Director Wray, about the incursions on an hourly basis of Chinese in particular, but as well as other countries, into our corporate databases, our government databases and so forth, I thought about how impossible the task must be to try and protect all the places people can attack. I was reminded of the mutual assured destruction orientation that was part of our national security with regards to nuclear weapons.

Should we have a mutually assured disruption effort of some kind, which is to say is the only way to prevent the number of attacks and the severity of attacks that we are seeing an indication that we can do the same thing to them, only we can do it harder and bigger and more destructively such that they say, OK, we better stop or we are going to suffer as well?

Mr. WRAY. I do not know if I would say that is the only way. I think offensive cyber operations are an important part of any nation's cyber strategy and it is ours. We are working much more closely with the private sector than ever before in terms of trying to help them defend themselves and our relationships with businesses; ranging from small startups all the way to Fortune 100 companies are much more robust than when I was in this world when I was at DOJ many years ago. In many ways, today's cyber threat is less about and cybersecurity is less about preventing the intrusion in the first place, although that is obviously the goal, and more about detection as quickly as possible and mitigation as quickly as possible once you find it.

Think of the example it is great to put locks all around the outside of your house and cameras and lights and everything else. But if the guy has already managed to pay off somebody to get inside your basement and he is just hanging out there, all the stuff on the outside is not going to do a whole lot.

So a lot of the efforts today, working together with DHS and others, are trying to get organizations to be able to quickly find the threat, quickly tie it off, and prevent the damage from getting worse.

Senator ROMNEY. Just one question, and perhaps for any one of you or all three of you, and that relates to cryptocurrency. I am not on the Banking Committee. I do not begin to understand how cryptocurrency works. I would think it is more difficult to carry out your work when we cannot follow the money because the money is hidden from us and wonder whether there should not be some kind of effort taken in our Nation to deal with cryptocurrency and the challenges that that presents for law enforcement and for deterrence of terrorist activity. Am I wrong in thinking this is an area we ought to take a look at? Or is cryptocurrency just not a big deal as it relates to your respective responsibilities?

Mr. WRAY. Certainly for us, cryptocurrency is already a significant issue, and we can project out pretty easily that it is going to become a bigger and bigger one. Whether or not that is the appropriate subject of some kind of regulation as the response is harder for me to speak to. We are looking at it from an investigative per-

spective, including tools that we have to try to follow the money even in this new world that we are living in. But it is part of a broader trend, and Director Travers alluded to it in terms of the terrorist threat, in terms of our adversaries of all shapes and sizes becoming more facile with technology and, in particular, various types of technology that anonymize their efforts. Whether it is cryptocurrency, whether it is default encryption on devices and messaging platforms, we are moving as a country and as a world in a direction where, if we do not get our act together, money, people, communications, evidence, facts—all the bread and butter for all of us to do our work—we will be essentially walled off from the men and women we represent.

Senator ROMNEY. Thank you. I would just close, Mr. Chairman, and just acknowledging that the President today spoke of the tragedy which occurred in Mexico where apparently three women and six children were brutally murdered and has offered our national support to help the Mexicans get to the bottom of this. I appreciate the fact that you are willing to participate in that at the direction of the President, and hopefully we will find a way to bring people to justice who deserve to be brought to justice, and also prevent events like this from happening in the future.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator Romney.

Senator HAWLEY.

OPENING STATEMENT OF SENATOR HAWLEY

Senator HAWLEY. Thank you, Mr. Chairman.

Director Wray, a question on the cybersecurity topic, if I could, and as it relates to China in particular. Are you concerned about the growing practice of American technology companies, or any American companies, for that matter, storing large amounts of data, consumer data, business data, in China and sometimes storing the encryption keys to that data in China? What sort of a cybersecurity risk does this pose? Is this something you are tracking, that you are concerned about?

Mr. WRAY. It is something that we are concerned about, in part because Chinese laws require a level of access that is unparalleled certainly in this country in terms of law enforcement and security services. Chinese law essentially compels Chinese companies and typically compels U.S. companies that are operating in China to have relationships with different kinds of Chinese companies, to provide whatever information the government wants whenever it wants essentially just for asking. And so that creates all kinds of risks across the various threats that we have to contend with.

Senator HAWLEY. And your point there about the Chinese laws and the access to data that Beijing requires sort of works in two ways, doesn't it? It is a problem for American companies who choose to store large amounts of data in China because to do so, they have to partner under Chinese laws with some sort of Chinese counterpart that often has ties to the government, right? That is number one.

Number two, it is also a security risk from the point of view of Chinese-based companies who have access to our market, who do business here, gather large amounts of information on American

consumers, like TikTok, for instance, but actually are owned or based in China and, therefore, are subject to those same Chinese laws on data and data sharing. Is that fair to say?

Mr. WRAY. That is absolutely something that we are concerned about. You start with the proposition that an astonishing percentage of Chinese companies are, in fact, State-owned enterprises, but even the ones that are not technically State-owned enterprises, the ones that are ostensibly private are subject both to the Chinese laws that I referred to a minute ago as well as—and I think a lot of people just kind of gloss right over this. Any Chinese company of any appreciable size has by Chinese law embedded in them Chinese Communist Party cells, or “committees,” as they are called, whose sole function is to ensure that that company stays in lock-step with the Chinese Communist Party’s policies.

Can you imagine something like that happening with American companies and American policy? I mean, it is something that people need to take very seriously.

Senator HAWLEY. Yes, absolutely, and thank you for your work on this. I think as you point out, I think American consumers do not realize the threat to their own data security and privacy when American companies choose to store that data in China and thereby open up potentially that data to use by the Chinese Government, or they do not realize that Chinese-based companies who are doing business in this country are subject to those same laws. And so it works both ways.

Switching gears, Secretary Glawe, let me ask you about the border. Senator Portman was talking about the influx of meth and the serious effects it has in Ohio. I can tell you in the State of Missouri we are absolutely overwhelmed with meth coming across the border. There is not a community in my State—urban, rural, north, south, east, west—that is not just awash in meth.

You pointed out that between, I think it was, 2017 and 2019 the Southern Border apprehensions are up over 200 percent for meth. I just wanted to drill down on a few additional details here and to get your input.

Did I hear you to say to Senator Portman that the meth apprehensions and other drug apprehensions have continued to increase even as border apprehensions of illegal individuals have decreased? Is that right?

Mr. GLAWE. That is correct, and, again, this is a 2-year snapshot. So it was cocaine, 40 percent; fentanyl, 20 percent; heroin, 30 percent; and methamphetamine, 200 percent. That is at the border where we are seizing that. That is in addition to the migration challenges we have had just by officers taken offline with the detention processing. We are still seeing the numbers up.

Senator HAWLEY. Do you have any sense in the last few months—I know that we have seen a decline in the last few months of border apprehensions of individuals, but do you have a sense or do you know what the numbers for contraband look like?

Mr. GLAWE. Senator, we could get back as a QFR on that,¹ but what I would say—and I said this earlier—is the business model for the cartels is to move illicit goods and people across the border,

¹The get back response from Mr. Glawe appears in the Appendix on page 85.

to get them there and to move them. And that grows through a very sophisticated network inside the country of Mexico and south of Mexico, as well as a management structure called “plaza bosses” that occupy the entire Southwest Border. They control what goes across and what does not go across, and it is all based on money and moving people and goods.

Senator HAWLEY. Let me ask you this: You talked about fentanyl production moving at least to some degree to Mexico, from China to Mexico, although it sounds like it may be in partnership with Chinese outlets. Can you say something more about that?

Mr. GLAWE. What I would say is—we may want to take this into a classified setting, but we have seen that the fentanyl production and trafficking, as we would anticipate, the cartels own the supply chain in the United States and the trafficking routes getting in here, that fentanyl production and trafficking would begin to move into Mexico, and we are seeing that.

Senator HAWLEY. Finally, let me ask you this: You said that in order to address this crisis, the drug crisis, and the flow of drugs over the border, it would require a change in our whole strategic approach. Can you say more about what you have in mind and what you think needs to change, maybe what this Committee and this body would do to give you the tools that you need?

Mr. GLAWE. I would say I would welcome a conversation that would probably expand upon my partners here at this table, but in my prior capacity as a unique witness, I was the Deputy National Intelligence Manager for Transnational Organized Crime when I was at the ODNI. When I say that it is a strategic approach, what I mean is bringing law enforcement, U.S. intelligence community, Mexican intelligence community, and military assets to bear in Mexico in some of these lawless areas where the cartels are essentially running the area. But that also has to be hand-in-glove with our demand. The United States has a high demand for narcotics, so it is a joint process. It is in that realm of having that partnership with our Mexican counterparts in that space to identify the bad and fill it with the good.

Senator HAWLEY. Thank you very much.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator Hawley.

Before I turn it over to Senator Peters, just a quickly follow up, because I think we need to underscore this. Although our border is rather unsecure on our side, would you agree with the statement that on the Mexican side of the border it is pretty secure? There is not much that passes through the Mexican side of the border without Mexico—the cartels and human traffickers—knowing about it, correct?

Mr. GLAWE. The plaza bosses and the cartels run the south side of the border on the Mexico side. Does the Mexican military and law enforcement have the capability? They do. But it is going to require a strategic approach of how those resources that are deployed in partnership with us, but the cartels are incredibly powerful. We also have to bear in mind that there is a corruption angle that plays into this as well.

Chairman JOHNSON. So where there is a will to secure a border, there is a way, and Mexican cartels prove it on the southern side.

Mr. GLAWE. Chairman Johnson, I think your assessment there is correct, but there are models out there where we have been successful. Colombia is a model of success we had in partnership with that government years ago.

Chairman JOHNSON. Senator Peters.

Senator PETERS. Thank you, Mr. Chairman.

I just want to follow up on what I hope is the priority for all three of you, and that is to combat foreign influence in our elections. Director Wray, my question to you—and I think it is accurate that is a priority for you. Yes or no?

Mr. WRAY. Absolutely.

Senator PETERS. What direction, if any, have you received from the White House about the priority of foreign influence in our elections?

Mr. WRAY. I think it has been made crystal clear to us that it is a priority for us to combat malign foreign influence from any nation-state, including Russia, including China, including Iran, and others.

Senator PETERS. How has that been communicated to you by the White House?

Mr. WRAY. We have had numerous meetings over at the White House with the NSC and with others on election security issues, and so it has been sort of a recurring theme in those meetings.

Senator PETERS. Is the White House doing anything to coordinate with other security agencies? Are they pulling folks together in a coordination fashion, in your estimation? If you could explain how that is happening?

Mr. WRAY. Certainly we have had NSC meetings and NSC-driven coordination over the time that I have been Director. But, in particular, the way it works right now is that with the NSC's direction and the White House's direction, ODNI brings together a smaller group as opposed to the more sprawling NSC apparatus. In particular, it is us—FBI, ODNI, DHS, and National Security Agency (NSA) are sort of the key players and then others from time to time as need arises. There is all kinds of engagement between, for example, our Foreign Influence Task Force, which I stood up after becoming Director; the Russia small group at NSA that General Nakasone stood up; and there is, a similar type of body at DHS and so on, and ODNI. There is a woman at ODNI, very experienced, very seasoned, who then-Director Coats put and she has remained in charge of kind of coordinating the efforts kind of on a more day-to-day basis.

Senator PETERS. I continue to hear from my constituents in Michigan about very lengthy and intrusive screenings every time they travel, Secretary Glawe. They describe it as a “back-door travel ban” that discourages them from traveling, and it hurts their business and their families, and certainly maintaining safe and secure air travel while protecting civil rights of law-abiding travelers is a balance we may have to achieve, as we talked about earlier. You have a lot of balances that you have to do in your agency.

But my question to you is: The Department has indicated to my staff that they will now lead a comprehensive review of secondary screenings in fiscal year 2020 with input from other relevant Federal partners. Could you describe how you would envision that

process and how you would expect those recommendations to come out?

Mr. GLAWE. Ranking Member Peters, I would have to take that question for the record¹ to go back to U.S. Customs and Border Protection, who it sounds like would be leading that, because they are the ones that do the secondary inspections. But what I can say, coming from that organization, is we are always cognizant of the civil rights and civil liberties of U.S. citizens, foreign citizens who travel in the United States, and the protocols and the oversight with that has been very rigorous. But I will take that for the record and come back for an answer with you.

Senator PETERS. If you could do that in a quick manner, I would appreciate it.

The vast majority of constituents that I also hear from are very deeply dissatisfied with the DHS Traveler Redress Inquiry Program (TRIP), which is, as you know, the redress process for travelers who experience screening difficulties. Are there ways to expand and strengthen TRIP so that applicants do not feel ignored? Do you have some specific recommendations how we can make this process more efficient?

Mr. GLAWE. Again, similar to my prior answer. Being the head of intelligence, I will have to take that back for the record and have an answer for you on that.

Senator PETERS. I would hope we could get that answer quickly. I would appreciate it.

Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Sinema.

OPENING STATEMENT OF SENATOR SINEMA

Senator SINEMA. Thank you, Mr. Chairman. I appreciate our witnesses being here today.

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 to secure Arizona's border, keep Arizonans safe, and ensure that migrants are treated fairly and humanely.

I would like to start with the tragedy that occurred on Monday in Sonora, Mexico. My deepest sympathies and condolences go to the victims and their families. Details are still coming in, but we know that at least nine people, including mothers and young children, were murdered, apparently by transnational criminal organizations involved in the illicit drug trade. These victims have relatives from Arizona, and my State is hurting right now.

So my first question is for you, Mr. Wray. In this situation, will the FBI play a role in bringing these perpetrators to justice, ensuring that the families receive some redress?

Mr. WRAY. So thank you, Senator. We, too, are deeply troubled and heartbroken about the loss. We have through our legat office in Mexico reached out to our Mexican partners, to offer assistance and are engaged with them also with the embassy and the State Department.

¹ The get back response from Mr. Glawe appears in the Appendix on page 83.

In addition, we are in the process of having what we call our “Victim Services Division” get in touch with the relatives who are here in the United States to see if they can be of assistance. It is a Division that I think I am very proud of just given the way in which they bring a level of compassion and sometimes attention to some of the most basic concerns and needs of victims and their families.

Senator SINEMA. Thank you.

For all of our witnesses who are here today, I would like to get a commitment from each of you that my office is briefed on the investigation, and I would like to hear about your agencies’ efforts to combat transnational criminal organizations. As we see every day, the impact on Arizona and Arizonan families is unabated.

Mr. GLAWE. The FBI is the lead, obviously, with the United States persons being targeted by that violence overseas. What I would say is we are absolutely committed to meeting with you, Senator, and I would say as far as the benchmark of intelligence and operations, one of our top facilities is actually in your State, in Tucson, and I would be delighted if I could escort you there for a visit to see it. But it is really about that partnership with the State and local law enforcement, our Mexican partners, and sharing of that real-time, tactical-level information so we can identify those threats at the border, but really any way south of the border in Mexico and sharing that information with our partners in the Mexican Government.

Senator SINEMA. Thank you.

Mr. WRAY. Senator, we would be happy to try to keep you informed as best we can and as is appropriate. I will underscore that, of course, what role the FBI will be able to play in Mexico depends a lot on the willingness of our Mexican partners to embrace and bring us in, and that is still something that is being worked out. It is a very fluid situation right now.

So I do not, as we sit here right now, yet know exactly what our footprint, if you will, will look like, but we would be happy to follow back up with you as things progress.

Senator SINEMA. Thank you.

Mr. TRAVERS. The National Counterterrorism Center does not actually work that particular issue.

Senator SINEMA. Thank you.

I would like to ask you a question, Mr. Glawe. I spoke a few times with Secretary McAleenan about the need to improve information sharing between DHS and HHS regarding allegations of abuse that were reported by migrants who had been held at the Yuma Border Patrol station, I am sure you recall. Can you share the status of DHS efforts to ensure these types of incidents are reported more quickly and that swift action is taken when there are reports that require more protection of migrants and children?

Mr. GLAWE. Senator, as my role is the head of intelligence, I do not have a status update on that, but I will take that for the record and have an answer for you back.¹ But I will say as a career law enforcement official as well as a Federal law enforcement official, the men and women of the Department of Homeland Security oper-

¹ The get back response from Mr. Glawe appears in the Appendix on page 82.

ate at the highest standards, and when there is an incident that has to be reported to the Inspector General or to the FBI, that is handled quickly and mitigated as fast as possible within the Department.

Senator SINEMA. Thank you.

Back in September, this Committee held a hearing with outside experts on domestic terrorism. At that hearing I spoke about the importance of information sharing and ensuring that our State and local law enforcement entities can access the information they need. Such information sharing is always easier for larger police departments, such as those in Phoenix or Tucson, but is more challenging for our rural sheriffs.

With regard to information sharing between Federal, State, and local law enforcement entities, what steps have your agencies taken in the past year to ensure that small or rural law enforcement entities are able to get better access to information about threats and trends? What do these agencies still need to improve on?

Mr. WRAY. So I will start, and then turn it over to Under Secretary Glawe. On our end our principal engagement from a day-to-day basis with our State and local partners, which includes some very small departments, is through our Joint Terrorism Task Forces, and we have 200 of them all over the country. We have task force officers, which are essentially State and local officers from, in many cases, including some of those small departments who work full or in some cases part time on our task forces, which gives them access to all the same information that all the FBI folks and Federal partners on the task forces have. That is probably the most significant means.

In addition, we jointly with DHS on a number of instances will put out bulletins of different sorts—they are pretty frequent—that provide information in a fairly granular way about what we are seeing in terms of threats and so forth. So those are some of the big ones that I would highlight. I will maybe let David chime in.

Mr. GLAWE. Yes, just to follow on that, a couple of the big infrastructure—and I will talk about very specifics with Arizona and the Southwest border. So my office hosts the Homeland Security Information Network-Intel. So we host the products for the FBI, for the Department of Homeland Security, our State and local partners, and the private sector. There are currently 42,000 products on it. In fiscal year 2017, we had about 17,000 or so views. I am happy to report that in 2019, after a very aggressive rollout we had over 90,000 views. We hosted over 11,500 products. This is an unclassified network that is available in all Fusion Centers as well as satellite locations at a log-in capability.

Regarding the Southwest border, because, you are right, we have a limited capacity, and they need intelligence officers to give them tactical-level information, unclassified information and classified. I did a pilot program starting in, I believe it was, June and May. I put 19 DHS intelligence officers on the Southwest border to include Arizona. That resulted in 45 drug seizures—45 drug-related arrests, 35 seizures of weapons and drugs, and 115 intelligence reports. I am going to permanently deploy I think right around ten intelligence officers permanently to the Southwest border in the

very small sheriffs' and municipal law enforcement departments to enable them to do an enterprise approach and scale capabilities to share information.

Senator SINEMA. Thank you.

A follow up question for both of you. Last year, Congress passed and the President signed into law the Preventing Emerging Threats Act which grants authorities to DHS and the DOJ to counter threats from unmanned aircraft systems. During my visits to the border, I have seen evidence of the threats these drones can pose. I have actually watched drones come over the border in broad daylight.

So could you tell us about what DHS and DOJ are doing to mitigate the dangers to our Nation from these unaccompanied aircraft system threats?

Mr. GLAWE. Senator, thank you for the question, and I was Chairman Johnson's—one of his lead witnesses in the lead-up to passing that legislation that he championed, so I can speak specifically, and I was also on the Southwest border and did a report from there for one of the news networks. So this is a threat that continues to be a threat. We track that at the Department of Homeland Security, not just on the Southwest border but on drone incursions over critical infrastructure, and we are seeing a percentage increase that just keeps increasing. In engagement with our State and local and private sector partners, I was just out with the Los Angeles Police Department chief and the New York Police Department commissioner, on drones. While the drone legislation was an outstanding first step, they are saying now that they need more capabilities and more within their own authorities to mitigate these threats.

But the Southwest border is just one of the many drone threats that threatens our critical infrastructure, our mass gatherings, and ways to move illicit goods over the border as well as use it as a countersurveillance platform to suck up information from our military or our law enforcement or our private institutions in the country.

Mr. WRAY. I would just add that while we are extremely grateful to the Chairman and others for that legislation, this is a threat that is overtaking us in many ways. We are currently investigating a number of incidents in the United States of attempts to weaponize drones in one way or another. Certainly we have been seeing them, as you mentioned, down on the border. We have also seen drones used to deliver contraband into prisons, and, of course, as the rest of the Committee knows as well, there have been efforts to use drones quite frequently on the battlefield against our forces and our allies overseas.

Our focus from the FBI end has been principally on the mass gathering situations, so we are very focused on things like the Super Bowl, etc., not because the others are not incredibly important, but just in the realm of being able to prioritize the use of these new authorities. That is at the moment where we are. There is going to be a need for more technological solutions. Disrupting drones over large, crowded civilian areas is a different kind of exercise than doing it in the battlefield. We are working very closely

with our partners, DHS, Department of Transportation (DOT), Department of Defense (DOD), and obviously DOJ on that.

Senator SINEMA. Thank you.

Mr. Chairman, I have exceeded my time. Thank you for your indulgence.

Chairman JOHNSON. Yes, you have.

Senator SINEMA. Sorry. I apologize. [Laughter.]

Chairman JOHNSON. Thanks, Senator Sinema. But you used it well because you actually asked a question I was going to ask about drones.

Senator SINEMA. Oh, see? Then it is not actually my time. It is fine. It does not count.

Chairman JOHNSON. So let me quickly follow up on that, though. We always felt that piece of legislation was just a first step, begin those authorities so you could begin doing the research and develop the strategies for doing something very difficult to do.

So the question I have: How far have we come in terms of doing that research, developing those strategies? Do you already need more authority? Do you need another piece of legislation? Have you come far enough where we need to go to the second step?

Mr. WRAY. I do not think I am quite ready in this kind of setting to propose some kind of additional legislation, but what I would say is that I think there is—if memory serves, there is a report that we are scheduled to be providing to you all on exactly the question you are raising to address the need for identifying other gaps that might exist. And I do know, from traveling around the country and meeting with State and local law enforcement, that while they are very excited that Federal authorities now have this civilian use capability, they want to know when they can get it.

Chairman JOHNSON. They are still acting.

Mr. WRAY. Right.

Chairman JOHNSON. So you are not ready to say—I will ask Under Secretary Glawe the same thing. You may not be ready right now to propose a piece of legislation, but you are basically saying sometime in the future you will need some more authority, if not the Federal Government, also local officials.

Mr. GLAWE. Yes, just to follow on what Director Wray said, our science and technology branch is partnering with the FBI down at Quantico on the countermeasures and how we are supporting national security special events and identifying and mitigating those threats. But the threat is bigger than those national security special events.

What I would say is we monitor it from the analyst side of the emerging technologies. We have radio-controlled drones. We are now moving into 4G, which will have 5G capabilities. What is that going to look like? Is the legislation keeping up with that capability of the emerging technologies? I think that is a question to come back and have that discussion on.

But as this technology advances so rapidly for commerce purposes, the nefarious aspects of it or just from a safety aspect, I think there is a conversation to be had on how we have to really stay on top of the legislation on this.

Chairman JOHNSON. Again, we will have to cooperate. That report will be important.

By the way, part of the main reason we were able to pass that piece of legislation is because we have the video of—I believe it was ISIS using this in Iraq, and you can see the drone go over the target, lower, drop a bomb, boom, pinpoint accuracy. And that got everybody's attention. It still took us a little while. We were not able to put it in the National Defense Authorization Act (NDAA). We finally got it in the Federal Aviation Administration (FAA) reauthorization bill, but that cooperation is going to be important.

Director Travers, you addressed a little bit the situation of ISIS prisoners. I want to drill down a little bit deeper. First of all, have our European partners started stepping up to the plate and gotten a little more serious about—and, again, I realize, because I talk to them all the time, it is very difficult. They do not necessarily have laws to handle this. But are they considering the return of foreign fighters and prosecuting them under their own laws so that they are just not looking to somebody else to detain these people forever?

Mr. TRAVERS. You are quite right that the issue of repatriation has been a problem for years because of the inability to either prosecute—because of lack of evidence or short sentences, they have not been willing to bring prisoners back. They have been somewhat more willing to bring women and children back, but even that has been a bit of an issue.

Ever since over 2 or 3 weeks ago when the incursions started, there has been a flurry of activity I think within European capitals about trying to bring their women and children home, in particular, out of some of the internally displaced person (IDP) camps, out of humanitarian interests. We have not seen any increased level of willingness to bring their foreign fighters back. In fact, there has been some getting rid of citizenship just so that they can kind of wipe their hands of it.

Chairman JOHNSON. In terms of responsibility duty sharing, I have heard the proposal that maybe the Arab States could go into the camps with women and children, go through a sorting process to a certain extent, which of those detained individuals can potentially be rehabilitated, brought back into society versus those that need to be considered for longer-term detention. Are you hearing efforts or any kind of initiatives occurring along those lines?

Mr. TRAVERS. I think frankly, right now, because there is so much turmoil and uncertainty geopolitically about who is going to control these things, the likelihood of that is probably going down. There has certainly been some willingness on the part of the Iraqis in particular to bring back IDPs out of Al Hol and so forth. There are 30,000 or 40,000 people there. But, in general, it is a pretty difficult proposition to even know where these people are as they get moved around.

Chairman JOHNSON. So give me your general assessment of all the players, and we have Turkey and we have the SDF and we have Assad and we have Russia, we have Iran. Obviously, we have our desire to make sure that ISIS cannot reconstitute. Is there pretty much a universal desire not to allow ISIS to reconstitute? Or is there a little bit less commitment on the part of some of those players?

Mr. TRAVERS. There is no one that wants ISIS to reconstitute. I think it is fair to say that the Turks, for instance, are more concerned about PKK than they are against ISIS. I do not think anyone has as much concern as perhaps we do in the area about ISIS. But, in general, for instance, my guess is there is going to be an effort to keep those prisoners in prison whomever gets control of the prisons if the Turks move any further south.

Chairman JOHNSON. OK. My final question is for honestly all of you who want to contribute to this, but the Blue Ribbon Study Panel that we had testimony from a couple of years ago, their primary conclusion was we need somebody in charge. I think their recommendation was put it in the Vice President's office, and back then Vice President Biden, pretty close to the end of their term, said, every administration will be somewhat different. But we had the same issue when we were discussing 5G in our hearing just last week. I think we found out that it is the National Economic Council and Larry Kudlow is kind of in charge of the 5G aspect of cyber.

But if you go all the way down the list, whether it is, catastrophic electromagnetic pulse (EMP) or geomagnetic disturbance (GMD) attack, a cyber attack shutting down our electrical grid or financial system, some kind of weapons of mass destruction (WMD) chemical or biological attack—natural disaster, I think we pretty well assume Federal Emergency Management Agency (FEMA) is going to take charge of that, starting with local, then State, and then FEMA comes in when it overwhelms the State and local governments.

In the other instances, is there a sense within your agencies that you know exactly who is going to be stepping up to the plate in terms of recovery and response to one of these potential catastrophic threats? I will start with you, Under Secretary Glawe.

Mr. GLAWE. From the Department it is very well defined. I mean, the Federal Emergency Management Agency is there as well as the Cybersecurity and Infrastructure Security Agency Director Chris Krebs in that position. So within the Department it is clear, and the lines from the intelligence, from the vulnerability side, are clearly mine, and the collection requirements going to the U.S. intelligence community and foreign partners flows through me. So I would say within the Department I am very comfortable to say the lines of effort are—

Chairman JOHNSON. But, again, that is within the Department. Are there going to be turf battles? Is everybody going to be looking at and pointing fingers at somebody else in terms of who has the overall responsibility, who is in charge?

Mr. GLAWE. I mean, from FEMA's standpoint, I think that is very clear, their response capability. And within the Cybersecurity and Infrastructure Security Agency, I think that is very clear.

From the intelligence apparatus, as Director Wray had mentioned, we have a National Intelligence Manager for Cyber that aligns our intelligence capability at the ODNI.

Chairman JOHNSON. Director Wray, obviously, the FBI frequently is first on the spot in some of these mass shootings. What about a catastrophic type of attack on infrastructure? Do you have a sense or do you know exactly what the line of authority is, obvi-

ously starting with the President, but I mean at an operational level within these departments and agencies?

Mr. WRAY. I will take the two categories in turn. There is the terrorist category, if you will, and then there is the cyber category. I think you are asking about both? Or—

Chairman JOHNSON. Yes, I am just talking about no matter what might shut down an electrical grid or shut down our financial, whatever could really represent almost an existential threat to this Nation or be so catastrophic in terms of power outage.

Mr. WRAY. I think what I would say on the terrorist attack category, for example, I have actually—as somebody who was in the FBI headquarters building on 9/11 and intimately involved in these issues during the years after 9/11, and then having now come back to this world with some time in the private sector in between, I can tell you that the machine that exists now across the U.S. Government with our partners at the State and local level, through the Joint Terrorism Task Forces, etc., is so much more mature and robust and kind of a well-oiled machine in terms of everybody working together that it was one of the most pleasant surprises I found in coming back. So I think the lanes in the road and the way in which everybody works together is pretty well defined in the terrorist space.

In the cyber arena, likewise, although it is slightly different lanes. As I said in response to one of your colleagues' earlier questions, in a major cyber incident, the FBI is in charge of investigating the threat, but DHS has to be joined at the hip in terms of making sure that appropriate steps are taken to protect the asset, and there are well-defined lanes there.

I think there is a temptation sometimes to assume that one person needs to be responsible for all those things. I think really the premium is on coordination, and at some level, given the unique nature of the authorities that are involved in whether it is a terrorist incident or a cyber incident, you start talking about law enforcement authorities that are constitutionally entrusted to the Attorney General. You have military responsibility, offensive cyber, for example, that are in the lane of DOD. I think that while it might sound nice to try to create some new person who would be in charge of all that, I think, in fact, it would be more complicated and actually would not accomplish what was designed.

So the key is to make sure everybody has their lanes and their responsibilities well defined and the partnership, and that is what I think I am seeing day to day.

Chairman JOHNSON. So not to put you at odds with the Blue Ribbon Study Panel, you are a little less concerned about that. What you are seeing now, you are seeing a fair amount of coordination, and you do not lose a whole lot—you may lose sleep over the threat, but you do not lose sleep over the fact that it would just be chaos, that nobody would know who is in charge or we would not know how to coordinate or cooperate within the agencies?

Mr. WRAY. There is always room for improvement, and that is important. I do not want to be understood as thinking everything is just hunky-dory. But we are, I think in a so much better place as a country and as a government, and I would say that across gov-

ernments, Federal, State, and local, than we were even just 5 or 6 years ago.

Chairman JOHNSON. Again, I think we learned a lot from Hurricane Katrina, and from what I can assess, we have made great strides since that point in time.

Director Travers, do you have anything to add to that?

Mr. TRAVERS. "Whole of Government" rolls off the tongue pretty easily. I would completely agree with Chris. I have been doing terrorism pretty much since 9/11, and I do think that the counterterrorism community, writ large, is the best integrated effort across the entirety because we have been doing it forever.

Because we have not been attacked in the country now really—you have to go back 10 years to Umar Farouk, something really potentially big, there is a muscle memory issue, it seems to me, and I am big into interagency exercises to just kind of compare notes and who is doing what, because new people come around. While we are much better coordinated than we were, I think it is always useful to get people together and put them through their paces.

Chairman JOHNSON. OK. I did not think it possible, but actually the answer to that last question gave me just a little bit more optimism.

Again, let me thank you all for your service, and like so many of my colleagues on the Committee here, please convey to the men and women that serve with you our sincere appreciation for their service and sacrifice. I think that came across loud and clear, and we sincerely mean it. That also gives me a fair amount of optimism. When I see the quality of the Federal workforce, it does make you rest a little bit easier, even though we are facing some pretty complex, pretty difficult threats. So, again, thank you for your service.

The hearing record will remain open for 15 days until November 20th at 5 p.m. for the submission of statements and questions for the record.

This hearing is adjourned.

[Whereupon, at 4:45 p.m., the Committee was adjourned.]

A P P E N D I X

Opening Statement of Chairman Ron Johnson “Threats to the Homeland” November 5, 2019

As submitted for the record:

The threats we face today are all too familiar. Most fall within the categories of the four main homeland security priorities of this committee: border security, cyber security, critical infrastructure security, and countering violent extremism. Unfortunately, these threats are evolving with the advance of technology, and countering them is becoming increasingly more complex and difficult.

This past year, 977,509 illegal aliens, mostly families, streamed across our southern border. This unprecedented surge is the product of a broken immigration system with legal loopholes that create perverse incentives for families to make a perilous journey to our country. Cartels and transnational criminal organizations profit not only from the fees they charge for safe passage, but also by using migrants as a diversion to smuggle even more illegal narcotics into our country. In the worst circumstances, these criminals traffic migrants against their will or subject them to involuntary servitude. Although the illegal flow has decreased from the month of May's daily average of 4,651, the daily average still exceeds 1,400, and Congress has failed to act to address the root causes.

As our world becomes increasingly interconnected, the risk of - and harm caused by - cyber-attacks have grown exponentially. In addition to the persistent threats posed by state actors like Russia, China, Iran, and North Korea, we must also confront the threat posed by criminal actors. Ransomware attacks not only target individuals, they have held entire cities hostage.

The 16 sectors of our critical infrastructure remain vulnerable to attack from foreign actors and to natural disasters like an EMP or GMD event. The race to 5G is underway, and we need focused and determined leadership to unlock this tremendous value for the U.S. economy. We must also protect our supply chain and that of our allies and close international partners. Supply chains that are not secure pose risks to our competitive advantage in commerce and to our national security.

Terrorism and targeted violence remain serious threats to our nation. Over the past year, the number of domestic terrorist attacks has continued to rise. Although the threat of international terrorism has seemingly waned after the defeat of ISIS's physical caliphate and the recent elimination of its leader, we must remain vigilant as terrorist organizations regroup and evolve, foreign fighters leave Syria in search of new battlefields, and homegrown violent extremism becomes a growing reality.

Today, we will hear from three of the key agencies charged with defending our nation. I thank each of you for your service, and for participating in this important hearing. I look forward to your testimony.

**U.S. Senate Committee on Homeland Security and Governmental Affairs
“Threats to the Homeland”**

**OPENING STATEMENT OF RANKING MEMBER GARY C. PETERS
NOVEMBER 5, 2019
AS PREPARED FOR DELIVERY**

The Department of Homeland Security was created to defend the United States from any and all threats to the safety of our nation. The Department and its leaders are critical to our national security efforts, and we rely on them to effectively coordinate with both the National Counterterrorism Center and the FBI to provide a unified effort to defend the homeland.

When DHS was first created, in the aftermath of 9/11, the agency’s mission was clear – combat the scourge of international terrorism and ensure that we could say with confidence: never again.

But over time, that narrow focus has expanded, as the threats to our homeland have grown and become more dynamic.

New terrorist groups devoted to striking America and our allies have emerged.

Foreign adversaries and cyber criminals seek to infiltrate and disrupt the nation’s cyber networks, posing an asymmetric threat that could cripple our economy with the click of a button.

Foreign interference in our domestic affairs has presented a complicated new challenge that we are still scrambling to adequately address.

A rise in domestic terrorism, specifically acts of violence carried out by white supremacist extremists, has targeted racial and religious minority communities across the country.

Every year, we hold this hearing to examine these and other threats facing our country and to hear from the heads of the agencies responsible for keeping Americans safe.

The safety of Americans is built on partnership – partnership between our security agencies here today, partnership between agency leadership and their staff, and partnership between Congress and the Administration.

As we convene this hearing without a Secretary of Homeland Security, Acting or otherwise, I am deeply concerned these partnerships are unravelling. The absence of steady leadership at the Department of Homeland Security is a driving force for institutional breakdowns that risk making us all less safe.

The Department needs, and the American people deserve, qualified, consistent and stable leadership that will empower the brave women and men at DHS to protect the homeland, respond to natural disasters, and allow our nation to grow and prosper.

This Committee will continue to exercise thorough oversight of your departments’ efforts to ensure that communities are protected from these threats. But that requires cooperation from your agencies and your compliance with Constitutionally-mandated oversight requests.

I am extremely disappointed in your agencies' failures to provide a sufficient, or in the case of the FBI, any, response to bipartisan requests from this Committee about the growing threat of domestic terrorism and white supremacist violence.

No one should live in fear of being attacked in their neighborhoods or in their houses of worship. This is a serious and growing threat, one we must address in order to save lives and to protect the very core of what makes us a free, diverse, and vibrant people.

I am grateful that your departments have taken the important step of presenting a framework for addressing this threat. But we cannot stop with a simple acknowledgement or a strategy put onto paper. This threat is not theoretical, and neither should be our response.

I insist that you comply with our outstanding, bipartisan requests immediately as Congress works to combat the very real threat of domestic terrorism.

This Committee and your agencies must work together to review the policies and actions needed to keep Americans safe and ensure they are successful.

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.



TESTIMONY OF

David J. Glawe
Under Secretary
Office of Intelligence and Analysis
U.S. Department of Homeland Security

BEFORE

U.S. Senate
Committee on
Homeland Security and Governmental Affairs

ON

"Threats to the Homeland"

2:30 p.m., Tuesday, November 5, 2019
216 Hart Senate Office Building, Washington, DC

Introduction

Chairman Johnson, Ranking Member Peters, and distinguished Members of the Committee, it is my honor to appear before you today to testify about the Department of Homeland Security's (DHS) vital national security mission and explain how we are implementing policies to confront today's emerging worldwide threats.

Let me first say that the men and women of DHS are exceptional and dedicated professionals who work tirelessly to protect the Homeland from foreign and domestic threats. Their efforts play a vital role in ensuring that all Americans can be confident in their homes, schools, and houses of worship, as well as in public spaces. They represent the core of our Department and the best of our country. I appreciate your continued support for them and the various missions they undertake each day.

The Evolving Threat Environment Since 9/11 Attacks

As you know, our Department was created in the wake of the devastating 9/11 attacks and was charged with coordinating and unifying the Nation's homeland security enterprise. Our mission is multidimensional, built on the five pillars of prevention, protection, mitigation, response, and recovery. It is a calling that has been heeded by thousands and a mission that has been achieved successfully for nearly two decades.

Although many years have passed since the pivotal moment that gave us a permanent mission, we have not forgotten that day or relaxed at our post. We cannot afford to, especially with the new threats that are arising throughout the world.

Today, I will share with you seven major shifts I see in the threat landscape since 9/11, and the efforts DHS is executing upon to combat them. Specifically, I would like to speak about the threats we face from foreign terrorism, domestic terrorism, malicious cyber activities and the illicit use of emerging technologies, counterintelligence and foreign influence within the homeland, and the broad topic of the illicit movement of people and goods, particularly in the Western Hemisphere, which supports human smuggling and human trafficking, and global illicit drug sales and distribution.

Underpinning nearly all these threat vectors is an increasing rise in adversarial engagement from nation-states such as China, Russia, and Iran. I would like to be clear at the outset that we face today nation-state-level challenges to our interests and global democratic principles of a degree that we have not faced in many, many years. These nation-state adversaries seek to undermine, destabilize, discredit and damage the United States through dynamic and multi-dimensional strategies that target not only our physical assets, but also our social cohesion and our confidence in our very way of life.

Foreign Terrorist Organizations

That said, the primary reason DHS was formed was to counter the threat of terrorism. Therefore, the first issue I want to address in the threat landscape is the threat posed by Foreign Terrorist Organizations (FTOs), which remain a core priority of DHS's counterterrorism efforts.

We have had significant successes mitigating the foreign terrorist threat here at home since 9/11 and continue to make substantial progress in our ability to detect, prevent, protect against, and mitigate the threats that these groups pose. We have achieved these successes by utilizing a range of tools to identify and detect foreign terrorist actors and prevent them from entering the country. To ensure that foreign terrorist actors cannot enter through designated ports of entry or exploit the immigration system, the Department maintains numerous vetting programs and capabilities. We prevent thousands of terrorist-watchlisted individuals from entering or traveling to the United States each year through these efforts, in cooperation with the Department of State, Federal Bureau of Investigation (FBI), and other agencies. Additionally, DHS, particularly through Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) and U.S. Customs and Border Protection (CBP), represents the largest federal contributor of personnel, outside of the FBI, to the Joint Terrorism Task Forces (JTTFs). At the JTTFs, DHS officers and agents are engaged in a majority of counterterrorism investigations every year and employ their unique authorities and capabilities every day to identify, disrupt, and dismantle threats associated with foreign terrorist organizations. Furthermore, our DHS component agencies patrol and rigorously enforce land, air, and sea borders, offering a critical final line of defense.

However, in spite of these successes, the threat of foreign terrorist organizations remains a significant concern. Whether through direction or inspiration, these groups seek to spur our youth and our disaffected to violence — encouraging them to strike the heart of our nation and attack the unity of our vibrant, diverse society. ISIS, al Qa’ida, Lebanese Hezbollah, returning foreign terrorist fighters, and those still in prison in theater represent significant, persistent, and long-term national security threats to the United States.

Since 2011, the situation in Iraq and Syria has marked one of the most significant challenges to our ability to track and combat foreign terrorist actors. As many of you know, failed states and lawless areas represent opportunities for the restructuring, rearmament, consolidation, and emergence of FTOs. These organizations may target our interests and aspire to target us here at home. Given the opportunity to identify and control safe havens, they have proven capable at directing such attacks beyond the boundaries of a geographic region.

We must ensure that we continue to work aggressively across our government, and with our international partners, to pressure and disrupt ISIS and other terrorist organizations targeting the United States homeland. DHS will continue to work closely with our international partners in the European Union and around the world to ensure that we are leveraging our expertise in screening, vetting, and border security — particularly in areas known to be vulnerable to large influxes of migration from this region, as these locations offer significant opportunities for exploitation by our FTO adversaries — to enhance our partners’ capabilities.

We need not only focus on detained ISIS fighters, but also on gaining a better understanding of those individuals who have been forced into displaced persons camps within the region and subsequently potentially subjected to attempts from hardened ISIS fighters or sympathizers to radicalize them to violence. Furthermore, we must recognize that the threat from women and teenagers radicalized to violence is potentially as critical today as that from men. We must adapt to this reality.

DHS Strategic Framework for Countering Terrorism and Targeted Violence

Perhaps one of the most significant evolutions over the past few years has been domestic actors' adoption of FTO techniques to inspire individuals via the internet to carry out acts of terrorism and targeted violence. Of specific concern has been an increase in racially and ethnically motivated violence. In September, DHS introduced a new *Strategic Framework for Countering Terrorism and Targeted Violence*, which explains how we will use the tools and expertise that have protected the country from foreign terrorist organizations to address the evolving challenges of today. The *Strategic Framework* is intentionally forward-looking in its understanding of technology's role as a factor that can exacerbate problems, but also one that can provide new solutions to combat the threats we confront. We have begun the implementation of the *Framework* and will publish a public Action Plan that captures how DHS is working alongside our interagency partners to see this vision to fruition by the end of the Calendar Year.

The framework is designed to assess DHS's past and provide a guidepost to its future. Today, we face a growing threat from domestic actors inspired by violent extremist ideologies. The prevalent trend of Americans driven by violent extremist ideologies or personal grievances to commit acts of terrorism, mass violence, or targeted violence with little apparent warning creates a unique challenge to traditional law enforcement and investigation methods. We must address and prevent the mass attacks that have too frequently struck our houses of worship, our schools, our workplaces, our festivals, and our shopping spaces. The *Framework* lays out a comprehensive approach to enhancing our prevention capabilities here at home in an age of complex and multidimensional threats, regardless of ideology. Importantly, the framework explicitly recognizes the need to focus on and protect our most vulnerable populations, particularly our youth.

The *Strategic Framework* also introduces a new annual assessment that will examine the state of the threat to the nation. This new assessment will help to inform all levels of government and the broader public about the various threats the Homeland faces each year. Within this report we will analyze the threat of white supremacist violent extremism, one type of racially- and ethnically-motivated violent extremism.

Acts of "Domestic Terrorism" and Targeted Violence

There is no moral ambiguity on this issue. Racially-and ethnically-motivated violent extremism, including violent white supremacy extremism, is one the most potent forces driving acts of domestic terrorism. Lone attackers, as opposed to cells or organizations, generally perpetrate these attacks motivated by this ideology, but they are also part of a broader movement. White supremacist violent extremists, for example, have adopted an increasingly transnational outlook in recent years, largely driven by technological forces. Similar to how ISIS inspired and connected with potential radical Islamist terrorists, white supremacist violent extremists connect with like-minded individuals online.

At the federal level, the FBI and the Department of Justice (DOJ) are the U.S. Government (USG) leads for investigating violent extremism and acts of terrorism and prosecuting related individuals, while DHS informs, equips and trains our homeland security partners to enhance

their prevention and protection capabilities. DHS's primary responsibilities include: (1) Informing, equipping, and training state, local, tribal and territorial governments, civil society, and the private sector to take preventative and protective actions. (2) In conjunction with the FBI, DHS produces joint strategic products identifying trends as well as findings and lessons learned from acts of domestic terrorism.

To this end, in April, we announced the creation of the Office of Targeted Violence and Terrorism Prevention (TVTP) – the primary entity responsible for driving the prevention mission. TVTP is a program office that uses awareness briefings, strategic engagements, technical assistance, information sharing and grants to catalyze the formation and expansion of locally-based prevention efforts. TVTP also looks across the Department to identify complementary efforts that amplify this work by addressing gaps through the creation and deployment of prevention programs that support these state and local efforts. To accomplish this, TVTP works alongside the United States Secret Service's (USSS), National Threat Assessment Center (NTAC), Cybersecurity Infrastructure Security Agency (CISA), and Federal Emergency Management Agency (FEMA) to ensure all of DHS's office and components have the necessary tools to prevent domestic terrorism and targeted violence.

Weapons of Mass Destruction and Health Security

The Department fully concurs with the Director of National Intelligence (DNI) that the weapons of mass destruction (WMD) threat continues to rise. Specific to the Homeland, the period of sustained chemical weapons use on battlefields in the Middle East (Syria and Iraq), coupled with the ever expanding online proliferation of related expertise, could inspire chemical attacks against U.S. interests at home and abroad. These attacks in Syria and Iraq, along with the very public Russian Novichok use in the U.K. and North Korean VX use in Malaysia, have flouted international norms against the use of chemical weapons, raising the risk of more brazen attacks in the future.

Furthermore, the increased diversity in biological and health related threats is concerning. Advances in biotechnology are changing the threat agent landscape, and the decreasing cost and access of dual-use technologies and materials will inevitably expand the threat actor landscape as well.

These issues, coupled with the already complex risks from emerging infectious diseases, and food, agricultural, and veterinary threats, require an elevated integrator and broader all-hazards approach, necessitating organizational change. To this end, in December 2018, the passage of Pub. L. 115-387, the Countering Weapons of Mass Destruction Act of 2018 finalized the creation of DHS's Office of Countering Weapons of Mass Destruction (CWMD) – the primary entity responsible for driving the CWMD planning, detection and protection missions and the Department's health security. We are actively working to overcome the routine challenges of organizational transition as we build out this new office.

The office is also the Department lead on CWMD issues and works with interagency partners including the Assistant Secretary for Preparedness and Response at the Department of Health and Human Services, the National Nuclear Security Agency at the Department of Energy, and Special Operations Command at the Department of Defense to establish policy and operational plans to keep the United States secure from Chemical, Biological, Radiological and Nuclear and other emerging threats.

Cyber Threats and Emerging Technologies

Cyber Threats

DHS, our government partners, and the private sector are all engaging in a strategic and unified approach towards improving our nation's overall defensive posture against malicious cyber activity. In 2018, the Department published the *DHS Cybersecurity Strategy*, outlining a strategic framework to execute our cybersecurity responsibilities during the next five years. The *National Cyber Strategy*, released later that year, reiterates the need to acquire U.S. technology and capture U.S. data, communications, and intelligence property to support its goal of collaboration being the world leader in technology development and strengthens the government's commitment to work in partnership with industry to combat cyber threats and secure our critical infrastructure. Together, the *National Cyber Strategy* and *DHS Cybersecurity Strategy* guide DHS's cybersecurity efforts.

The Coast Guard is the lead Sector-Specific Agency (SSA) for ensuring the safety, security, and environmental protection of the maritime domain against threats in both the physical and the cyber realm. The Coast Guard coordinates closely with the Cybersecurity and Infrastructure Security Agency (CISA) which leads in assisting the Secretary with carrying out his or her responsibilities to coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure, as well as CISA's other authorities to provide for physical and cybersecurity assistance across all critical infrastructure. In responding to maritime cyber incidents, the Coast Guard exercises its authorities under the Maritime Transportation Security Act and its Captain of the Port Authorities under 33 CFR Part 6. As with any other physical or natural incident in the Marine Transportation System, the Coast Guard coordinates its response with other federal, state, and local partners. The Coast Guard also worked with International Maritime Organization Member States to develop a framework for identifying and mitigating cyber risks at foreign ports with a U.S. national security interest. The Coast Guard is growing its capacity and capability to support the maritime sector in preventing cyber incidents and to bring quick and effective resolution when cyber attacks do occur. The Cybersecurity and Infrastructure Security Agency (CISA), operates at the intersection of the Federal Government, state and local governments, the private sector, international partners, law enforcement, intelligence, and defense communities. Division N of Pub. L. 114-113, the Cybersecurity Act of 2015, established DHS as the Federal Government's central hub for the sharing of cyber threat indicators and defensive measures. Additionally, Pub. L. 113-283, the Federal Information Security Modernization Act of 2014, assigns DHS key responsibilities for protecting federal networks. CISA works to enhance information sharing with partners and stakeholders, domestically and internationally, to help critical infrastructure entities and government agencies strengthen their cyber posture.

By bringing together all levels of government, the private sector, international partners, and the public, CISA strengthens the resilience of our Nation's critical infrastructure and enables collective defense against cybersecurity risks. Specifically, CISA is working through the Critical

Infrastructure Partnership Advisory Council (CIPAC) structure to engage with private sector stakeholders, especially the Communications and Information Technology Sector Coordinating Councils and the Enduring Security Framework Operations Working Group to collaborate on the posed by supply chain vulnerabilities and the adoption of 5G technologies. DHS is also leading, in coordination with the IT and Communications Sector Coordination Councils, the ICT Supply Chain Risk Management Task Force with the critical mission of identifying and developing consensus strategies that enhance ICT Supply Chain security. The ICT SCRM Task Force's participants include 20 federal partners, as well as 40 of the largest companies in the Information Technology and Communications sectors.

Cyber threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. Nation-states, cybercriminals, and criminal hackers, are increasing the frequency and sophistication of their malicious cyber activities. In a 2018 report, *Foreign Economic Espionage in Cyberspace*, the U.S.'s National Counterintelligence and Security Center stated, "[w]e anticipate that China, Russia, and Iran will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace." Strategic competitors such as China, Russia, and Iran are developing and using advanced cyber capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democratic institutions.

Increasingly, many or most discussions around cybersecurity threats include some risk calculation around supply chain, third party, or vendor assurance risk. Vulnerabilities in supply chains – either developed intentionally for malicious intent or unintentionally through poor security practices – can enable data and intellectual property theft, loss of confidence in the integrity of the system, or exploitation to cause system and network failure. Increasingly, these vulnerabilities can be viewed as a principal route into our most critical systems and technologies, and we are increasingly concerned with aggressive actions by potential foreign adversaries.

5G Technology

Ultimately, 5G technology may enable significant advances in our society and the prosperity of the United States, but will also usher in an age of significantly greater cyber vulnerability. Advances in 5G technology, the Internet of Things (IoT), and other emerging technologies are driving significant transformation in how we communicate, operate our critical infrastructure, and conduct economic activity. This represents the next generation of networks that will enhance the bandwidth, capacity, and reliability of mobile communications. The United States and South Korea launched 5G on a limited basis at the end of 2018, and more countries are rolling it out this year. According to the Global System for Mobile Alliance (GSMA), 5.1 billion people, or 67 percent of the global population, are subscribed to mobile services. It is expected that 5G networks will cover 2.7 billion people, or 40 percent of the global population, by 2025.

The first generation of wireless telecommunications networks in the United States was deployed in 1982, and its capabilities were limited to basic voice communications. Later generations added capabilities like: text, picture, and multimedia messaging; Global Positioning System (GPS) location; video conferencing; and multi-media streaming. 5G networks will support greater

capacity for tens of billions of sensor and IoT smart devices, and ultra-low latency necessary for highly-reliable, critical communications. According to GSMA, between 2018 and 2025, the number of global IoT connections will triple to 25 billion. Autonomous vehicles, critical manufacturing, medical doctors practicing remote surgery, and a smart electric grid represent only a small fraction of the critical technologies and economic activity that 5G will support. These dramatic advancements in telecommunications and technologies associated with them come with increased risk to the Nation's critical infrastructure.

Risks to mobile communications generally include such activities as call interception and monitoring, user location tracking, cyber actors seeking financial gain through banking fraud, social engineering, ransomware, identity theft, or theft of the device, services, or any sensitive data. Integrating 5G into current wireless networks may convey existing vulnerabilities and impact 5G network security. Capabilities of 5G will allow for exponentially more data transmission across networks. Data on 5G networks will flow through interconnected cellular towers, small cells, and mobile devices and may provide malicious actors additional vectors to intercept, manipulate, or destroy critical data. Due to the nature of 5G network architecture, many more pieces of cellular equipment will be present in the physical world. Deployment of 5G networks will change information sharing as it exists today for public safety officials who critically rely on broadband communications capabilities during a response.

Released in 2018, the *National Cyber Strategy*, also reiterates the need to acquire U.S. technology and capture U.S. data, communications, and intelligence property to support its goal of collaboration being the world leader in technology development and strengthens the government's commitment to work in partnership with industry to combat cyber threats and secure our critical infrastructure. Together, the *National Cyber Strategy* and *DHS Cybersecurity Strategy* guide DHS's cybersecurity efforts to prioritize the development of secure and reliable advanced information technology risks posed by supply chain vulnerabilities and the adoption of 5G technologies. To manage and address the risks posed by 5G, the U.S. government is taking an interagency approach, led by the White House. National Security Council (NSC) Cybersecurity Directorate and the National Economic Council co-lead a regular 5G interagency Policy Coordination Committee (PCC) through the National Security Presidential Memoranda (NSPM) - 4 process. DHS participates in these meetings and they provide an excellent opportunity to discuss and come to decisions on key 5G issues.

Unmanned Aircraft Systems

Criminal entities and terrorist organizations continue to promote and use unmanned aircraft systems (UAS) for illicit activity in order to support surveillance, smuggling, and harassment and, at times, use as weapons. The UAS threat to critical infrastructure and security activities will likely increase soon as the number of UAS introduced into the national airspace continues to increase, and the use of technical means to detect, track, and disrupt malicious UAS operations will likely remain limited. In order to combat the rising threat of UAS, DHS conducts counter aircraft system (CUAS) operations authorized by law, to disrupt malicious use of UAS at facilities or DHS supported activities within the United States, and as designated by the Secretary of DHS.

Supporting Election Security

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

To date, because of our holistic USG wide response to this threat, there is no evidence that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political or campaign infrastructure used in the 2018 midterm elections for the United States Congress. We must be uniform and clear in our communication of this fact to the American Public.

We must make the important distinction between malign foreign attempts to influence U.S. public opinion and actual incidents/attacks on activities targeting/against our election infrastructure. While we see many examples of the first each every day – Russia and other foreign countries, including China and Iran, conduct malign influence activities and messaging campaigns targeting the United States to advance their strategic interests – there is no evidence of successful exploitation of our election or political campaign infrastructure. We must combat both election infrastructure threats and malign foreign influence campaigns holistically as a U.S. government and U.S. society, building resistance and resilience to attempts by foreign nation-state adversaries to pull at the seams of our diverse social fabric and sow discord in our political process.

DHS is holistically dedicated to the security of our electoral process as it is a vital national interest. We regularly coordinate with the Intelligence Community and law enforcement partners, as well as relevant private sector entities, to assess the scale and scope of malicious cyber activity potentially targeting the U.S. election infrastructure. It is our goal to ensure the American people enter the voting booth with the confidence that their vote counts and is counted correctly.

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

CISA, in coordination with our interagency partners, is also helping Americans recognize and avoid foreign disinformation operations impacting our elections through innovative efforts like the #WarOnPineapple campaign. The #WarOnPineapple is aimed at educating Americans on the use of malign foreign influence campaign tactics by highlighting a topic that citizens can easily relate to: the divisiveness of pineapples on pizza. Through this work, CISA is helping Americans recognize and avoid foreign disinformation operations impacting homeland security, including our elections.

Counterintelligence

The foreign intelligence threat faced by DHS in today's global environment has quickly evolved into one of the most significant threats to our country in decades. Although the leading state intelligence threats to U.S. interests will likely continue to be China, Russia, Iran and North Korea—based on their capabilities, intent, and broad operational scope, other Foreign Intelligence Entities (FIE) in Latin America, South Asia, the Middle East, and East Asia pose local and regional intelligence threats to U.S. interests which cannot be ignored. Additionally, non-state actors, including international terrorist organizations, transnational criminal organizations (TCOs), drug trafficking organizations (DTOs), and foreign cyber actors will likely continue to employ and improve their intelligence collection capabilities using human, technical, and cyber means in efforts to obtain and exploit sensitive DHS information and national security programs.

As China's intelligence services continue to grow, they utilize and imbed into America's academic and scientific communities and pose a significant risk to economic and national security through technology transfer via foreign direct investment, venture capital investments, joint ventures, licensing agreements, cyber espionage, traditional espionage, and Talent Programs. The Chinese Government's Talent Programs are aimed at targeting and recruiting overseas Chinese and foreign experts, among them academics and business entrepreneurs, in strategic sectors to teach and work in China. Through its various Talent Programs, China has targeted foreign experts in the United States in order to acquire technology and know-how that is directly aligned with China's Five-Year Plans, science and technology, economic, and military modernization efforts. U.S. academic institutions are at particularly risk of exploitation due to their openness and collaborative research approaches.

Chinese citizens who come to the United States to study or teach at U.S. academic institutions also present a significant risk of technology transfer. While they competitively develop their science and technology workforce, we must continue to lead and out-produce China in this area. The most immediate threats have far reaching and enduring implications to U.S. national security: influence operations, critical infrastructure, supply chain, as well as traditional and economic espionage. Developing technologies and artificial intelligence (AI) systems will influence the way we engage in national security in the future. It is essential that we lead the global AI race to ensure that we are ready for national security threats of the future.

Illegal Cross-Border Movements of People and Goods: Illegal Immigration, Human Trafficking, Human Smuggling, and the Global Illicit Drug Trade

Illegal Immigration

This year, our nation has experienced an unprecedented and unsustainable humanitarian and national security crisis at the Southwest Border. This crisis has presented unique challenges that our Department has never seen. Nevertheless, this Administration has taken extraordinary and successful steps to secure our borders and restore integrity to our immigration system.

As you all know, the scale of illegal immigration encountered by DHS this year, including the number of families and children crossing the border, has been unparalleled in recent history. The

increased shift to more families and children and the overwhelming numbers profoundly affect our ability to patrol the border, ensure strong interior enforcement, and diminishes our ability to prevent deadly illicit drugs and dangerous people from entering our country. It also detracts from our ability to facilitate lawful trade and travel.

Every day, DHS employees from CBP and ICE work to reduce the illegal crossings into our country. CBP focuses primarily on enforcing U.S. immigration laws at and between the ports of entry while ICE is charged with enforcing immigration laws in the interior of the country. DHS is receiving international cooperation. Mexico and our Central American partners are also stepping up to help stop the flow of illegal migrants. Further, with the help of the U.S. military, CBP is on track to build 450-500 new miles of border wall by the end of 2020.

In the case of the foreign terrorist threat, border security is a zero-sum challenge. Similarly, with an ongoing opioid epidemic in our country that has led to staggering numbers of casualties through overdose and violence, each drug shipment that illegally crosses our border is, in effect, responsible for the loss of American lives. Consequently, the challenge of illegal immigration – which diverts our resources along the border from our critical counterterrorism and counter narcotics missions – represents a critical national security concern.

We must continue to recognize the zero-sum nature of border security and address the significant increases in mass migration. This involves not just building the border wall that will conserve overstretched law enforcement resources, but also fixing our immigration laws that serve as “pull factors” for illegal immigration and working with our foreign partners to alleviate the “push factors” in Latin American countries, particularly within El Salvador, Guatemala, and Honduras, that cause mass departures in the first place.

Global Illicit Drug Trade

The United States is in the midst of an opioid epidemic that is being fueled by the smuggling and trafficking of heroin, illicit fentanyl, fentanyl analogues, and other synthetic opioids. Based on investigative efforts, United States law enforcement has identified China and Mexico as primary sources of the U.S. illicit fentanyl threat.

Due to President Trump’s engagement with Chinese President Xi, China added fentanyl to the country’s list of controlled substances, effective May 1st, 2019. Chinese fentanyl being shipped directly to the United States decreased significantly. Illicit fentanyl, fentanyl analogues, and their immediate precursors are most often produced in China. From China, these substances are shipped primarily through international mail or express consignment carriers (such as DHL, FedEx, or UPS) directly to the United States or, alternatively, shipped directly to transnational criminal organizations (TCOs) in Mexico.

Since May 1, 2019 it appears opioid traffickers have started altering their methods by either trafficking non-fentanyl opioids such as U-48800 to the United States as it is not scheduled in China, which is illegally shipped directly to the United States through the international mail or consignment carriers. Criminals and criminal organizations are also sending pre-precursor chemicals such as 4-AP to Mexico where Mexican cartels are synthesizing their own fentanyl from these chemicals. While the direct shipment of Chinese fentanyl to the United States has dramatically dropped, China is still ultimately responsible for most of the fentanyl reaching the

United States due to its supply of pre-precursors to transnational criminal organizations in Mexico.

Once in the Western Hemisphere, fentanyl or fentanyl analogues are prepared and mixed with other narcotics and fillers and/or pressed into pill form, and then moved to the illicit U.S. market where demand for prescription opioids and heroin remain at epidemic levels. In some cases, regional distributors smuggle industrial pill presses and components into the United States to operate illicit fentanyl tableting operations domestically.

Mexican cartels have seized upon the profit potential of illicit synthetic opioids and intend to grow their share of this illicit market. Given its low cost coupled with high potency, one kilogram of fentanyl can generate almost \$10 million in revenue on the illicit market. We are now seeing instances in which precursors originating in China and smuggled into the United States have traveled through the United States, destined for the U.S. southwest border locations. The Mexican cartels have then smuggled the precursors out of the country, synthesized them into illicit fentanyl, and imported the finished product back into the United States for distribution and consumption. The final product may be advertised as heroin, and the end user may not be aware of the presence of fentanyl.

Migrant Smuggling and Human Trafficking

Alongside illegal immigration and human smuggling, human trafficking continues to pose a humanitarian and law enforcement challenge. Migrant smuggling and human trafficking are often used interchangeably in error when they are two distinct crimes. Migrant smuggling is a crime committed against the sovereignty of a state, while human trafficking is a crime of exploitation against an individual. Migrant smuggling involves the provision of a service—typically, transportation or fraudulent documents—to an individual who voluntarily seeks to enter a foreign country illegally. Human trafficking on the other hand, is a crime compelling an individual to perform forced labor or a commercial sex act through force, fraud, or coercion; or compelling a minor to perform a commercial sex act, regardless of force, fraud or coercion. Immigration status or country of citizenship is not an element of human trafficking, nor is movement across an international border. Human trafficking is also an underreported crime because victims rarely come forward to seek help. This may be because they are unable to do so or because their vulnerabilities are being exploited, preventing them from seeking assistance. Proper identification, assistance, and protection of victims is essential to successfully combating this crime.

Transnational Crime Organizations

Based on the collection of intelligence and investigatory evidence from USCG, CBP and ICE, we observe that human smuggling enterprises and the drug cartels maintain a symbiotic relationship. Certain members of these criminal enterprises control the major United States and foreign illicit drug markets, and others control the “smuggling flow,” otherwise known as the “illicit pathways.” It is critical to both our values as a nation and the long-term stability of our Western Hemisphere – including the health and prosperity of our Latin American partners – that we work to disrupt these smuggling and trafficking organizations, protect the vulnerable populations they exploit, and help to build and strengthen our foreign partners’ domestic institutions and societies to protect their citizenries.

As we all know, cartels and other transnational organized crime (TOC) networks serve as organizing forces behind the illicit mass migration and migrant smuggling and human trafficking I discussed just a moment ago. These TOC networks threaten the homeland, support hostile foreign powers, and drive regional instability, crime, corruption, and violence. TOC networks maintain a diverse portfolio of crimes, including fraud, human trafficking, kidnapping, and extortion. They are also heavily involved in human, weapon, bulk cash, and drug smuggling through their sophisticated criminal networks.

TOC networks are motivated by money and power and have little regard for human life. These networks are commodity agnostic—a human being is moved along with no more care than a gun or a bundle of drugs. When desperate aliens enter these networks, they may find themselves beaten, assaulted, raped, and even killed by network members.

TOC networks continually adjust their operations to avoid detection and interdiction by law enforcement, and—like legitimate businesses—are quick to take advantage of improved technology, cheaper transportation, and better distribution methods.

DHS uses a multi-layered threat-based strategy—conducts overseas operations and capacity building, at-sea interdictions, border interdictions, and interior enforcement activities—to leverage its unique criminal, civil, military, and administrative authorities to achieve mission objectives and counter TOC.

Conclusion

Every day, the 240,000 men and women of the Department of Homeland Security work to ensure the safety and security of all Americans and are dedicated to building a brighter future. They deserve our support and thanks.

I want to thank you, Chairman Johnson, Ranking Member Peters, distinguished Members, and staff for the support you have shown the Department and the work undertaken by this Committee to ensure DHS has the tools it needs to adapt to the changing threat environment.

I look forward to your questions.



Department of Justice

STATEMENT OF

**CHRISTOPHER WRAY DIRECTOR
FEDERAL BUREAU OF INVESTIGATION**

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

**AT A HEARING ENTITLED
“THREATS TO THE HOMELAND”**

**PRESENTED
NOVEMBER 5, 2019**

STATEMENT OF
CHRISTOPHER WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

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

AT A HEARING ENTITLED
“THREATS TO THE HOMELAND”

PRESENTED
NOVEMBER 5, 2019

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. Our nation continues to face a multitude of serious and evolving threats ranging from homegrown violent extremists (“HVEs”) to cyber criminals to hostile foreign intelligence services and operatives. Keeping pace with these threats is a significant challenge for the FBI. Our adversaries — terrorists, foreign intelligence services, and criminals — take advantage of modern technology to hide their communications; recruit followers; and plan, conduct and encourage espionage, cyber attacks, or terrorism to disperse information on different methods to attack the U.S. homeland, and to facilitate other illegal activities.

Just as our adversaries evolve, so, too, must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our national security, our economy, and indeed our communities. These diverse threats underscore the complexity and breadth of the FBI’s mission: to protect the American people and uphold the Constitution of the United States.

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 most persistent threats to the Nation and to U.S. interests abroad are homegrown violent extremists (“HVEs”), domestic violent extremists, and foreign terrorist organizations (“FTOs”). The IT 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. We remain concerned that groups such as the Islamic State of Iraq and ash-Sham (“ISIS”) and al Qaeda have the intent to carry out large-scale attacks in the U.S.

The FBI assesses HVEs are the greatest, most immediate 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, and the use of encrypted communications.

In recent years, prolific use of social media by FTOs has greatly enhanced their ability to disseminate messages. We have also been confronting a surge in terrorist propaganda and training available via the Internet and social media. Due to online recruitment, indoctrination, and instruction, FTOs are no longer dependent on finding ways to get terrorist operatives into the United States to recruit and carry out acts of terrorism. 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. They motivate these individuals to act at home or encourage them to travel. This is a significant transformation from the terrorist threat our nation faced a decade ago.

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 enter 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 for lone offender attacks in Western countries. Recent ISIS videos and propaganda have specifically advocated for attacks against soldiers, law enforcement, and intelligence community personnel.

Many foreign terrorist organizations 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. 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.

The threats posed by foreign fighters, including those recruited from the U.S., are very dynamic. We will continue working to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIS, those foreign fighters who may attempt to return to the United States, and HVEs who may aspire to attack the United States from within.

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.

In addition to FTOs, domestic violent extremists collectively pose a steady 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, and reactions to legislative actions — remain constant. 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 domestic violent extremists than international terrorists in recent years.

The recent attacks in Texas and California underscore the continued threat posed by domestic violent extremists and perpetrators of hate crimes. Such crimes are not limited to the United States and, with the aid of Internet like-minded hate groups, can reach across borders. To combat the threat at home, the FBI established the Domestic Terrorism-Hate Crimes Fusion Cell, in spring 2019. Composed of subject matter experts from both the Criminal Investigative and Counterterrorism Divisions, the fusion cell offers program coordination from FBI Headquarters, helps ensure seamless information sharing across divisions, and augments investigative resources.

As the threat to harm 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, 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 foreign terrorist organizations and homegrown violent extremists. 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.

Counterintelligence

The Nation faces a continuing threat, both traditional and asymmetric, from hostile foreign intelligence agencies. Traditional espionage, often characterized by career foreign intelligence officers acting as diplomats or ordinary citizens, and asymmetric espionage, typically carried out by students, researchers, or businesspeople operating front companies, is prevalent. Foreign intelligence services not only seek our nation's state and military secrets, but

they also target commercial trade secrets, research and development, and intellectual property, as well as insider information from the Federal Government, U.S. corporations, and American universities. Foreign intelligence services continue to employ more creative and more sophisticated methods to steal innovative technology, critical research and development data, and intellectual property, in an effort to erode America's economic leading edge. These illicit activities pose a significant threat to national security and continue to be a priority and focus of the FBI.

Foreign influence operations — which may include covert actions by foreign governments to influence U.S. policy decisions, political sentiment or public discourse — are not a new problem. But the interconnectedness of the modern world, combined with the anonymity of the Internet, have changed the nature of the threat and how the FBI and its partners must address it. The goal of these foreign influence operations directed against the United States is to spread disinformation, sow discord, push foreign nations' policy agendas, and ultimately undermine confidence in our democratic institutions and values. Foreign influence operations have taken many forms and used many tactics over the years. Most widely reported these days are attempts by adversaries—hoping to reach a wide swath of Americans covertly from outside the United States — to use false personas and fabricated stories on social media platforms to discredit U.S. individuals and institutions. However, other influence operations may include targeting U.S. officials and other U.S. persons through traditional intelligence tradecraft; criminal efforts to suppress voting and provide illegal campaign financing; concealing efforts to influence U.S. government activities, cyber attacks against voting infrastructure, along with computer intrusions targeting elected officials and others; and a whole slew of other kinds of influence, like both overtly and covertly manipulating news stories, spreading disinformation, leveraging economic resources, and escalating divisive issues.

Almost two years ago, I established the Foreign Influence Task Force (“FITF”) to identify and counteract malign foreign influence operations targeting the United States. The FITF is uniquely positioned to combat this threat. The task force now brings together the FBI's expertise across the waterfront — counterintelligence, cyber, criminal, and even counterterrorism — to root out and respond to foreign influence operations. Task force personnel work closely with other U.S. government agencies and international partners concerned about foreign influence efforts aimed at their countries, using three key pillars.

Currently there are open investigations with a foreign influence nexus spanning FBI field offices across the country. Second, we are focused on information and intelligence-sharing. The FBI is working closely with partners in the Intelligence Community and in the federal government, as well as with State and local partners, to establish a common operating picture. The FITF is also working with international partners to exchange intelligence and strategies for combating what is a shared threat. The third pillar of our approach is based on strong relationships with the private sector. Technology companies have a front-line responsibility to secure their own networks, products, and platforms. But the FBI is doing its part by providing actionable intelligence to better enable the private sector to address abuse of their platforms by foreign actors. Over the last year, the FBI has met with top social media and technology

companies several times, provided them with classified briefings, and shared specific threat indicators and account information, so they can better monitor their own platforms.

But this is not just an election-cycle threat. Our adversaries are continuously trying to undermine our country, whether it is election season or not. As a result, the FBI must remain vigilant.

In addition to the threat posed by foreign influence, the FBI is also concerned about foreign investment by hostile nation states. Over the course of the last seven years, foreign investment in the U.S. has more than doubled. Concurrent with this growth, foreign direct investment (“FDI”) in the U.S. has increasingly become a national security concern, as hostile nations leverage FDI to buy U.S. assets that will advance their intelligence, military, technology, and economic goals at the expense of U.S. national security. The Committee on Foreign Investment in the U.S. (“CFIUS”), an Executive Branch committee chaired by the Department of Treasury, was statutorily created to address potential risks to U.S. national security resulting from foreign acquisitions or mergers with U.S. companies. As part of this process, the FBI provides input and analysis to the National Intelligence Council within eight days of a CFIUS filing and a risk assessment to the Department of Justice within 30 days of a CFIUS filing. As a result of the Foreign Investment Risk Review Modernization Act (“FIRRMA”), which was enacted last year, the FBI anticipates its workload to increase dramatically.

Cyber Threats

Virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated. We face threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. On a daily basis, these actors seek to steal our state secrets, our trade secrets, our technology, and the most intimate data about our citizens — things of incredible value to all of us and of great importance to the conduct of our government business and our national security. They seek to hold our critical infrastructure at risk, to harm our economy and to constrain our free speech.

As the Committee is well aware, the frequency and severity of malicious cyber activity on our Nation’s private sector and government networks have increased dramatically in the past decade when measured by the amount of corporate data stolen or deleted, the volume of personally identifiable information compromised, or the remediation costs incurred by U.S. victims. We expect this trend to continue. Within the FBI, we are focused on the most dangerous malicious cyber activity: high-level intrusions by state-sponsored hackers, global organized crime syndicates, and other technically sophisticated and dangerous actors. FBI agents, analysts, and computer scientists are using technical capabilities and traditional investigative techniques — such as sources, court-authorized electronic surveillance, physical surveillance, and forensics — to counter these threats. We continue to actively coordinate with our private and public partners to pierce the veil of anonymity surrounding cyber based crimes.

Botnets used by cyber criminals have been responsible for billions of dollars in damages over the past several years. The widespread availability of malicious software (malware) that can create botnets allows individuals to leverage the combined bandwidth of thousands, if not millions, of compromised computers, servers, or network-ready devices to disrupt the day-to-day activities of governments, businesses, and individual Americans. Cyber threat actors have also increasingly conducted ransomware attacks against U.S. systems, encrypting data and rendering systems unusable — thereby victimizing individuals, businesses, and even emergency service and public health providers.

Cyber threats are not only increasing in size and scope, but are also becoming increasingly difficult and resource-intensive to investigate. Cyber criminals often operate through online forums, selling illicit goods and services, including tools that lower the barrier to entry for aspiring criminals and that can be used to facilitate malicious cyber activity. These criminals have also increased the sophistication of their schemes, which are more difficult to detect and more resilient to disruption than ever. In addition, whether located at home or abroad, many cyber actors are obfuscating their identities and obscuring their activity by using combinations of leased and compromised infrastructure in domestic and foreign jurisdictions. Such tactics make coordination with all of our partners, including international law enforcement partners, essential.

The FBI is engaged in a myriad of efforts to combat cyber threats, from improving threat identification and information sharing inside and outside of the government to developing and retaining new talent, to examining the way we operate to disrupt and defeat these threats. We take all potential threats to public and private sector systems seriously and will continue to investigate and hold accountable those who pose a threat in cyberspace.

Conclusion

In closing, the work being done by the FBI is immeasurable; however, we cannot afford to be complacent. We must seek out new technologies and solutions for the problems that exist today as well as those that are on the horizon. We must build toward the future so that we are prepared to deal with the threats we will face at home and abroad and understand how those threats may be connected.

Chairman Johnson, Ranking Member Peters, and members of the Committee, thank you again for this opportunity to discuss the FBI's efforts to combat the myriad of threats it faces. I appreciate your continued support and look forward to answering any questions you might have.

UNCLASSIFIED

**Hearing before the Senate Committee on
Homeland Security and Governmental Affairs**

“Threats to the Homeland”

**Mr. Russell Travers
Acting Director, National Counterterrorism Center
Office of the Director of National Intelligence**

November 5, 2019

Chairman Johnson, Ranking Member Peters, and members of the committee, thank you for the opportunity to be with you today. I will begin with a brief overview of the terrorism threat before discussing related threats to the homeland in more detail. I will close my opening remarks with a discussion of global trends impacting counterterrorism efforts, along with comments on the way forward, from NCTC’s perspective.

Terrorism Threat Overview

The US and its allies continue to pursue an aggressive global campaign against a complex array of terrorist actors. Operating across Africa, Asia, and the Middle East, US and partner forces have killed or captured thousands of terrorist leaders and operatives since September 11, 2001, exemplified most recently with the heroic removal of the brutal ISIS in Iraq and Syria leader, Abu Bakr al-Baghdadi, on October 26th. These removals degrade the ability of terrorists to organize, communicate, and strike the US. Working unilaterally or with partner-nations, the US has disrupted numerous attack plots, saving the lives of countless potential victims. At home, federal, state, and local intelligence and law enforcement agencies—working in close cooperation—continue to counter terrorist activity. Enhanced border security efforts have constrained groups’ ability to infiltrate the US, and we now assess the most predominant terrorist threat to the Homeland to emanate from US-based lone actors. Additionally, the US government and private sector allies have made significant strides curtailing terrorists’ online presence.

While these efforts have diminished the terrorist threat to the US, we have enjoyed less success staunching terrorist growth overseas. When I testified before this committee over a year ago, I warned that the terrorist threat was becoming more diverse, dispersed, and unpredictable; unfortunately, these trends have only continued, posing an increasingly complex challenge for the US and its allies. In several regions, we

UNCLASSIFIED

UNCLASSIFIED

continue to observe the expansion or revival of familiar threats, as well as the emergence of new ones.

- First, the overall threat from radical Islamist terrorists has not abated and, in some regions, is growing. Prominent groups including ISIS and al-Qa'ida are expanding into new areas and reinforcing their networks' cohesion, bolstering the overall movement's reach, resiliency, and threat to US interests.
- At the same time, the US is confronting an aggressive Iran and its network of terrorist proxies, who are employing violence to undermine US pressure and influence throughout the Middle East. Tehran, including the Islamic Revolutionary Guard Corps-Quds Force (IRGC-QF), and its formidable allies like Lebanese Hizballah are strengthening their relationships with a wide array of militants and exporting advanced tactics and weaponry – capabilities that can be turned against US personnel with little warning.
- Finally, high profile attacks in the United States and abroad—most notably the March attacks against mosques in Christchurch, New Zealand and the August attack in El Paso, TX —highlight that the US is facing threats from a broader range of terrorist actors, to include violent extremists motivated by racial and ethnic hatred. While primarily a lone actor threat, these violent extremists in the US and abroad are deftly using technology to recruit others to their extreme ideology.

Several broader global trends are adding to the complexity of the terrorist threat landscape including the availability of disruptive technologies, enduring conflicts and instability, the drift of focus and resources away from CT, and the rising global influence of US competitors. These concurrent and interrelated dynamics are increasingly affecting—at times negatively—our ability to mobilize or sustain effective pressure against terrorists. In this environment, staying ahead of terrorist adaptation requires an increasingly nimble US response that better leverages foreign allies, private sector partners, and whole-of-government resources.

The Terrorist Threat to the Homeland

Throughout 2019, persistent US and allied CT pressure against key al-Qa'ida and ISIS leaders and operatives have continued to degrade these groups' ability to launch terrorist attacks against the US. Radical Islamist terrorists' external plotting capabilities

UNCLASSIFIED

UNCLASSIFIED

may have been further hampered by the demands of sustaining large-scale insurgent campaigns, combatting capable local US allies, or fighting other militant competitors.

Despite our successes, leaders of both al-Qa'ida and ISIS retain the intent to strike the US and have proven resourceful in finding ways to evade US defenses. I would refer to the example of al-Qa'ida in the Arabian Peninsula (AQAP) which, while fighting an insurgency in Yemen, nevertheless attempted three external operations against US aviation between 2009 and 2012 using novel explosive designs. Currently, al-Qa'ida, ISIS, and several of their local affiliates and branches retain key competencies and resources—including explosives expertise and foreign operatives—that could support attacks in the US or the West. Further declines in CT pressure could enable them to quickly reinvigorate or expand external plotting. This could include additional attacks against aviation, which remains of great interest to terrorists because of the potential economic and psychological impacts.

As we sustain pressure against radical Islamist terrorists' external operations capabilities, we will likely continue to face a more persistent threat from US-based homegrown violent extremists, which we assess represent the preeminent Sunni terrorist threat to the US. While there has only been one such attack in the US this year, it remains a serious threat and poses an enduring detection challenge because of these attackers' lack of direct connections to known violent extremists or terrorist groups, their use of easy-to-acquire weapons and tactics and tendency to operate alone or in small groups. In addition, radical Islamist terrorist groups overseas continue to promote lone actor attacks through their media outlets, viewing them as an efficient tactic to terrorize the US and other opponents.

The threat from terrorists motivated by ideologies unconnected to radical Islamist terrorism are also a concern. Since the beginning of 2018, these terrorists have conducted the vast majority of lethal homeland terrorist attacks. Most of these attacks were perpetrated by lone actors adhering to a racially or ethnically motivated violent extremist ideology who have been radicalized, in part online, and motivated by a range of grievances associated with political and/or social agendas. While most of these actors have used readily available firearms and edged weapons against soft targets, 2019 has been the most lethal year for these attacks since 1995.

Finally, Iran and Hizballah's ongoing efforts to expand their already robust global networks also threaten the homeland. The arrests last year of Iranian operatives and diplomats in the US and Europe linked to attack plotting underscore Tehran's determination to use violence against its adversaries around the world, potentially including within the US. Additionally, the arrest in July of a Hizballah-trained operative in

UNCLASSIFIED

UNCLASSIFIED

New Jersey who conducted surveillance of US landmarks on behalf of the group is emblematic of the reach of its sophisticated global network, which has been active in Europe, South America, and Africa.

The Terrorist Threat Overseas

While our CT campaign has diminished terrorists' external attack capabilities, our efforts to curtail radical Islamist terrorist growth and the threat to US interests overseas have proven less successful. Radical Islamist terrorist groups are now operating in more countries around the world than ever before, threatening a widening circle of US interests and allies.

I will begin with ISIS in Iraq and Syria, where US and coalition efforts have eliminated the physical caliphate and removed the group's long-time leader, Abu Bakr al-Baghdadi, demoralizing ISIS fighters and demonstrating the persistence of US and coalition forces to eliminate terrorist threats wherever they are. However, the terrorism threat persists as ISIS has successfully transitioned to a clandestine insurgency consisting of thousands of committed operatives across the two countries. ISIS cells continue to conduct a diminished but steady rate of IED attacks, raids, and ambushes against local security forces and other opponents. ISIS fighters are attempting to evade local counterterrorism pressure by using safehavens in rural, under-governed areas of northern and western Iraq and eastern Syria. Senior leaders have publically encouraged adherents to be patient and persevere, pointing to the group's previous successes rebounding from setbacks.

In an effort to enable its revival and attract new recruits, the group continues to stoke and exploit Sunni fears of sectarian violence and economic and political marginalization while targeting populations vulnerable to ISIS's appeals, including refugees. ISIS leaders since at least mid-September have also prioritized the freeing of thousands of detained members in prison and IDP camps across Iraq and Syria. The release and reintegration of these veteran operatives would greatly augment the group's operations, mirroring the dynamic we saw play out in 2013. Finally, ISIS leaders will likely move to exploit the recent instability and the attrition and cooption of CT forces in northeastern Syria to reinvigorate their insurgent and external operations efforts.

Outside of Iraq and Syria, ISIS's global network remains robust and—in some areas—is expanding, thanks to its approximately 20 global branches and networks. This year, the group publically announced new branches in Mozambique, Pakistan, and Turkey, underscoring leaders' determination to sustain their global reach amidst setbacks in Iraq and Syria. The capabilities of these branches and networks vary, but ISIS groups in

UNCLASSIFIED

UNCLASSIFIED

Afghanistan, the Philippines, the Sinai Peninsula, and West Africa have the capacity to conduct sophisticated attacks against local security forces and target US interests and personnel. Even networks lacking direct connection to ISIS core can be deadly—the attacks in April in Sri Lanka that killed over 290 people—including four Americans—serves as a salient reminder of ISIS’s reach and threat to US citizens. Additionally, the far-flung ISIS enterprise retains a degree of cohesion: ISIS this year launched several synchronized attack and propaganda campaigns in which numerous branches and networks participated, which is an indicator of enhanced connectivity.

Meanwhile, al-Qa’ida and its affiliates continue to target US interests, expand their regional insurgencies, and strengthen their connectivity. Senior leaders, including several based in Iran, oversee these global efforts, sustaining the network’s cohesion. In September, group leader Ayman al-Zawahiri praised the 9-11 attacks, reiterated his call for attacks against US and Israeli targets, and urged extremists to travel to radical Islamist terrorist battlefields, highlighting al-Qa’ida’s multi-pronged strategy. In addition, group leaders’ announcement in January of a “Jerusalem Will Never Be Jewish” campaign in response to the move of the US embassy to Jerusalem underscores their interest in executing transnational campaigns. Two attacks in Kenya and Mali, conducted by al-Shabaab and the al-Qa’ida-aligned, West Africa-based Jama’at Nusrat al-Islam wal-Muslimin (JNIM), have since been included under this campaign.

Al-Qa’ida’s regional insurgencies continue to achieve varying levels of success. In Somalia, al-Shabaab has ramped up its campaign against African Union forces, the local government, and US and Western personnel. In September, the group launched a large-scale assault on a base in Baledogle that houses US military personnel. In Mali and other parts of West Africa, JNIM and allied fighters have ramped up their attacks against international peacekeepers and local security forces, exacerbating instability and humanitarian conditions. In North Africa, local CT operations in Libya and Tunisia have probably stunted the growth of al-Qa’ida in the Lands of the Islamic Maghreb (AQIM), but the group continues to pose a threat to government and Western targets throughout the region.

In Yemen, AQAP has sustained its insurgent campaign and may expand their efforts as continuing political instability threatens to diminish CT pressure against the group. In Syria, Hurras al-Din—an al-Qa’ida aligned group consisting of veteran extremists—is working to advance the group’s global agenda, although the deaths of at least one senior operative and the tenuous status of its safehaven in northwest Syria could impede their efforts. In Afghanistan, the death in September of the leader of al-Qa’ida in the Indian Subcontinent (AQIS) may disrupt their regional operations. Finally, al-Qa’ida

UNCLASSIFIED

UNCLASSIFIED

retains its long-standing ties to the Haqqani Network and other militant networks active in Afghanistan and Pakistan that frequently target US personnel.

In Iran, the regime continues to use terrorism to threaten the United States, our allies, and other opponents, as well as to cement its long-term political influence throughout the Middle East. As we have observed in recent months from Tehran's attacks on international shipping and Saudi oil facilities, the regime is intent on escalating its efforts to intimidate and impose costs on its opponents, posing a growing direct and indirect threat to US interests and personnel. Iran, through the IRGC-QF and other malign elements like the Ministry of Intelligence and Security (MOIS) maintains links to terrorist operatives and networks in Europe, Asia, and Africa that could be called upon to target US or allied personnel.

Iran can also call upon a wide-range of proxy groups to support its terrorist and regional influence operations. Tehran is poised to use these entities to target US personnel in the event that the regime is threatened. Iranian leaders also nurture these alliances in pursuit of long-term political advantage, similar to its decades-long partnership with Hizballah, which wields significant political influence within Lebanon and possesses a formidable military force including thousands of rockets. In Iraq, Iran has provided weapons and funding to a wide-variety of powerful militia groups, whose influence and advanced terrorist capabilities threaten the US presence there. Iran is also supporting Huthi forces in Yemen, whose increasingly bold attacks against Saudi Arabia could indirectly endanger US personnel. Finally, Iran maintains ties to several Palestinian military groups including Palestine Islamic Jihad, which has killed numerous civilians in Israel.

Global Trends Increasingly Impacting the CT Fight

Our ability to combat the diverse range of terrorist threats continues to be influenced, at times negatively, by broader military and political trends. Navigating these challenges will likely require leveraging a broad range of government resources and capabilities across the interagency, given their scope and scale.

- **Emerging technologies.** Terrorists continue to exploit rapid technological advances in fields like encrypted communications, social media, and unmanned aircraft systems (UAS). The speed at which industry responds to consumer demands for newer, more capable technologies also fuels terrorist innovation and, at times, limits our ability to disrupt their operations. Specifically, terrorists are continuing to explore the use of increasingly ubiquitous, more secure modes of communications in order to evade detection. While the amount of terrorist

UNCLASSIFIED

UNCLASSIFIED

content on mainstream platforms like Facebook has been curtailed, terrorists have responded by using less-accessible platforms to communicate and disseminate propaganda. Finally, commercially available unmanned systems—like aircraft (UAS) and surface vehicles (USV)—are enabling some groups to conduct tactical surveillance, smuggling operations, and attacks against key critical infrastructure targets like oil refineries or airports that can result in significant economic damage.

- **Conflict and Instability.** Enduring conflicts in several countries including Egypt, Mali, Nigeria, Libya, Syria, and Yemen continue to serve as incubators for terrorist presence. The intractable nature of these conflicts, their spillover into neighboring countries, and the long-term impacts on humanitarian conditions continue to provide terrorist groups with new opportunities to carve out safehavens, bolster operations, derive resources, and recruit the next generation of fighters. As an example, several ongoing conflicts and insurgencies across Africa have enabled terrorists aligned with al-Qa'ida and ISIS to expand their influence and embed with local militant groups, fueling an unprecedented rate of jihadist growth across the continent.
- **Partner Complacency and Distraction.** Some partners' perception that the terrorist threat has been sufficiently reduced or eclipsed by other political or security concerns may increasingly prompt them to allocate resources away from CT efforts, potentially diminishing pressure on some networks.
- **Influence by Strategic Competitors.** The growing influence and footprint of US competitors—particularly China and Russia—in key CT theaters could constrain our ability to mobilize and direct local CT operations. Both Beijing and Moscow have increased their security, military, and CT assistance programs as part of their campaign to undermine and supplant US influence in parts of Africa, Asia, and the Middle East – regions that also host preeminent terrorist groups. In addition, our competitors often promote punitive and anti-democratic CT strategies that could fuel further radicalization to violence.

The Way Forward

These challenges require a nimble, aggressive US response that makes greater use of foreign partners and resources resident in both the interagency and private industry. An over-reliance on “business as usual” practices or kinetic efforts will increase the risks of

UNCLASSIFIED

UNCLASSIFIED

being outpaced by our terrorist adversaries and marginalized by our competitors, particularly as competing demands on US national security resources mount.

- **Bolstering Foreign Allies.** As the scale of the global terrorism challenge grows, foreign partners will play an increasingly central role in fighting it. Sustained US leadership, advisory, and capacity building efforts in both the military and non-military areas remain instrumental in ensuring that partners implement effective, comprehensive, and balanced CT measures, sufficiently resource them, and cooperate with neighbors and other allies. As noted in the 2018 National Strategy for Counterterrorism, proactively identifying and focusing on those allies that are best positioned and able to advance US CT efforts will prove key in countering the terrorist threat; this includes working with allies and partners on preventing and countering terrorist radicalization and recruitment in the first place – through not only strategic communications but community engagement and other “countering violent extremism” approaches.
- **Mobilizing Tech Sector Partners.** As noted previously, terrorist actors continue to move aggressively to exploit new technologies to communicate, appeal to new audiences, and recruit adherents. Establishing and supporting relationships with those companies that are driving these technological changes remains critically important in countering such efforts. These partnerships have already borne fruit: for instance, private sector action—enabled by government assistance—has greatly curtailed the accessibility of violent extremist content from ISIS on the internet. However, subsequent terrorist adaptations, including the increased use of closed social media forums, only highlight the need to sustain and build on these partnerships. US government engagement with entities like the industry-led Global Internet Forum to Counter Terrorism (GIFCT) could help combat a broader spectrum of violent extremist content by using lessons learned in countering ISIS’s online presence, while also helping these companies navigate free speech issues. This should be complemented by support for local alternative narratives and counter-messaging in key countries around the world.
- **Exploiting Data.** I have previously testified about the growing data challenge the CT community faces. We continue to see an ever-expanding corpus of pertinent data, an explosion in social media information, and competing equities and authorities, non-standardized data, and challenges with incorporating biometrically-based screening systems. To overcome these challenges, we must increase our focus on expanding information sharing and improving our use of

UNCLASSIFIED

UNCLASSIFIED

data-driven techniques to counter terrorists' attempts to evade CT pressure. Given the wide range of US stakeholders with interests in data, broad reforms of our disclosure and information-sharing processes will require a whole-of-government approach that works to broadly reorient mindsets and cultures. In addition, we will continue to move towards standardizing our existing systems and developing common guidelines for use in order to facilitate greater access for relevant authorities.

Mr. Chairman, thank you again for the opportunity to present NCTC's views and assessments this afternoon. I look forward to the Committee's questions.

UNCLASSIFIED

RICK SCOTT
FLORIDA

United States Senate

ARMED SERVICES
HOMELAND SECURITY
COMMERCE, SCIENCE, AND
TRANSPORTATION
BUDGET
SPECIAL COMMITTEE
ON AGING

April 8, 2019

Director Christopher A. Wray
Federal Bureau of Investigation
935 Pennsylvania Avenue N.W.
Washington, D.C. 20535-0001

Dear Director Wray:

This February marked the one-year anniversary of the Marjory Stoneman Douglas High School shooting in Parkland, Florida, that claimed the lives of 17 innocent victims and continues to impact that community. Over the past year, I have met with the families of those victims, and the remarkable strength they have shown in the aftermath of such an unspeakable tragedy is inspiring.

Following this attack, I signed into law the “Marjory Stoneman Douglas High School Public Safety Act,” which implemented programs to improve school safety and enhance law enforcement’s ability to intervene when an individual poses a substantial risk of self-harm or harm to others. The legislation also established the Marjory Stoneman Douglas High School Public Safety Commission to investigate systemic failures that resulted in this devastating incident.

In the aftermath of the attack, repeated failures by the Federal Bureau of Investigation (FBI) to investigate and act on specific tips received about the shooter came to light. Most troubling, a detailed warning received by the FBI’s national call center just weeks before the attack was never forwarded to the South Florida field office, even after it was linked to the earlier threat logged by the your agency. I first learned of the FBI’s investigative failures as I was leaving the funeral of one of the victims, and I understand the families of the several victims were informed of such lapses by a conference call.

I am sure that you agree these failures are inexcusable, and so I request an update on the steps you have taken to hold accountable those responsible for these grave lapses in your agency’s core investigative function.

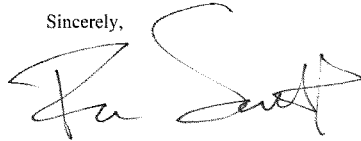
Additionally, given the FBI’s documented pre-attack interactions with other high-profile perpetrators of heinous acts of violence in Florida in recent years – including the attacks at the Broward airport, the Pulse nightclub, and the Tallahassee yoga studio – I request an update on the measures you have taken to improve the agency’s identification of and intervention against legitimate threats of mass violence. Although no action can bring back the victims lost in these

Director Christopher Wray
April 8, 2019
Page 2

senseless attacks, demanding accountability for lapses that enabled them to occur can help avoid similar tragedies in the future.

Thank you for your prompt attention and responses to these requests.

Sincerely,

A handwritten signature in black ink, appearing to read "Rick Scott", with a large, stylized "S" at the end.

Senator Rick Scott

Committee:	Senate Homeland Security and Governmental Affairs Committee
Hearing:	"Threats to the Homeland"
Date:	November 5, 2019
Topic:	Election Security
Primary MOC:	Senator Lankford (R-OK)

HSGAC Getback #1: How much has been spent of the \$380 million in election security funding allocated by Congress in 2018.

CISA Response:

The \$380 million was appropriated to the Election Assistance Commission (EAC). As such, the Department defers to the EAC on the purposes for which the funding was used by states, as well as the amount that has been spent by the states.

Committee:	Senate Homeland Security and Governmental Affairs Committee
Hearing:	“Threats to the Homeland”
Date:	November 5, 2019
Topic:	CBP Facility Conditions
Primary MOC:	Senator Sinema (D-AZ)

HSGAC Getback #2: The status of DHS efforts to ensure allegations of migrant abuse at Yuma border patrol station are reported more quickly and that swift actions to protect migrants and children are taken.

CBP Response:

CBP’s Office of Professional Responsibility (OPR) has received complaints into both the allegations of sexual misconduct and the conditions at the U.S. Border Patrol Station in Yuma, Arizona. Currently there are multiple investigations into both of those matters conducted by USBP Management, CBP OPR, and the Department of Homeland Security Office of the Inspector General. These cases are currently ongoing and will be completed when a thorough investigation has been completed. If misconduct is substantiated, appropriate corrective action will be initiated. However, the Privacy Act of 1974 generally precludes CBP from releasing information on disciplinary or other corrective actions taken against employees.

Committee:	Senate Homeland Security and Governmental Affairs Committee
Hearing:	"Threats to the Homeland"
Date:	November 5, 2019
Topic:	CBP Secondary Hearings
Primary MOC:	Sen. Peters (D-MI)

HSGAC Getback #3: (1) A description of the process for how DHS will lead a comprehensive review of secondary screenings in Fiscal Year 2020 with input from other relevant federal partners, and (2) what recommendations DHS expects to result from this review?

CBP Response:

CBP is tasked with protecting our Nation's borders, as well as enforcing numerous laws at our Nation's ports of entry on behalf of a variety of other government agencies, including state and local law enforcement. CBP officers routinely access information provided by these agencies to conduct examinations. All persons, baggage, and other merchandise arriving in or leaving the United States are subject to inspection and search by CBP officers. A secondary inspection occurs when the inspection cannot be completed on primary.

There are numerous inspectional procedures that may not be readily completed on primary and result in a referral to secondary for completion to maintain the flow of travelers. Some of the reasons for a referral for a secondary inspection include, but are not limited to:

- Processing of first-time immigrant visas.
- Processing of commercial entries requiring additional filings and paperwork (e.g. carnets).
- Processing of declarations for travelers carrying more than \$10,000.
- Processing of hunting trophies.
- Inspection of agricultural items, including items subject to the Food and Drug Administration prior notice rules.
- Verification of Public Health requirements for animals and/or biologicals.
- Verification of the importation of personally owned weapons.
- Verification of importation of foreign pharmaceutical items.
- Assessment and payment of duty and taxes (e.g., Cigarettes and Alcohol).
- At land border crossings:
 - Issuance of Form I-94 to nonimmigrant visitors.
 - Along the U.S./Canada border, the adjudication of TN work authorizations.

Therefore, secondary inspections allow CBP to inspect arriving persons thoroughly while facilitating legitimate travel and trade.

As part of the inspection process, CBP officers must verify the identity of persons, determine the admissibility of alien travelers, and look for possible terrorists, terrorist weapons, controlled substances, and a wide variety of other prohibited and restricted items. Occasionally, CBP may inconvenience law-

abiding persons in our efforts to detect, deter, and mitigate threats to our homeland caused by the few individuals who are involved in illicit activities. CBP relies on the patience, cooperation, and understanding of travelers to ensure the effective protection of our borders.

The review process begins at the ports of entry with the secondary management chain of command who reviews, approves, and disapproves actions daily. The vast majority of CBP operations are subject to oversight and supervisory approval prior to completion. Furthermore, CBP inspections are continually reviewed by both internal and other agencies within DHS to ensure that the inspectional process complies with all relevant laws and regulations protecting both the security of the United States and the civil rights of travelers. At the conclusion of these reviews, recommendations are made to improve CBP procedures to ensure compliance with laws and regulations of the United States.

CBP takes allegations of employee misconduct very seriously and has instituted policies pertaining to abuses of authority. Complaints of unprofessional conduct are recorded, investigated, and appropriate action is taken against CBP employees that are found to have violated policy. However, the Privacy Act prohibits any disclosure of discipline taken towards CBP personnel.

TSA Response:

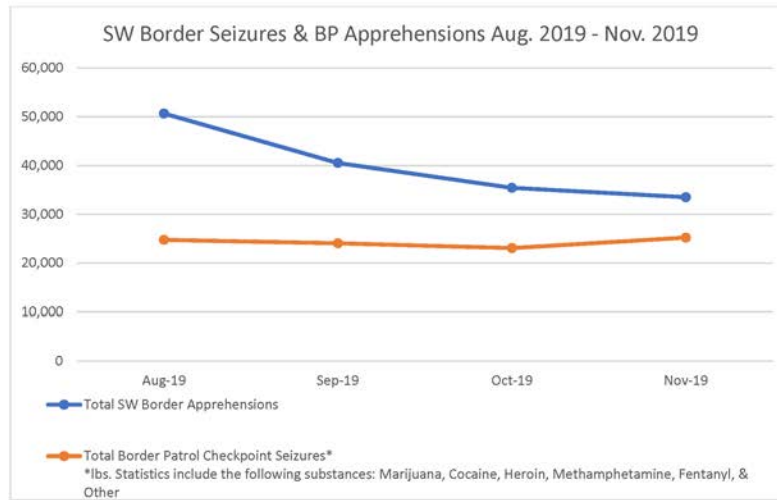
In many circumstances, TSA is limited for security and other reasons in providing detailed information in response to DHS TRIP inquiries. We recognize that these constraints, which are grounded in the need to protect certain security-related information, may cause frustration to individuals seeking a more comprehensive response. In 2018, DHS TRIP worked with TSA's Office of Intelligence and Analysis to ensure a robust process for handling applicants who have hit against intelligence-based rules. The process verifies that rule matches are valid and relevant cleared lists are operating as intended. Noting such, TSA has taken the following two actions to be as responsive as possible to traveler needs. For example:

- To increase customer service and effectiveness, DHS TRIP recently updated its public-facing website by improving its FAQ page, ensuring use of Plain Language, and making the interface more user friendly.
- DHS TRIP continually seeks process improvements that increase customer service by shortening response time to applicants. For example, in fiscal year 2014, DHS TRIP closed cases in 62 days on average. Implementation of performance-based metrics, increased outreach and training of partner agencies adjudicating TRIP cases, and other measures have consistently reduced average case cycle time. By the close of fiscal year 2015, DHS TRIP had reduced cycle time by 12 days. Ongoing attention to process improvement has led to a steady increase in efficiency, such that at the close of fiscal year 2019, DHS TRIP was closing cases in an average of 42 days. Currently, DHS TRIP is averaging 38 days to close a case.

Committee:	Senate Homeland Security and Governmental Affairs Committee
Hearing:	"Threats to the Homeland"
Date:	November 5, 2019
Topic:	Border Security/Drugs
Primary MOC:	Sen. Hawley (R-MO)

HSGAC Getback #4: To what extent is the decrease in apprehensions over the past two months reflected in terms of the amount of contraband seized?

CBP Response:



	Aug-19	Sep-19	Oct-19	Nov-19
Total SW Border Apprehensions	50,684	40,507	35,415	33,510
Total Border Patrol Checkpoint Seizures* *lbs. Statistics include the following substances: Marijuana, Cocaine, Heroin, Methamphetamine, Fentanyl, & Other	24,764.95	24,045.67	23,068.17	25,217.78

**Post-Hearing Questions for the Record
Submitted to Hon. David J. Glawe
From Senator Thomas R. Carper**

“Threats to the Homeland”

November 5, 2019

Question#:	1
Topic:	Climate Change
Hearing:	Threats to the Homeland
Primary:	The Honorable Thomas Carper
Committee:	HOMELAND SECURITY (SENATE)

Question: As you know, every two years at the start of each new session of Congress, the Government Accountability Office (GAO) produces something they called a "High Risk List." On the list for 2019, GAO lists climate change as a risk to not just the environment, but a significant fiscal risk to the federal government. As of December 2018, total federal funding for disaster assistance since 2005 is approaching half a trillion dollars, with the most recent catastrophic hurricanes, flooding, wildfires, and other losses that occurred in 2017 and 2018. Additionally, in January of this year, the Pentagon issued a report, "Effects of a Changing Climate on the Department of Defense." The report finds that the effects of a changing climate are a national security issue with potential impacts to DoD's missions, operational plans, and installations.

The January report quotes General Dunford, then-Chairman of the Joint Chiefs of Staff, as saying: "When I look at climate change, it's in the category of sources of conflict around the world and things we'd have to respond to. So it can be great devastation requiring humanitarian assistance-disaster relief-which the US. Military certainly conducts routinely."

Given these findings on climate change and the fact that your testimony does not touch on this evolving threat, does the Department of Homeland Security (DHS) have a similar analysis of climate risks to homeland security, comparable to the DoD report or the GAO report?

Response: The U.S. Department of Homeland Security (DHS) has conducted multiple mission focused analysis of climate risks to homeland security. The following activities, noted in the next response, have been conducted to address climate risks within the Department.

- February 2012, published DHS Environmental Justice Strategy
- October 2015, published DHS Directive 008-03, Continuity Programs
- July 2016, published DHS Climate Resilience Directive
- September 2016, published DHS Directive 023-04, Rev. 00, Environmental Justice
- November 2016, published DHS "Analytical Study on Mass Migration"

Question#:	1
Topic:	Climate Change
Hearing:	Threats to the Homeland
Primary:	The Honorable Thomas Carper
Committee:	HOMELAND SECURITY (SENATE)

- September 2017, formation of DHS Resilience Framework Tiger Team in collaboration with the Office of Operations, Continuity Division as a follow on of the Climate Resilience Directive
- August 2018, DHS Under Secretary of Management signed DHS Resilience Framework
- August 2019, Operational Components submitted their “Plan for Resilience”
- October 2019, officially formed the Critical Infrastructure Security and Resilience (CISR) Working Group (formerly the DHS Resilience Framework Tiger Team)

Question: If not, why not? Undersecretary Glawe, please enumerate the Department’s current efforts to quantify and address the threat to the homeland from climate change.

Response: Outlined below is a summary of efforts supporting the Departments efforts in climate risk and resilience.

In February 2012, DHS drafted its first Environmental Justice Strategy pursuant to Executive Order 12898, *Federal Actions to Address Environmental Justice in Minority Populations and Low Income Populations*, and the Memorandum of Understanding on Environmental Justice, signed by DHS in 2011. The Department makes achieving environmental justice part of its mission by identifying and addressing, as appropriate, high and adverse human health or environmental effects of its programs, policies, and activities on minority populations and low-income populations. Environmental justice communities continue to be at greater risk from elevated temperatures and associated co-pollutants, energy and food insecurity and the movement of goods, economically more vulnerable to natural disasters and illnesses, and are at greater risk of displacement due to rising sea levels. The change of the environmental justice landscape over the last ten years has necessitated the Department to update its’ Strategy in Fiscal Year 2020 to promote further integration within all mission areas, as necessary.

In July 2016, DHS issued the Climate Resilience Directive (No. 023-03), which established the Department’s authorities, responsibilities, policies, and requirements for climate resilience to support operations, missions, and infrastructure. This Directive incorporates procedures from numerous authorities, such as Executive Order (EO) 13690: Establishing a Federal Flood Risk Management Standard and a Process for Further Soliciting and Considering Stakeholders Input; EO 13689: Enhancing Coordination of National Efforts in the Arctic; and EO13653: Preparing the United States for the Impacts of Climate Change. In coordination with this Directive, the Climate Resilience Executive Steering Committee and Charter were executed to support this effort.

Question#:	1
Topic:	Climate Change
Hearing:	Threats to the Homeland
Primary:	The Honorable Thomas Carper
Committee:	HOMELAND SECURITY (SENATE)

In July 2016, DHS issued the Climate Resilience Directive (No. 023-03), which established the Department's authorities, responsibilities, policies, and requirements for climate resilience to support operations, missions, and infrastructure. This Directive incorporates procedures from numerous authorities, such as Executive Order (EO) 13690: Establishing a Federal Flood Risk Management Standard and a Process for Further Solicitating and Considering Stakeholders Input; EO 13689: Enhancing Coordination of National Efforts in the Arctic; and EO 13653: Preparing the United States for the Impacts of Climate Change. In accordance with Climate Resilience Directive, the Climate Resilience Executive Steering Committee formed in FY2016 was chartered to advance DHS climate resilience coordination and preparedness. This Directive and Executive Steering Committee has now formed into the Critical Infrastructure Security and Resilience (CISR). The Directive and Executive Steering Committee Charter is currently being updated to reflect the current Department Resilience process and posture. In September 2016, DHS issued Directive No. 023-04, Rev. 00, *Environmental Justice*, to establish Departmental policy regarding administration of the Environmental Justice program. The policy addresses nine program areas: federal grant and assistance programs; public participation and access to information; research, data collection and analysis; subsistence consumption of fish and wildlife; National Environmental Policy Act; Title VI of the Civil Rights Act of 1964; climate change; goods movement; and reporting.

In November 2016, DHS completed the "*Analytical Study on Mass Migration*." The study sought to enhance understanding of potential natural or man-made triggers, including climate change, that cause mass migration events. The results of the study 1) inform adjustments to the Department's Operational Plans and strategic approaches, 2) allow the Department to enrich the ability to predict these immigration surge events, and 3) improve preparedness to respond to these events. (Note: The *Analytical Study on Mass Migration* is Unclassified//FOUO/Law Enforcement Sensitive. Owner: U.S. Coast Guard and U.S. Citizenship and Immigration Services through the Strategy and Policy Executive Steering Committee.)

In September 2017, the Management Directorate (MGMT) formed a tiger team in collaboration with the Office of Operations Coordination (OPS), as a follow on of the Climate Resilience Directive. This tiger team developed the *DHS Resilience Framework*, which was signed by the DHS Under Secretary of Management in August 2018. This framework focuses on critical infrastructure areas: energy and water, facilities, information and communication technology, and transportation. It also establishes guidelines for implementing, monitoring, and identifying DHS resilience and mission readiness, and mandated each Operational Component to submit a "Plan for Resilience" by August 30, 2019. All Operational Components submitted these plans in August, 2019. Updates to the Plans are to follow the Continuity Directive process of formal updates every 2 years and informal annual updates if any assets change within Real Property.

Question#:	1
Topic:	Climate Change
Hearing:	Threats to the Homeland
Primary:	The Honorable Thomas Carper
Committee:	HOMELAND SECURITY (SENATE)

In October, 2019, the Resilience tiger team officially formed into the Critical Infrastructure Security and Resilience (CISR) Working Group, whose membership consists of each Operational Component, Headquarters offices and MGMT Lines of Business, and is spearheaded by the MGMT Chief Readiness Support Officer and the OPS. This working group continues the activities of implementing the DHS Resilience Framework within the Department.

Question: In what specific programs is this threat taken into account, and how does the threat influence resource allocation decisions within the Department?

Response: The Department addresses risk and threats in numerous ways. Through the CISR Working Group, the team has developed the Resilience Baseline Assessment Scoring (RBAS) tool and Plan for Resilience template to assess resilience and prioritize projects based on highest vulnerabilities. The template is a roadmap to use while developing the DHS Plan for Resilience. Each Component has a specific mission which has identified statutes, laws, and national and departmental resilience policies. This template serves as a guide on the necessary elements required to be included for the document to be holistic and result in prioritized projects to support resilience and mission readiness. The RBAS tool is an approach for documenting, scoring, and prioritizing projects and resilience capabilities at Component-wide planning levels. The outcome of this scoring is a single table using the “Resilience Factor” to determine the highest priorities of a Component’s mission essential assets. The scoring guides planners through a step-by-step process following the Resilience Framework. It is anticipated that the Operational Components will provide their first round of highest priority areas, based on vulnerabilities to high value assets, to the CISR Evaluation team in August 2020. The assessment of these high value assets will identify risks and threats and then evaluate specific gaps and potential solutions to support vulnerability mitigation.

Question#:	2
Topic:	Supplemental Funding
Hearing:	Threats to the Homeland
Primary:	The Honorable Thomas Carper
Committee:	HOMELAND SECURITY (SENATE)

Question: As you know, Congress passed on a broad bipartisan basis, and the President signed, a \$4.5 billion supplemental funding package to address the humanitarian crisis at our southern border. Over \$1.2 billion of that funding was provided to DHS.

Please provide a detailed breakdown of how that money has been allocated, obligated, and spent, including how much has been spent to this date and how much has yet to be spent. Where appropriate, please indicate the number of personnel hired by this funding.

Response: The Fiscal Year (FY) 2019 Emergency Supplemental appropriations provided DHS \$1.339 billion in funds to address the migration and humanitarian crisis at the U.S. southern border. These funds were essential in providing frontline operators the resources they needed to address the overwhelming onslaught of migrants illegally entering the United States or presenting themselves at ports of entry.

Of the funds provided, \$1.1 billion was allocated to U.S. Customs and Border Protection (CBP); \$209 million to U.S. Immigration and Customs Enforcement (ICE); and \$30 million to Federal Emergency Management Agency (FEMA). As of the end of FY 2019, CBP had obligated \$342 million; ICE had obligated \$208 million; and FEMA had obligated \$30 million. None of the funding was used to hire new federal employees.

Question: Please provide, in as much detail as possible, future plans for the expenditure of the remaining funds.

Response: DHS will continue to obligate and expend funds in accordance with the FY 2019 Emergency Supplemental appropriations bill and work with Congress to ensure obligations effectively support the Department's processing and care for migrants.

Question: Do you pledge to cooperate with the Inspector General's more detailed review of that funding so that Congress can carry out its oversight responsibilities?

Response: DHS is committed to cooperating fully with the Office of the Inspector General on their reviews of DHS's use of this funding.

**Post-Hearing Questions for the Record
Submitted to Hon. David J. Glawe
From Senator Kyrsten Sinema**

“Threats to the Homeland”

November 5, 2019

Question#:	3
Topic:	Strategic Framework
Hearing:	Threats to the Homeland
Primary:	The Honorable Kyrsten Sinema
Committee:	HOMELAND SECURITY (SENATE)

Question: Just before the Threats to the Homeland Hearing, DHS introduced their new "Strategic Framework". This document explains the nature of today's domestic challenges, including providing an extended assessment of the dangers posed by domestic terrorists, including racially-and ethnically-motivated violent extremists such as white supremacists.

This Strategic Framework is designed to assess the Department's past and provide a guidepost to its future. How long will it take for DHS to complete the in-depth analysis of current and emerging threats that the framework calls for?

Response: In addition to the priority action calling for the development of an Annual State of the Homeland Threat Assessment in the DHS Strategic Framework for Countering Terrorism and Targeted Violence, former Acting Secretary McAleenan provided supplemental guidance requesting the Office of Intelligence and Analysis (I&A) complete the Annual State of the Homeland Threat Assessment in the spring of each year.

Question#:	4
Topic:	Implementation Plan
Hearing:	Threats to the Homeland
Primary:	The Honorable Kyrsten Sinema
Committee:	HOMELAND SECURITY (SENATE)

Question: When the threat analysis mentioned above is complete, what is the timeline for DHS to develop an implementation plan to address the threats and challenges identified in the analysis?

Response: DHS continues to plan for the Strategic Framework's implementation. By summer 2020, DHS expects to release a public action plan, outlining our implementation objectives to achieve the Framework's goals. In the future, the Homeland Threat Assessment will further support proper resource placement, technical assistance requirements, and other necessary programming to achieve the Framework's goals.

Question#:	5
Topic:	SLTT Partners
Hearing:	Threats to the Homeland
Primary:	The Honorable Kyrsten Sinema
Committee:	HOMELAND SECURITY (SENATE)

Question: DHS's Office of Intelligence and Analysis (I&A) helps accomplish the Department's mission by integrating intelligence into operations across DHS Components, its partners in state and local government and the private sector to identify, mitigate and respond to threats to the Homeland, including: Counterintelligence, Counterterrorism, Cyber, Economic Security, and Transnational Organized Crime.

How does I&A ensure that all Arizona State, Local, Tribal, and Territorial (SLTT) partners are part of the information system and receiving the information they need to play their critical roles in protecting the homeland?

What capabilities does I&A need that it does not currently possess that would improve I&A collaboration with its SLTT partners?

Response: I&A has a multi-faceted approach to ensuring Arizona's State, Local, Tribal, and Territorial (SLTT) partners are fully integrated into the Homeland Security Enterprise and are receiving the information they need to protect the Homeland during steady and crisis states. This approach is consistently deployed across all states and other jurisdictions.

The primary mechanism through which information sharing occurs is via our field deployed personnel. I&A has four (4) intelligence officers currently assigned to Arizona who work closely with SLTT partners; by the end of January, three (3) more officers will be assigned to work with Arizona SLTT partners, bringing the total to seven (7) intelligence officers. I&A also maintains up-to-date distribution lists to ensure we are able to communicate with a vast array of SLTT partners in Arizona and across the nation to provide critical information sharing during times of crisis.

Additionally, I&A is the manager for the Homeland Security Information Network–Intelligence (HSIN-Intel), a community of interest located on HSIN, which is the premier destination for unclassified information sharing. The purpose of HSIN-Intel is to provide intelligence stakeholders across the Homeland Security Enterprise with a secure platform for effective, efficient, and timely collaboration and sharing of information, data, products, analytic exchange, and situational awareness. HSIN-Intel is the only federally sponsored system that is designed specifically to facilitate intelligence and information sharing among Federal, state, local, tribal, and territorial (SLTT) partners across the full spectrum of homeland security missions. HSIN-Intel has been adopted by the National Network of Fusion Centers (National Network) as the primary platform for unclassified information sharing and collaboration. HSIN-Intel has embraced a unified approach to fully incorporating other centralized intelligence capabilities,

Question#:	5
Topic:	SLTT Partners
Hearing:	Threats to the Homeland
Primary:	The Honorable Kyrsten Sinema
Committee:	HOMELAND SECURITY (SENATE)

such as Regional Information Sharing System Centers and High Intensity Drug Trafficking Areas, into the system as well to ensure information sharing across a broad intelligence stakeholder set. HSIN-Intel is a chartered and vetted community of over 4,000 intelligence professionals from homeland security, intelligence, and law enforcement communities at all levels of government who share homeland security-related information and analyses on a daily basis in order to address threats to the Homeland. The Arizona Counter Terrorism Information Center (ACTIC) has a dedicated HSIN-Intel Coordinator who is responsible for collaborating with the HSIN-Intel Program Management Office and coordinating with deployed DHS I&A field personnel.

Further, I&A has deployed the Homeland Secure Data Network (HSDN) to the ACTIC to enhance classified information sharing. I&A officers regularly access HSDN and share information meeting Arizona SLTT intelligence requirements with appropriately cleared partners.

Question: How does DHS measure the effectiveness of intelligence sharing with SLTT partners?

Response: I&A appends a survey to solicit feedback on all its released production, including that disseminated to SLTT partners via the (unclassified) HSIN and (SECRET-level) HSDN, to understand customers' use and utility, formulate intelligence requirements, and improve its dissemination process. I&A also tracks analytics associated with customer viewership on both of these networks towards these same goals. Specifically, I&A manages HSIN-Intel which contains over 42,000 intelligence products with over 11,500 of those products shared in 2019 alone. I&A's collaborative efforts increased product sharing and viewership year over year with over 91,000 product views in 2019. This significant increase demonstrates the value of the system to federal, state, and local partners.

Lastly, through I&A's annual fusion center assessment program, I&A works with the national network of fusion centers to assemble a range of data against a common set of performance measures related to multisector information sharing associated with raw, watchlisting-related, and finished intelligence that originate with both federal and SLTT entities.

Question: What capabilities does I&A need that it does not currently possess that would improve I&A collaboration with its SLTT partners?

Response: I&A currently possess the authorities and processes necessary to execute its information sharing mission throughout the United States.

**Post-Hearing Questions for the Record
Submitted to Hon. David J. Glawe
From Senator Kamala D. Harris**

“Threats to the Homeland”

November 5, 2019

Question#:	1
Topic:	Enhanced Use of Intelligence
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Earlier this year, you reportedly stated in a letter to Congress that "I&A is providing improved and enhanced intelligence capabilities to DHS components" including the "collection, reporting, and analysis [...]"

On November 1, 2019, ProPublica reported that the administration is creating a new "National Vetting Center" overseen by U.S. Customs and Border Protection. Reportedly, the new Center will give CBP access to information collected by U.S. intelligence agencies to make immigration decisions.

Is this Center being opened? If so, on what date will it become operational? Please provide all written documentation pertaining to the opening of the Center and the Center's purpose.

Response: The National Vetting Center (NVC) was established pursuant to National Security Presidential Memorandum (NSPM)-9, *Optimizing the Use of Federal Government Information in the Support of the National Vetting Enterprise*. The NVC became operational and began supporting its first vetting program, U.S. Customs and Border Protection's (CBP) Electronic System for Travel Authorization (ESTA), on December 12, 2018.

The NVC is a collaborative, interagency effort to provide a clearer picture of threats that individuals pose to national security, border security, homeland security, or public safety within the context of travel, immigration, and other vetting programs. Over time, the U.S. government developed multiple, unconnected processes to bring together threat information already lawfully held by the government in support of travel, immigration, and other types of vetting programs. The NVC centralizes and improves these processes to more efficiently and effectively inform department and agency vetting. Relevant, appropriate intelligence and law enforcement information is now accessible in a consolidated and timely manner to vetting programs that use the NVC's process and technology. Per NSPM-9, the NVC operates subject to the oversight and guidance of the National Vetting Governance Board, which is supported by an interagency legal

Question#:	1
Topic:	Enhanced Use of Intelligence
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

working group and separate privacy, civil rights, and civil liberties working group to ensure compliance with applicable law and appropriate protection of individuals' privacy, civil rights, and civil liberties.

Before the NVC started operations, the U.S. Department of Homeland Security (DHS) published a Privacy Impact Assessment (PIA) that describes the NVC's mission, purpose, use and sharing of data, and its support for the ESTA program. The DHS PIA is located here: <https://www.dhs.gov/publication/dhsallpia-072-national-vetting-center-nvc>.

DHS also released to the public a redacted version of the Implementation Plan that is required by NSPM-9. That document is located here: <https://www.dhs.gov/publication/national-vetting-center-implementation-plan>.

Additional information about the NVC is available on the CBP website at this location: <https://www.cbp.gov/border-security/ports-entry/national-vetting-center>.

Question: Which agencies will have access to intelligence information collected by the Center? Please list all sub-agencies within DHS that will have access to the Center's information.

Response: The NVC does not aggregate intelligence or law enforcement information to be shared wholesale with interested agencies; indeed, it does not control the data provided to agencies that operate vetting programs (Adjudicating Agencies) leveraging the NVC's process and technology at all. Instead, the NVC provides a process and technology by which the data vetted by Adjudicating Agencies (e.g., ESTA application data) is vetted against specific threat information held by national security partners (Vetting Support Agencies) that is relevant to the vetting of specific applications or determinations. The NVC does not independently collect or maintain the data in this process; it acts as a service provider to facilitate existing information sharing arrangements between Adjudicating Agencies and Vetting Support Agencies. This approach helps ensure this data remains current and accurate and is handled in accordance with law and policy and in a manner that protects individuals' privacy, civil rights, and civil liberties.

CBP is the first Adjudicating Agency to on-board a vetting program (ESTA) to the NVC and already has access to NVC technology to support its vetting mission. Decisions about which vetting programs will join the NVC are made by the National Vetting Governance Board, which is an interagency body established under NSPM-9 to direct the activities of the NVC.

Question: What immigration decisions will the information provided by the Center be used to determine?

Question#:	1
Topic:	Enhanced Use of Intelligence
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Response: The National Vetting Governance Board (“the Board”) decides which vetting programs will join the NVC in the future. At present, only the ESTA and nonimmigrant visa vetting programs have been approved by the Board to receive vetting support through the NVC.

Question#:	2
Topic:	Faulty Gang Intelligence
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: On July 8, 2019, ProPublica reported the story of a Salvadoran man who was separated from his children by CBP for six months based on faulty gang intelligence from a particular fusion center. The information was never made available to him or his lawyers because it was classified. As a result, the man was not able to challenge the validity of the evidence that was being used against him, resulting in his continued separation from his children and a lengthier immigration proceeding than might have otherwise been necessary.

What steps has DHS taken to ensure that the intelligence made available to DHS through the Center is accurate? Please provide any written guidance or directives on this issue to this Committee.

Response: CBP has employees embedded with this particular fusion center who ensure that the information being provided comes from official government databases and accredited officials. Individuals who have entered the United States illegally and have been subsequently apprehended by the U.S. Border Patrol (USBP) are detained and processed and queries are run through available databases to inform processing pathway determinations. USBP uses all information available at the time to make a processing pathway determination, which will in no way impact the subject's right to due process.

Question: Will the Center make classified information available to any sub-agencies within DHS? If so, what provisions have been made to ensure that individuals against whom that information is used has a fair opportunity to rebut that evidence?

Response: The fusion center at issue in this particular case does not share classified information. Aliens processed by CBP receive all process due under the law, including the Immigration and Nationality Act.

Question#:	3
Topic:	CBP's Targeting
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Agents within CBP have displayed an alarming anti-immigrant sentiment. My colleagues and I have called for an investigation into an anti-immigrant Facebook group of current and former CBP employees that mocked the deaths of several human beings at our borders.

We have also called for investigations into CBP's targeting of journalists, activists, and lawyers that oppose this administration's immigration policies.

In my Questions for the Record during your nomination, I asked you whether you "commit to resist any attempts . . . to politicize DHS's intelligence analysis." You responded YES.

Given the history of CBP's troubling conduct, what steps have you taken to ensure that the information CBP receives is not used to pursue a political agenda? Please provide any written materials that you have issued in connection with your efforts.

Response: DHS and CBP take seriously our responsibilities to the American people and those with whom our agents and officers come into contact, particularly with respect to activities protected by the 1st Amendment to the U.S. Constitution. I am committed to ensuring that DHS and CBP retain the trust of the American people through strict and consistent adherence to the laws and regulations that govern our national security mission and that sensitive information collected as part of that mission is not used to pursue a political agenda in any way. When our employees fall short of these expectations or we receive accusations of misconduct, we will thoroughly investigate and hold accountable those who fail in their duty to the American people.

CBP does not target journalists for inspection based solely on their occupation or their reporting. In accordance with guidance issued in May 2019 by the former Acting DHS Secretary, CBP does not target, discriminate, or profile any individual solely for exercising his or her rights under the First Amendment. CBP is committed to the fair, impartial and respectful treatment of all travelers, and has memorialized its commitment to nondiscrimination in its policies. Consistent with the Privacy Act (5 U.S.C. § 552a(e)(7)), CBP does not maintain records that describe how any individual exercises his or her First Amendment rights, unless "expressly authorized by statute, permitted by the individual about whom the record is maintained, or pertinent to and within the scope of an authorized law enforcement activity."

The former Acting Secretary's memo on protected 1st Amendment activity may be found at <http://dhsconnect.dhs.gov/news/Pages/Message-from-Acting-Secretary-McAleenan-on-the-First-Amendment-Protected-Activities.aspx>.

Question#:	4
Topic:	Facial Recognition Technology
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: On October 9, 2019, Politico reported that a facial recognition technology pilot is currently being deployed by CBP at a port-of-entry processing center in San Luis, Arizona, where traditional methods such as kiosks are not being used but instead cameras are capturing images of travelers for border security measures. According to a Politico article regarding the facial recognition technology being used at the San Luis port-of-entry, there is a lack of consent and limited understanding from travelers whose images are currently being captured. There have been serious concerns raised regarding the use of this technology as it relates to bias against persons of color and privacy interests. In California, there are restrictions on the use of certain facial recognition technology by law enforcement and local agencies due to concerns over the technology's inaccuracy.

For what purpose is this data being utilized?

Response: DHS is congressionally mandated to implement a biometric entry-exit system.¹ The Consolidated and Further Continuing Appropriations Act of 2013 (Public Law 113-6) transferred the biometric exit operations mission from DHS generally to CBP.

In 2017, CBP developed an integrated approach to the biometric entry-exit mandate using facial comparison technology. CBP introduced the use of facial comparison technology into an already established process that requires the verification of an individual's identity when entering or exiting the U.S. The facial comparison technology is used to match a traveler to their travel document, as an alternative to the manual check conducted today.

Moreover, CBP's Traveler Verification Service Privacy Impact Assessment (PIA)² thoroughly outlines CBP's biometric facial comparison technology use as well as policies and procedures for the collection, storage, analysis, use, dissemination, retention, and/or deletion of data. In

¹ The following statutes require DHS to take action to create an integrated entry-exit system: Section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-215, 114 Stat. 337; Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, 110 Stat. 3009-546; Section 205 of the Visa Waiver Permanent Program Act of 2000, Pub. L. No. 106-396, 114 Stat. 1637, 1641; Section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272, 353; Section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), Pub. L. No. 107-173, 116 Stat. 543, 552; Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108-458, 118 Stat. 3638, 3817; Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266, 338; and Section 802 of the Trade Facilitation and Trade Enforcement Act of 2015, Pub. L. No. 114-125, 130 Stat. 122, 199.

² <https://www.dhs.gov/publication/dhscbpia-056-traveler-verification-service-0>

Question#:	4
Topic:	Facial Recognition Technology
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

accordance with DHS policy, CBP uses the Fair Information Practice Principles, or FIPPs, to assess the privacy risks and ensure appropriate measures are taken to mitigate risks from data collection through the use of biometrics, all of which is included in the PIA.

Question: How long is the facial recognition data retained? Please provide any written guidance relating to this issue.

Response: As discussed in CBP's PIA,³ facial images for arriving and departing non-U.S. citizens and lawful permanent residents are retained by CBP for up to 2 weeks. Photos of non-U.S. citizens are shared and stored in DHS's Automated Biometric Identification System (IDENT) for up to 75 years.⁴ U.S. citizens are not in-scope⁵ for biometric exit, therefore photos of U.S. citizens used for biometric comparison purposes are deleted immediately upon confirmation of US citizen status, and are not shared with DHS or other components.

³ <https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0>

⁴ <https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf>

Question#:	5
Topic:	Plans to Implement Facial Recognition
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: What entities is this facial recognition data being shared with?

Response: CBP will continue to share biographic entry and exit data, consistent with the terms described in the relevant System of Record Notices (SORNs) listed in the PIA.⁶ CBP updates these notices for any new uses. CBP may also share information with federal, state, and local authorities on a case-by-case basis, which may be authorized or required by law to use the information for purposes beyond the scope of CBP's mission for law enforcement, judicial proceedings, congressional inquiries, audits, and other lawful purposes. However, CBP does not share the U.S. citizen photos taken at entry or exit. Consistent with existing practice, CBP entry and exit records for non-U.S. citizens are available to authorized users of IDENT who may access this data in support of their own law enforcement missions.

Under the Transportation Security Administration (TSA) exit demonstration and the partner process initiative, CBP may share the result of the facial comparison (i.e., simply a "match" or "no match" result) with the approved partner agency or organization in order to allow the traveler to proceed. CBP shares the facial images of in-scope travelers within DHS, with IDENT, and on occasion with DHS's Science and Technology Directorate (S&T) for testing purposes. CBP also partners with the National Institute of Standards and Technology (NIST) to test technologies developed by specified vendors and to evaluate algorithms on biometric projects.

Question: Has CBP's use of facial recognition technology resulted in any immigration enforcement activities? If so, what activities resulted from CBP's use of the technology?

Response: Since the implementation of the new facial comparison entry process, CBP officers have successfully identified seven imposters in the airport environment using this technology, including two with genuine U.S. travel documents (passport or passport card), who were using another person's valid travel documents as a basis for seeking entry to the U.S. Of the seven, four received a final order of removal through the expedited removal process.

In the land environment, as of November 25, 2019, CBP has identified 215 imposters on entry using facial recognition technology, including over 50 with genuine U.S. travel documents. Of the 215 imposters identified in the land environment, 39 had criminal histories, including charges of assault, kidnapping, extortion, and drug smuggling.

⁶ See Section 1.2 of the Traveler Verification Service Privacy Impact Assessment, available at: <https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0>

Question#:	5
Topic:	Plans to Implement Facial Recognition
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Additionally, as of November 19, 2019, CBP has biometrically confirmed over 31,000 overstays on exit. This biometric confirmation is essential for maintaining the integrity of the U.S. immigration system as under current immigration laws, staying in the U.S. without official permission from the U.S. Government may result in a legal bar to reentry to the U.S. for three or ten years following departure.

Question: Are there any other plans to implement facial recognition technology along other areas of the Southern border? If so, where will such technology be deployed?

Response: CBP has deployed facial comparison technology at pedestrian entry operations in Nogales and San Luis, Arizona, as well as Laredo and El Paso, Texas. While the exact plans are still being finalized, CBP has plans to expand to additional Southwest Border locations.

Question: Are there any current plans to expand the use of facial recognition technology by other departments within DHS? Please describe in detail any such plans.

Response: CBP and TSA are evaluating the use of facial comparison technology at the TSA checkpoint for identity verification. CBP and TSA have established a three-phase pilot, beginning with a successful pilot completed at John F. Kennedy International Airport in October 2017 to perform data collection, followed by an enhanced pilot at Los Angeles International Airport from August to October 2018 and an ongoing pilot at Atlanta International Airport (October 2018). As with phases one and two, any information regarding additional CBP and TSA pilots will be reflected in the Traveler Verification Service PIA updates.⁷ The Office of Biometric Identity Management (OBIM) has existing facial recognition services available; before Components or Offices utilize these services, appropriate privacy compliance documentation (such as the Traveler Verification Service PIA), detailing useage, will be completed.

U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI), in partnership with S&T, initiated a project to evaluate and potentially implement a capability to collect and analyze facial imagery from publicly available websites world-wide to identify individuals engaged in human rights violations and war crimes. The intent of the project would be to prevent human rights violators from entering the United States and to pursue accountability measures against human rights violators and war criminals in the United State so that the United States does not become a safe haven for human rights violators and war criminals. The process would involve isolating facial images of individuals engaged in human rights violations and war crimes abroad and sharing those images with DHS OBIM, the Federal Bureau of Investigation, and the Department of Defense databases for potential matches that would then be evaluated by facial forensic analysts. Any potential matches would be shared with ICE HSI along with any

⁷ <https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0>

Question#:	5
Topic:	Plans to Implement Facial Recognition
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

derogatory information contained within the identity databases. This project has not been deployed yet.

Additionally, the ICE HSI Child Exploitation Investigations Unit (CEIU), Victim Identification Section, is expanding its use of facial recognition technology to assist in the identification of offenders who sexually abuse children. Currently, CEIU is testing and developing facial recognition tools that are intended to serve as pointers or leads for agents/analysts in attempting to identify suspects in child exploitation investigations.

While ICE HSI special agents primarily utilize facial recognition technology to support criminal investigations into child exploitation and human trafficking, facial recognition technology may be utilized to assist ICE HSI in identifying individuals involved in financial fraud schemes, identity and benefit fraud, and other forms of transnational crime.

Question#:	6
Topic:	Facial Recognition Software
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: What company's facial recognition software is currently being deployed at the San Luis port-of-entry?

Response: CBP's Traveler Verification Service utilizes the NEC facial matching algorithm that was procured by OBIM.

Question: What testing measures did this software undergo before utilized at this port-of-entry?

Response: The NEC facial matching algorithm has been ranked #1 in NIST's Face Recognition Vendor Test the last few years and a version of it has also been evaluated by S&T. NEC's facial recognition algorithm has also been selected by OBIM as the Department's facial recognition algorithm and licensing is provided to CBP as part of their enterprise license agreement.

In advance of deploying this facial recognition technology to airport entry/exit processing, CBP undertook numerous pilot workflow evaluations, followed by technology demonstrations at eight airport locations to determine operational feasibility. In addition to technical considerations, traveler time and motion evaluation were performed to ensure that the introduction of new technology would not adversely impact travel flows or disrupt CBP operations. CBP continues to evaluate operational system performance of both the facial recognition technology and traveler processing.

Question#:	7
Topic:	Scan People of Color
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Research has shown that there is higher rate of inaccuracies when certain facial recognition technology is used to scan people of color. What measures has DHS taken to prevent racial bias to ensure that this technology does not disproportionately discriminate against people of color? Please provide any written guidance on this issue.

Response: CBP is fully committed to the fair, impartial and respectful treatment of all members of the trade and traveling public.⁸ CBP has rigorous processes in place to review data and metrics associated with biometric entry and exit facial comparison performance to assess and guard against operational variances. CBP data does not demonstrate any significant variance in match rates that can be attributed to demographic variables.

CBP continuously monitors the biometric comparison service and conducts a variety of statistical tests to bolster performance thresholds and minimize any possible operational variances.

As NIST concluded during its 2018 Face Recognition Vendor Test, there have been massive improvements in the accuracy of face comparison algorithms in the last 5 years.⁹ The performance of CBP's biometric comparison service continues to improve over time due to technical, operational, and procedural advancements including threshold adjustments. CBP has also issued various updates to the algorithms, which increase the algorithm's ability to create biometric templates from non-frontal images taken during the U.S. entry or exit process.

Additionally, CBP is partnering with NIST to conduct a comprehensive analysis of facial comparison technologies in CBP's biometric entry-exit efforts, in order to improve data quality and integrity, and ultimately the accuracy of technology that informs agency decision-making that affects people. NIST will provide guidance and data that allows CBP to set a threshold, given CBP's security and facilitation goals for large-scale face comparison of travelers at air, land, and sea port of entry.

⁸ CBP Policy on Nondiscrimination in Law Enforcement Activities and all other Administered Programs, available at <https://www.cbp.gov/about/ceo-diversity/policies/nondiscrimination-law-enforcement-activities-and-all-other-administered>.

⁹ See NIST Interagency Report 8238, available at <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf>.

Question#:	8
Topic:	State DMV Databases
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: On July 7, 2019, the New York Times reported that ICE officials have accessed state Department of Motor Vehicles (DMV) information using facial recognition technology without the knowledge of the subjects. Reportedly, ICE had requested access to state DMV databases from at least three states and the universe of individuals subjected to ICE's access included legal permanent residents and citizens. Many states, including California, permit undocumented individuals to secure drivers' licenses so that they can attend to their day-to-day needs, including taking their children to school and daycare and driving to work so they can put food on the table. These individuals may not have been advised when they apply for the license that they need that their information might be turned over to ICE.

Please list all instances in which ICE has executed a facial recognition search of a state DMV database, including the date of the search, the purpose of the search, the number of records accessed, and the relevant state.

Response: U.S. Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations does not apply facial recognition technology to state Department of Motor Vehicles (DMV) data for routine civil enforcement activities.

ICE Homeland Security Investigations (HSI) Special Agents have only had the ability to utilize facial recognition technology through queries of state DMV databases in Maryland, New Jersey, Pennsylvania, Florida, and previously New York until December 2019. The state New York blocked ICE HSI access to DMV records. ICE HSI does not track the details relating to these queries such as the date conducted or the number of records pursuant to each query. ICE HSI utilizes facial recognition queries in furtherance of criminal investigations, many of which involve crimes such as child exploitation, human trafficking, and financial fraud. ICE HSI does not use the technology to locate illegal aliens solely for purposes of administrative enforcement. The following summarizes the nature and purpose of ICE HSI's related activities conducted in the above-identified states:

- ICE HSI Baltimore utilizes facial recognition queries to advance investigations targeting criminals involved in child exploitation and human trafficking. ICE HSI Special Agents discover and obtain evidence in an effort to identify the abuser, identify the location of abuse, and rescue the victim. During an investigation, ICE HSI will lawfully utilize facial recognition to provide a possible match in identity of a subject previously suspected to be involved with the exploitation or trafficking of victims. Besides facial recognition, investigators utilize DMV information including photos, biographical data, and registration information to confirm the identification of suspects who are involved in

Question#:	8
Topic:	State DMV Databases
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

the ongoing abuse of children, exploitation of victims, as well as the location of the abuse.

- ICE HSI Newark reported utilizing facial recognition queries in furtherance of investigations into violent gang activity (including homicide), narcotics trafficking, money laundering, credit card fraud, and national security/terrorism-related offenses. These queries were initiated in an effort to identify individuals suspected of involvement in these types of criminal violations.
- ICE HSI offices in Pennsylvania have used facial recognition technology to identify and arrest a network of individuals who stole hundreds of identities from JP Morgan Chase Bank to illegally obtain identification cards used to establish lines of credit and defraud casinos; to identify, arrest, and extradite a U.S. citizen who committed a murder in Canada and fled back to the United States; to identify and arrest leaders and members of criminal organizations responsible for committing identity theft and the manufacturing of counterfeit credit cards leading to millions in losses; to identify a previously convicted sex offender suspected of abusing several minors; and to identify a suspect involved with smuggling large quantities of cocaine into the United States.
- ICE HSI offices in Florida reported utilizing facial recognition technology to attempt to identify possible matches to images of unidentified individuals who could be suspects, persons of interest, or victims in ICE HSI criminal investigations. These queries enable ICE HSI to obtain identifying information, such as name and date of birth, that can then be used to help progress cases. ICE HSI queries of the Florida DMV have been used in furtherance of child exploitation investigations, financial fraud investigations, and narcotics trafficking investigations.

Question#:	9
Topic:	Investigations Opened
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Has ICE undertaken any immigration actions, including the opening of an investigation or the institution of removal proceedings, in connection with individuals identified using state DMV database? Please provide a complete list of all such actions taken or investigations opened.

Response: ICE cannot provide information relating to pending or ongoing investigations, nor does it provide details on investigative methodologies and techniques utilized in its investigations.

Question#:	10
Topic:	Suicide Prevention Among Air Marshals
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: On September 15, 2019, ABCnews.com published a story entitled, "Nearly 18 years after 9/11, the federal air marshals program is in 'crisis.'" This article cited to a "union official" that said active-duty or recently retired federal air marshals died by suicide at a rate of 3-5 times per year. The ABCnews.com report also reviewed "14 suicides, psychotic breakdowns and other incidents" and their review "suggest[s] that in nearly every case prolonged, work-related stress may have played a role."

Have you read the aforementioned ABCnews.com new report?

What is DHS and TSA doing in response to the extremely high number of suicides by active-duty or recently retired federal air marshals?

Has DHS or TSA engaged with federal air marshal representatives on how to improve the physical and mental health of federal air marshals?

Response: TSA is aware of the ABC news report and takes the issues raised in the article very seriously. TSA's Federal Air Marshal Service (FAMS) has programs in place to help any employee experiencing a personal or professional crisis. FAMS engages with associations to discuss health issues facing the workforce. FAMS also constantly works to raise awareness of the multiple resources available to all FAMS employees and their family members.

Any TSA employee can contact TSA's Employee Assistance Program, which provides short-term counseling and resources, and referral services at no cost to employees and family members. The FAMS maintains a physician and other full-time medical professionals who are available 24 hours a day, seven days a week to answer questions and provide guidance to all FAMS personnel.

The FAMS also provides peer support services to all of its personnel. Since 2010, the Critical Incident Response Unit, provides guidance and support to field office Critical Incident Response Team (CIRT) trained personnel to respond to and assist FAMS employees and their families during critical incidents; specifically helping to stabilize and mitigate the psychological impact of a critical incident. CIRT personnel also provide ongoing suicide prevention and awareness training. Additionally, CIRT personnel also support employees who are experiencing personal and/or professional issues before they reach crisis level.

DHS supports the passage of H.R. 3735, *Law Enforcement Suicide Data Collection Act* that is currently with the House Subcommittee on Crime, Terrorism, and Homeland Security and would allow the U.S. Department of Justice and Federal Bureau of Investigation to receive data on

Question#:	10
Topic:	Suicide Prevention Among Air Marshals
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

suicides and attempted suicides within and from federal, state, and local law enforcement agencies.

Question#:	11
Topic:	Scheduling Federal Air Marshals
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: The same ABCnews.com news report included a representation based on interviews with "a dozen active air marshals" that scheduling guidelines for federal air marshals are "commonly disregarded by scheduling supervisors."

What is DHS doing to ensure that scheduling supervisors are following guidelines for scheduling federal air marshals?

Response: TSA's FAMS continually reviews mission scheduling protocols to support the quality of life for Federal Air Marshals and balance operational requirements. TSA monitors Federal Air Marshal mission schedules and reviews those schedules to ensure adherence to prescribed guidelines. No individual supervisor has sole control of the mission schedule of a Federal Air Marshal. Instead, the mission scheduling process involves multiple layers of review, both automated and manual, conducted by headquarters supervisors, and senior management. If a discrepancy is revealed during the review process, the issue is corrected prior to the mission.

Question#:	12
Topic:	Permanent Secretary
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Over the last two years, California has experienced its largest and most destructive wildfires in history. I visited with evacuees in Mendocino, and I walked through Paradise while the embers were still burning. This fall, while enduring mass blackouts due to corporate negligence, California experienced dozens of wildfires as a result of extremely dry conditions and hurricane-strength winds. Californians rely on the federal government to help plan for and recover from disasters like the wildfires we have experienced over the past few years.

DHS has not had a permanent Secretary since April. How can I assure my constituents that DHS is prepared to help my state recover when there is no official leadership?

Response: Acting Secretary Wolf has served more than 7 years at DHS, including during the earliest days of the Department's formation. Acting Secretary Wolf deeply understands the Department's mission to prepare for, monitor, and respond decisively to natural and man-made disasters. The Department is also thankful that the U.S. Senate confirmed Federal Emergency Management Agency (FEMA) Administrator Pete Gaynor. Administrator Gaynor and Acting Secretary Wolf will work together to lead the more than 240,000 men and women of the DHS workforce and leveraging the experience of the many senior leaders who have decades of experience in their fields, all committed to protecting the homeland against all threats.

Question#:	13
Topic:	California
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: President Trump recently threatened to withhold disaster aid from California. Do you think it is appropriate for a president to do that?

Response: DHS and FEMA continue to work under the authorities of the Stafford Act to support wildfire survivors across the state through the assistance programs approved in the Major Disaster Declarations. The President has repeatedly applauded the work of FEMA and the partner organizations helping the disaster survivors. He has also directed his Administration to look at all options for ensuring that California effectively mitigates against forest fires.

Question#:	14
Topic:	Address Climate Change
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Climate change is a homeland security threat. We know that climate change is exacerbating wildfires across the West and particularly in California. From larger wildfires and stronger hurricanes to increased migration as a result of droughts and floods abroad, if we do not prepare for and fight climate change, it will be to our collective peril. The reality is that climate change is here and lives are at risk every day. However, when in office, Kirstjen Nielsen completely ignored the threat climate change poses to our nation.

What is DHS doing to explicitly address climate change and the risks it poses to our homeland?

Response: Disaster suffering and disaster costs are increasing across the nation. For FEMA to continue to accomplish its mission of helping people before, during, and after disasters, the agency is taking steps to support communities in their adaptation efforts. Addressing future risks, such as those posed by extreme weather events regardless of their cause, is key to FEMA's mission. Accordingly, consistent with FEMA's focus on enabling disaster risk reduction, FEMA is supporting state, local, and tribal governments with efforts to prepare for the impacts of extreme weather through adaptation, which means planning for the changes that are occurring and expected to occur.

The Stafford Act sets the statutory framework from which FEMA manages its role in mitigation and addresses future risk. The Stafford Act stipulates that mitigation activities must "substantially reduce the risk of future damage." This law mandates that FEMA address future risk and helps ensure federal taxpayer dollars are used responsibly given the prospect of changing conditions. Additionally, the Stafford Act requires state, local and tribal governments to develop plans for hazards, risks and vulnerabilities in their respective jurisdictions. State, local and tribal mitigation plans are required to include the "probability of future hazard events" occurring in a given jurisdiction. Also, the plans must contain a mitigation strategy that speaks to reducing or avoiding the long-term vulnerabilities that hazards pose. Without this future look, a community cannot adequately prepare to mitigate against future loss of life and property and reduce disaster suffering.

Planning for Future Conditions

FEMA's State Mitigation Plan Review Guide ("Guide") is FEMA's official policy on the natural hazard mitigation planning requirements from Title 44 Code of Federal Regulations Part 201, and federal regulations for state hazard mitigation plans, inclusive of the District of Columbia and five U.S. territories. The guide provides guidance for state, tribal, and local government mitigation planning, including the importance of measures to identify risks and vulnerabilities associated with natural disasters and establish a long-term strategy for protecting people and

Question#:	14
Topic:	Address Climate Change
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

property in future hazards events. State mitigation plans are one of the conditions of eligibility for certain FEMA assistance, such as the Public Assistance Mitigation and HMGP. States are required to update their state mitigation plan every five years. This guide asks states to consider the probability of future hazard events, including changing future conditions, development patterns, and population demographics. The Guide clarifies that the probability of future hazard events must include considerations of changing future conditions, including the effects of long-term changes in weather patterns and extreme weather events on the identified hazards. States must continue to provide an inclusive overview of natural hazards that can affect the state, using maps where appropriate.

To better reduce risk and enhance resilience, the Guide encourages states to take a holistic approach and include not only emergency management, but also the sectors of economic development, land use and development, housing, health and social services, infrastructure, and natural and cultural resources in their planning process and mitigation program, where practicable. These mitigation plans form the basis for state mitigation grant priorities, and all of FEMA's mitigation investments must align to risks and vulnerabilities contained within these mitigation plans.

Investing in Resilience

FEMA's current Hazard Mitigation Assistance (HMA) grant programs: 1) Pre-Disaster Mitigation (PDM); 2) Building Resilient Infrastructures and Communities 3) Flood Mitigation Assistance (FMA); and 4) Hazard Mitigation Grant Program (HMGP) and 5) HMGP Post Fire Program share a common mission of preventing loss of life and property damage from natural hazards and reducing the risks from future disasters. Additionally, FEMA leverages the expertise accumulated in these programs to support the resilience-enhancing efforts of FEMA's largest grant program, Public Assistance, so that communities are more able to build back better after disasters. Two of the programs – PDM and FMA – are proactive programs aimed at building a community's resilience before disasters by reducing overall risk to the population and structures from future natural hazards, while also reducing reliance on Federal funding in future disasters for response and recovery costs.

Floodplain management regulations are effective in helping to incorporate flood resistance into new development and construction. In fact, a recent Losses Avoided Study by FEMA's Floodplain Management Division indicates that, on average, FEMA's floodplain management regulations save over \$2.4 billion annually in flood damages in the US, and the local adoption of these standards has resulted in at least \$100 billion in avoided losses over the last 40 years.

Question#:	14
Topic:	Address Climate Change
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Since 1980, there have been 78 flood and tropical storm events in the U.S that resulted in estimated losses of \$1 billion or more. Those events account for a total of over \$1.1 TRILLION dollars in losses and over 61% of the total costs of ALL disasters during that time. In the last decade, billion-dollar flood and tropical storm events increased in frequency by 50%. The toll, in economic costs and lives lost, increased by similar percentages. The frequency and severity of these events is increasing exponentially. In fact, 2/3rds of those billion-dollar disasters in the last decade occurred in the last 5 years, and 70% of the costs were incurred in the last 3 years.¹⁰

Over the 50-year history of the National Flood Insurance Program, FEMA has gained a deeper understanding of community needs and motivations and recognizes the need to adapt to lessons learned and standardized best practices. Emerging trends in the environment are also a call to action, including: the increasing frequency, severity, and costs of disasters; recent legislation (e.g., Disaster Recovery Reform Act of 2018) and NFIP program changes that will demand program agility and adaptability; the necessity and complexity of engaging an increasingly diverse set of partners; and the pace of technological advancements that open up new possibilities and raise expectations for data-driven decisions, while also meeting the requirements to secure and protect that data.

FEMA makes federal funds available through the FMA grant program to states, local communities, tribes and territories (SLTTs) to reduce or eliminate the risk of repetitive flood damage to buildings and structures insured under the National Flood Insurance Program (NFIP). The FMA grant program strengthens national preparedness and resilience and supports the mitigation mission area through FEMA's strategic goal of building a culture of preparedness. While FEMA continues to prioritize mitigating severe repetitive loss and repetitive loss properties through the FMA grant program, the total number of these properties continues to increase.

FEMA's new pre-disaster mitigation program, Building Resilient Infrastructures and Communities, which will now replace PDM, is funded with a 6 percent set aside from major disaster funding, and BRIC will provide a robust and vigorous means of mitigating the increased risk from natural hazards.

FEMA has been working diligently to launch the BRIC program this fall by engaging with thousands of stakeholders to design the program, developing the proposed BRIC Policy, drafting a Notice of Funding Opportunity, and creating a new application system to provide applicants and subapplicants with a better customer experience. FEMA's goal for the BRIC program is to transform how the Nation invests in mitigation and to build community capability to increase resilience. BRIC is an invitation to get creative, be innovative, and to build strategic partnerships

¹⁰Analysis from data maintained at <https://www.ncdc.noaa.gov/billions/summary-stats>

Question#:	14
Topic:	Address Climate Change
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

across state, local and private sector partners to bring life-saving infrastructure projects to fruition. FEMA is very enthusiastic about the BRIC program. We fully embrace this game-changing opportunity to move mitigation forward across the nation and build more resilient communities.

Applicants for FEMA's HMA grant programs can include future risk in planning their flood mitigation projects and can incorporate National Oceanic and Atmospheric Administration (NOAA) and U.S. Army Corps of Engineers (USACE) estimates of a range for future sea level rise. The effects of the projected rates of sea level rise over the course of a project's useful life can be added by the applicant to the current flood elevations for the project area in addition to any required freeboard, which is a margin of safety built into flood mitigation projects.

The new Disaster Recovery Reform Act (DRRA) provisions, Sections 1204 and 1205, continue to focus on reducing risk from wildfire particularly in the Wildland Urban Interface (WUI), as higher temperatures and drier conditions render populations in the WUI vulnerable not only to increased risk from wildfire, but to post-fire effects like erosion and flooding. DRRA Section 1204 permanently established the HMGP Post Fire program (which allows for wildfire mitigation assistance derived from a Fire Management Assistance Grant (FMAG) in addition to major disaster declarations) and provides more access to mitigation funding in high fire risk areas with infrequent major disaster declarations. DRRA Section 1205 listed 14 activities for wildfire and wind mitigation to be allowed under the HMA programs. FEMA has implemented these provisions to further help states and communities reduce their wildfire risks.

Question#:	15
Topic:	Climate Change Removed
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Climate change appeared multiple times in previous FEMA Strategic Plans. Why was climate change removed from the recent FEMA Strategic Plan?

Response: Although ‘climate change’ is not directly specified in the plan, the goal of the plan is to emphasize all aspects of disaster preparedness and response to all hazards, regardless of cause.

The Strategic Plan has a central theme that emergency management is the shared responsibility of the entire Nation. Natural or man-made hazards, longstanding or emerging threats, and catastrophic events threaten the well-being and livelihood of people in every state, tribe, territory, and locality. FEMA’s mission of helping people before, during, and after disasters requires a Strategic Plan that encompasses and embraces every community it serves. Importantly, the Strategic Plan recognizes potential future risks including those associated with extreme weather events and future changing conditions and commits the Agency to taking proactive steps to increase pre-disaster investments in preparedness and mitigation. The Strategic Plan states that disaster costs are expected to continue to increase due to rising natural hazard risk and population increases in coastal areas, and notes that both natural and manmade hazards are becoming increasingly complex and unpredictable. A key strategic objective in the Strategic Plan is to “Incentivize Investments that Reduce Risk, Including Pre-Disaster Mitigation, and Reduce Disaster Costs at All Levels.” FEMA recognizes that universal access to accurate and up-to-date risk information is a critical component of informed investment decisions and has therefore committed to improving the Agency’s ability to assess and quantify risk from multiple hazards, increasing risk mapping, identifying partnerships related to risk study and mitigation investment, and clearly presenting risk information to the American public. Additionally, FEMA is working with state, local, tribal, and territorial partners and non-governmental stakeholders to adopt and enforce modern property and building codes based on the latest available reliable risk information, which includes potential factors such as sea level rise. The Agency also proactively works to expand the number of properties covered by flood insurance and all-hazards insurance with the understanding that, both now and in the future, any property can flood. In these ways and more, FEMA demonstrates its commitment to fostering well-informed pre-disaster mitigation efforts throughout the Nation.

Question#:	16
Topic:	Future Threats
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: How can you prepare for future threats that will not look like historical threats due to climate change if you do not explicitly incorporate climate change into your planning?

Response: FEMA is planning and preparing for future threats. FEMA's Strategic Plan highlights that disaster costs are expected to continue to increase due to rising natural hazard risk. To address the changing nature of risk, FEMA's Strategic Plan then directs the agency to: build a culture of preparedness; ready the Nation for catastrophic disasters; and, reduce complexity so that communities have the data and tools they need to take mitigation actions.

In 2019, FEMA and its federal partners, in close coordination with experts across governmental agencies, academia and non-governmental organizations, released the National Mitigation Investment Strategy (Investment Strategy). The Investment Strategy represents a robust interagency and cross-government planning effort to develop a single national strategy for advancing hazard mitigation investment to reduce risks (for example, sea level rise, droughts, floods, hurricanes, tornados, and wildfires). The Investment Strategy addresses future risks throughout, as the scope includes "changing conditions," including: population growth, development, and changing weather conditions. In addition, resilience is defined in the Investment Strategy as "the ability to prepare for anticipated hazards, adapt to changing conditions, and withstand and recover rapidly from disruptions." The Investment Strategy encourages the whole community—including individuals—to invest in mitigating future hazard risks, pre- and post-disaster, by adopting the Investment Strategy's three shared goals. Supporting recommendations focus specifically on how the Federal Government and nonfederal partners can identify, support, influence, and align whole community hazard mitigation investments. FEMA is currently working with federal and non-federal partners on the implementation phase of the Investment Strategy to reduce current and future hazard risks.

Question#:	17
Topic:	Up-to-Date Scientific Modeling
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Is it possible to be an all-hazards agency regardless of cause if you do not incorporate the most up-to-date scientific modeling that demonstrates that climate change will cause future natural hazards to be unlike historical examples?

Response: Addressing all-hazards and the changing nature of risk requires FEMA to work with its partners to incorporate the best available scientific data. Wherever possible, FEMA brings data to bear and works in support of state, local and tribal needs and priorities. By addressing future risks, state, local, tribal and territorial governments are best prepared for future extreme weather events and can bounce back faster at the individual and community level.

FEMA strongly encourages communities to incorporate future conditions information into projects and plans. The agency points communities to data and tools including the U.S. Climate Resilience Toolkit, and NOAA's Sea Level Rise Viewer. In addition, FEMA points to additional future conditions information from the National Climate Assessment, NOAA, and the USACE. These Federal agencies provide future conditions data and tools that can apply at a local or regional scale.

Unclassified (U)/For Official Use Only (FOUO)

**Post-Hearing Questions for the Record
Submitted to Hon. Christopher Wray
Director
Federal Bureau of Investigations
U.S Department of Justice**

**“Threats to the Homeland”
Full Committee
Senate Homeland Security and Governmental Affairs Committee
November 5, 2019**

From Senator Thomas R. Carper

1. In your testimony, you state that more deaths were caused by domestic violent extremists than international terrorists in recent years.
 - a. What is the difference, if any, between domestic violent extremism and domestic terrorism? Are there legal distinctions between these terms that are important for policymakers to take into account?

Response: (U) The terms Domestic Violent Extremism and Domestic Terrorism are essentially equivalent.

From Senator Kamala Harris

Violence Against Transgender and Gender Non-conforming People

Transgender people—and in particular, transgender women of color—are facing an epidemic of violence. According to reports, more than 150 transgender or gender non-conforming people were killed in the United States since 2013. At least 22 people have been killed in 2019 alone.

2. Since 2017, on how many occasions did local authorities initiate contact with the FBI following the homicide of a transgender or gender non-conforming victim?
 - a. In how many of those cases did the FBI investigate whether the incident constituted bias-motivated violence?
 - b. In how many of those cases did the FBI offer or provide technical assistance to local authorities?

Response: (U) The FBI does not collect this data or classify cases to the degree of specificity required to answer these questions. The FBI can state that, since 2017, it has initiated 112 investigations that have a sexual orientation, gender, or gender identity bias nexus.

3. Since 2017, on how many occasions did the FBI initiate contact with local authorities following the homicide of a transgender or gender non-conforming victim?

Unclassified (U)/For Official Use Only (FOUO)

- a. In how many of those cases did the FBI investigate whether the incident constituted bias-motivated violence?
- b. In how many of those cases did the FBI offer or provide technical assistance to local authorities?

Response: (U) The FBI does not collect this data or classify cases to the degree of specificity required to answer these questions. The FBI can state that, since 2017, it has initiated 112 investigations that have a sexual orientation, gender, or gender identity bias nexus.

4. Since 2017, on how many occasions did local authorities initiate contact with the FBI following non-lethal incidents of violence involving a transgender or gender non-conforming victim?
 - a. In how many of those cases did the FBI investigate whether the incident constituted bias-motivated violence?
 - b. In how many of those cases did the FBI offer or provide technical assistance to local authorities?

Response: (U) The FBI does not collect this data or classify cases to the degree of specificity required to answer these questions. The FBI can state that, since 2017, it has initiated 112 investigations that have a sexual orientation, gender, or gender identity bias nexus.

5. Since 2017, on how many occasions did the FBI initiate contact with local authorities following non-lethal incidents of violence involving a transgender or gender non-conforming victim?
 - a. In how many of those cases did the FBI investigate whether the incident constituted bias-motivated violence?
 - b. In how many of those cases did the FBI offer or provide technical assistance to local authorities?

Response: (U) The FBI does not collect this data or classify cases to the degree of specificity required to answer these questions. The FBI can state that, since 2017, it has initiated 112 investigations that have a sexual orientation, gender, or gender identity bias nexus.

6. How would you characterize the FBI's relationship with the LGBTQ community? What steps is the FBI taking, under your leadership, to strengthen that relationship?

Response: (U) The FBI has strong relationships with the LGBTQ community, both at FBI Headquarters and the 56 Field Offices around the country. Protecting Civil Rights is a top priority of the FBI, and every Field Office is encouraged to provide training to local law enforcement partners, non-governmental organizations (NGOs), and community groups meant to

Unclassified (U)/For Official Use Only (FOUO)

encourage dialogue and strengthen ties. The goal is to encourage everyone who is the victim of a hate crime to report it to the FBI.

Despite the work of advocates, there is currently no official, comprehensive, accurate data on anti-transgender violence, in large part because state and local law enforcement agencies are not required to track and report incidents of bias-motivated violence, including violence targeting individuals on the basis of their sexual orientation and gender identity.

7. What steps is the FBI currently undertaking, under your leadership, to improve the tracking and reporting of bias-motivated violence?

Response: (U) The Uniform Crime Reporting is an important tool for all law enforcement to report and track biased motivated incidents. The FBI provides training on how and when to report, and encourages all law enforcement partners to report. The 2018 UCR data shows FBI reporting as well.

8. Does the FBI support legislative efforts to strengthen data collection, such as the Khalid Jabara-Heather Heyer NO HATE Act?

Response: (U) The FBI respectfully defers to the Department of Justice (DOJ) regarding proposed legislation.

Gun Violence

On November 14, 2019, a student opened fire at Saugus High School in Santa Clarita, California, killing three students and injuring three others. The shooter pulled a .45 caliber handgun from his backpack and fired on fellow students in the school's quad.

Just three days later, on November 17, two men reportedly entered a backyard in Fresno, California, and began shooting attendees at a family gathering, killing four men and wounding six others.

9. Is the FBI working with state and local law enforcement to investigate the shooting at Saugus High School?

Response: (U) In order to protect the integrity of all investigations, the FBI does not comment on the status or existence of any investigation.

- a. What, if anything, can you disclose about the shooter's motives?

Response: (U) In order to protect the integrity of all investigations, the FBI does not comment on the status or existence of any investigation.

- b. Please describe the FBI's efforts to prevent and detect potential school shootings. What guidance and resources, if any, are made available to state and local law enforcement?

Unclassified (U)/For Official Use Only (FOUO)

Response: (U) Recently in FBI Los Angeles' Lancaster Resident Agency's (RA) area of responsibility (AOR), there was a Campus Security Symposium. Representatives from the FBI, LASD, and security teams from schools in the area attended the symposium. The purpose of the symposium was for agencies to share contact information and gain an understanding of what to look for in order to prevent or detect potential threats of school violence. The FBI gave presentations on various topics, including involuntary celibate ("incel") ideology and extremism, and case studies which discussed behavior analysis.

(U) FBI Field Offices across the country provide training to state and local law enforcement partners on topics including active shooter response, behavior of potential active shooters, and case studies of past active shooters. Additionally, the FBI conducts Advanced Law Enforcement Rapid Response Training (ALERRT) to state and local law enforcement which focuses on tactical response to an active shooter scene.

(U) The FBI's Behavioral Threat Assessment Center (BTAC), housed within the Critical Incident Response Group's (CIRG) Behavioral Analysis Unit (BAU), provides behaviorally-based investigative and operational support (primarily in the form of threat assessment, threat management, investigative strategy, and prosecution strategy) to federal, state, local, tribal, and campus law enforcement agencies engaged in investigations focused on the prevention of active shootings and other acts of targeted violence.

10. Is the FBI working with state and local law enforcement to investigate the shooting in Fresno, California?

Response: (U) In order to protect the integrity of all investigations, the FBI does not comment on the status or existence of any investigation.

a. What, if anything, can you disclose about the shooter's motives?

Response: (U) In order to protect the integrity of all investigations, the FBI does not comment on the status or existence of any investigation.

b. Please describe the FBI's efforts to counter and address gun violence generally. What guidance and resources, if any, are made available to state and local law enforcement?

Response: (U) FBI is very involved with local law enforcement. For example, the Sacramento Field Office (FBI SC) participates in monthly Chief meetings with representatives from multiple local agencies in their AOR and discusses local issues. FBI SC provides training to these agencies free of cost in many areas that include, active shooter, interview and interrogation, and gun case investigations through Project Safe Neighborhood (PSN). FBI SC meets on a weekly basis with local law enforcement and county DA/USAO to review state and local cases related to gun violence through PSN. If the PSN case meets federal jurisdiction, the FBI adopts the case and assists the USAO in prosecuting the suspects in federal court. FBI SC also provides investigative and analytical support to local and state agencies in support of their investigations. FBI SC opened part-time analytical support task force officer spots to allow local and state analysts to come into FBI space and work with FBI intel analysts and staff operation specialists (SOSs) in order to help their investigations. FBI SC also provides common investigative resources such as DNA/fingerprint testing of weapons and digital image enhancements.

Unclassified (U)/For Official Use Only (FOUO)

(U) The FBI is authorized to assist in the investigation of active shooter incidents even when it is not the lead investigative agency. At the request of state or local law enforcement, the FBI can provide crisis management and command post facilities, tactical support, crime scene processing, investigative support, victim assistance, bomb technician support, and media affairs assistance. The FBI also regularly provides training and resource materials to its domestic and international law enforcement and security partners to help them prevent, prepare for, respond to, and recover from active shooter incidents. The Criminal Investigative Division, Office of Partner Engagement, and CIRG liaise with local law enforcement and academia to track and analyze active shooter incidents in the United States, including active shooter incidents in schools (ASIS). The FBI produces intelligence reports highlighting trends and significant analytic findings for dissemination to our law enforcement partners.

White Supremacist Violence

An unclassified May 2017 FBI-DHS joint intelligence bulletin found that white supremacists were responsible for 49 homicides in 26 attacks from 2000 to 2016—more than any other domestic extremist movement.

11. In light of that data, why does the FBI only track domestic terrorism broadly, without a targeted focus on white supremacist violence?

Response: (U) The FBI's records and analysis demonstrate that since 2015, of the 26 lethal attacks by Domestic Violent Extremists (DVEs), 20 were perpetrated by Racially or Ethnically Motivated Violent Extremists (RMVEs). Among the FBI's RMVE cases and disruptions in recent years, approximately 90% are RMVEs who advocate for the superiority of the white race.

(U) The FBI investigates five categories of Domestic Terrorism threats corresponding to five types of DVE: RMVE; Anti-Government/Anti-Authority Violent Extremism; Animal Rights/Environmental Violent Extremism; Abortion-Related Violent Extremism; and All Other Domestic Terrorism Threats.

(U) The FBI defines (RMVE) as threats involving the potentially unlawful use or threat of force or violence, in furtherance of political and/or social agendas derived from bias, often related to race or ethnicity, held by the actor against others or a given population group. We believe RMVE is an appropriate term because it focuses on the violence involved, not the underlying First Amendment-protected beliefs. This category allows us to both balance the current threat and evolve with emerging trends. It also accurately conveys the threat and allows us to look at the combinations of motivations often present behind an attack. The term RMVE came about as a result of Intelligence Analysts identifying similar characteristics in the driving factors of the threat actors involved. Discussion with Special Agents in Charge and subject matter experts across FBI Field Offices, combined with insight from management and guidance here at Headquarters, ultimately led us to the decision to recommend that all DT threat actors motivated by an ideological justification related to race or ethnicity be described as RMVEs. The FBI continually challenges, reviews, and evaluates intelligence to ensure we are appropriately identifying and categorizing the threats we face. Within the RMVE threat category, the FBI investigates violence perpetrated by RMVEs who advocate for the superiority of the white race.

Unclassified (U)/For Official Use Only (FOUO)

According to the FBI's 2018 Hate Crime Statistics, there were 7,120 hate crimes reported to the FBI. The majority of the reported hate crimes were motivated by race, ethnicity, or ancestry bias (59.6 percent).

12. Given the threat of hate crimes motivated by race and ethnicity, what can you tell us about resources dedicated specifically to combatting white supremacist violence?

Response: (U) The FBI uses the term RMVE to describe all threats involving the potentially unlawful use or threat of force or violence, in furtherance of political and/or social agendas derived from bias, often related to race or ethnicity, held by the actor against others or a given population group. This threat includes violent extremists who advocate for the superiority of the white race. We do not assign resources specifically to "white supremacist violence."

(U) Nationally, the proportion of Special Agent resources allocated between the FBI's DT and International Terrorism programs is commensurate with the number of predicated investigations in each program. But it is important to note that the front line of the Counterterrorism mission in the United States is the FBI-led Joint Terrorism Task Forces (JTTFs). These JTTFs investigate all types of terrorism, both domestic and international, and everything that falls within those broad categories. The FBI maintains about 200 JTTFs nationwide across all 56 FBI Field Offices and in many of our satellite Resident Agencies (RAs), with the participation of over 50 federal and over 500 state, local, tribal, and territorial agencies. The JTTFs are comprised of approximately 4,400 investigators, including FBI Special Agents and Task Force members. These partnerships at the state, local and federal levels are critical to the FBI's success as they permit the FBI to surge resources to threats as they arise. The force multiplier effect provided by the JTTFs is demonstrated by the fact that in FY19, in coordination with our JTTFs across the country, over 40% of DT subjects disrupted by arrest were arrested by JTTFs on state or local charges.

(U) An additional asset in the fight against DT is the Domestic Terrorism-Hate Crimes Fusion Cell, established in 2019, which regularly investigates and works to counter threats including those posed by RMVEs who advocate for the superiority of the white race. As just one example of the success of this Fusion Cell, in November 2019 the Denver JTTF arrested Richard Holzer on federal charges of attempting to obstruct religious exercise by force using explosives in violation of the Hate Crimes Act. Holzer planned to destroy a synagogue in Colorado, and he told undercover agents that he wanted to do something that would tell Jewish people in the community that they were not welcome in the town. The FBI's Counterterrorism and Criminal Divisions working together were able to disrupt a terrorism plot before it occurred and, for the first time in recent history, make a proactive arrest on a Hate Crimes charge.

(U) Every year the FBI conducts an in-depth review of all threats facing the American people, and in FY20 RMVEs occupied the highest priority threat band, on par with high-priority threats relating to International Terrorism, such as the threats posed by Homegrown Violent Extremists (HVEs) and ISIS.

13. What percentage of your total available resources is dedicated to white supremacist violence and what percentage is dedicated to other threats?

Unclassified (U)/For Official Use Only (FOUO)

Response: (U) All Special Agents and Intelligence Analysts assigned to threats in DT programs work to counter this threat as a subset of the RMVE threat picture. Approximately 50% of FBI's DT cases are classified as RMVE. Approximately 90% of RMVE cases are investigating RMVEs who advocate for the superiority of the white race. Resources are designated commensurate to the threat.

On March 19, 2018, Muslim Advocates, the Leadership Conference on Civil and Human Rights, and other civil rights groups wrote to you and requested a meeting to discuss the threat of white nationalists.¹ They have yet to receive a response.

14. Will you commit to meeting with these civil rights groups within the next 90 days?

Response: (U) One of the FBI's Mission Priorities is the protection of civil rights. As part of this mission, the FBI has established productive and meaningful liaison relationships with state and local law enforcement agencies, prosecutors, non-governmental organizations, and community and minority groups to improve reporting of civil rights violations, promote the benefits of sharing information and intelligence, and develop proactive strategies for identifying and addressing trends in this field. Hate crimes are the highest priority of the FBI's civil rights program because of the devastating impact they have on families and communities. The Bureau investigates hundreds of these cases every year, and we work to detect and prevent incidents through law enforcement training, public outreach, and partnerships with community groups. We will continue to engage with these groups and organizations to reinforce and build our community relationships and to foster a trusting and collaborative atmosphere with the communities we protect and serve.

Using FBI Resources to Investigate Protesters at the Border

According to an FBI "external intelligence note" obtained by Yahoo News, the FBI has monitored advocates that oppose the administration's immigration policies. The "note" reportedly lists several groups and attributes demonstrations at the border to "anarchist extremists." It further opines that the groups "are encouraging likeminded individuals to retaliate against perceived USG border atrocities."² It specifically notes that the subject groups "view US immigration policies and procedures for handling illegal immigrants-including arrests, removal, and border barriers-as violations of human rights and supporting government facilities and personnel as symbols of US tyranny." The details set forth in the note reference social media posts, articles, and other materials to support its thesis regarding groups that oppose the current administration's immigration policies.

15. Who directed the preparation of this document?

¹ Letter from Muslim Advocates, *et al.*, to Christopher Wray (Mar. 19, 2018), available at <https://www.muslimadvocates.org/files/FINAL-Ltr-to-FBI-Director-Wray-03.19.19.pdf>.

² Jana Winter and Hunter Walker, Yahoo News, *Exclusive: Document reveals the FBI is tracking border protest groups as extremist organizations* (Sept. 4, 2019), available at <https://news.yahoo.com/exclusive-document-reveals-the-fbi-is-tracking-border-protest-groups-as-extremist-organizations-170050594.html>.

Unclassified (U)/For Official Use Only (FOUO)

16. Was any individual outside the FBI involved in the preparation of this document, including in the initial decision to issue it? If so, please provide the names of any such individuals, their employers and titles, and a description of the nature of their involvement.
17. How was the information contained in this document collected? Please provide a detailed description of how the specific sources cited within the document were identified, including any ongoing monitoring activities that resulted in identification of such sources.
18. What other local or federal agencies did the FBI share this document with?
19. Did the FBI directly share this document with the Department of Homeland Security (DHS)? If so, please explain which sub-agencies within DHS received the document from the FBI, the purpose for which the FBI provided the document to DHS or any of its sub-agencies, and any information available to the FBI regarding how DHS or its sub-agencies have used or intend to use the information provided.
20. This “note” focuses on entities or individuals that oppose the administration’s immigration policies. What groups or individuals is the FBI currently monitoring that fall into this category? Please provide a complete list of each group or individual, any formal threat classification applied by the FBI to the group or individual, the reason for which they are being monitored, and the monitoring activities being deployed by the FBI.
21. Have any of the groups or individuals falling into the category described above been investigated by the FBI? For each such investigation, please provide the date that the investigation was commenced and whether the investigation remains pending. If the investigation has been closed, please provide the disposition of the investigation.

On September 4, 2019, The Hill reported an FBI statement that “[w]hile our standard practice is to not comment on specific intelligence products, FBI field offices routinely share information with their local law enforcement partners to assist in protecting the communities they serve.”³

22. Has the FBI shared the information contained in the “external intelligence note” described above to any local law enforcement partners? Please provide a complete list of all local law enforcement partners that received the “note” from the FBI.

Response: (U) While our standard practice is to not comment on specific intelligence products, FBI field offices routinely share information with their local law enforcement partners to assist in protecting the communities they serve.

Driver’s License Information

In June, the Government Accountability Office issued a report regarding the FBI’s use of state Department of Motor Vehicles (DMV) information. Among other recommendations, the report

Unclassified (U)/For Official Use Only (FOUO)

noted that the FBI has not assessed the accuracy of external partners that it relies upon in connection with its efforts to utilize state DMV records. It concluded that “[u]ntil FBI officials can assure themselves that the data they receive from external partners are reasonably accurate and reliable, it is unclear whether such agreements are beneficial to the FBI, whether the investment of public resources is justified, and whether photos of innocent people are unnecessarily included as investigative leads.”⁴

On July 7, 2019, the New York Times reported that ICE had accessed certain state driver’s license databases between 2014 and 2017, but that it was unclear whether states continued to comply with ICE requests for such access.

23. Has ICE ever requested that the FBI provide it with information obtained from state DMV databases? If so, please provide the date and content of each such request since 2017, including whether specific states’ data was requested.

Response: (U) No, Immigration and Customs Enforcement (ICE) has never requested information from the Federal Bureau of Investigation’s (FBI’s) Facial Analysis, Comparison, and Evaluation (FACE) Services Unit.

24. Has the FBI provided any records secured from state DMV databases to Immigration and Customs Enforcement (ICE)? If so, please list all states whose DMV data was provided to ICE and the dates on which such records were shared.

Response: (U) No, the FACE Services Unit has never provided any records or information to ICE.

25. In light of the GAO report, how does the FBI verify the accuracy of the information it collects before sharing it outside the FBI?

Response: (U) The FBI enters into Memorandums of Understanding (MOUs) with each state Department of Motor Vehicles (DMV)/agency. Each state DMV/agency is authorized to share driver’s license or personal identification information with the FBI for authorized law enforcement purposes. Each state DMV/agency complies with its own state’s privacy laws and the MOUs state that each party is responsible for making reasonable efforts to ensure that the information disclosed is accurate, complete, timely, and relevant. The FACE Services Unit only provides investigative lead support to the FBI Field Offices, operational divisions, and Legal Attaches. This requires an open assessment or investigation in accordance with the Attorney General’s Guidelines for Domestic FBI Operations (AGG-DOM) and the Domestic Investigations and Operations Guide (DIOG). The FBI’s FACE Services Unit offers its face recognition (FR) support and expertise only within the FBI and does not share the information outside the FBI. All DMV records returned are reviewed, analyzed, and evaluated by trained FBI Biometric Image Specialists for likely candidates prior to any responses being provided to an FBI Field Office.

Unclassified (U)/For Official Use Only (FOUO)

(U) The Government Accountability Office (GAO) recommended the FBI's Criminal Justice Information Services Division should determine whether each external FR system used by the FACE Services Unit is sufficiently accurate for the FBI's use and whether results from those systems should be used to support FBI investigations. In response, the FBI's FACE Services Unit mailed a questionnaire in July 2019 to the 23 federal and state DMV/agencies currently collaborating with the FBI's FACE Services Unit. Not all agencies responded to the survey; however, sixteen agencies responded that their FR algorithm was tested and participated in the NIST FACE Recognition Vendor Test (FRVT) algorithm accuracy testing and performance evaluations.

26. For what amount of time does the FBI retain the information collected from the state DMVs?

Response: (U) The FBI's FACE Services Unit uses its FACE Phase II case management system (FCMS) for automated workflow and data management. The FCMS is a major system application within the Next Generation Identification (NGI) system architecture.

(U) In the FCMS, the probe photos are retained in accordance with the retention schedule approved by the National Archives and Records Administration (NARA) for the FBI's FACE Services Unit. The NARA records schedule number is DAA-0065-2015-0004 and the NARA has approved the destruction of work log data when queries, photos, or log entries are (1) 20 years old, (2) are no longer needed for analysis, or (3) if 20 years have passed since last activity.

(U) The probe photo from the FBI agent and the likely candidate photo, if any, are also maintained in Sentinel, the FBI's classified case management system. FBI agents can retain the generated report, their probe photo, and likely candidate photo in their investigative case file. In many instances, no candidate is returned to the FBI agent because none meet a high enough face similarity and quality threshold. After the FR examiner completes their analysis and review, all candidate gallery photos are deleted and are not retained.

(U) It should be noted that there are several additional retention schedules associated with each specific FBI system. Both the FBI's Sentinel system and the FBI's NGI system have significantly longer retention schedules compared to the FBI's FACE Services Unit FCMS and would permit retrieval of the probe photos, if needed after deletion from the FCMS.

(U) For the FBI's NGI system, the NARA has approved the destruction of fingerprint cards and associated information, including photos, when criminal and civil subjects attain 110 years of age or seven years after notification of death with biometric confirmation. All biometrics may be removed from the FBI's NGI system earlier than the standard NARA retention period pursuant to a request by the submitting agency or the order of the court of competent jurisdiction.

(U) Disposition of records within the FBI's Sentinel system will use the same processes and procedures established by the FBI's Records Management Division for the disposition of existing hard and soft copy records. The FBI's data is divided into multiple classifications (e.g., public corruption cases, counterterrorism cases), which will be retained in the FBI's Sentinel

Unclassified (U)/For Official Use Only (FOUO)

system. The exact period of retention is determined by the type of data and/or case classification. Information will be disposed of in accordance with General Records Schedules issued by the NARA, or in accordance with specific records schedules approved by the NARA for particular case classifications.

From Senator Kyrsten Sinema

27. Transnational Criminal Organizations (TCOs) represent a major threat to the United States, especially considering the amount of illegal drugs that are smuggled into our nation on a daily basis. TCOs can also be exploited and used by Foreign and Domestic Terror entities. What capabilities does the FBI need, that it does not currently possess, to more effectively disrupt these TCOs?

Response: (U) A significant challenge the FBI is working to confront is encryption and lawful access. There is a definitive need for the FBI to legally gain access to encrypted data. With increased frequency, the FBI is unable to obtain critical information in an intelligible and usable form (or at all), despite having a court order authorizing the government's access to that information. Criminal actors are aware of these limitations and exploit their ability to hide on encrypted devices and inside encrypted messaging platforms. The inability to lawfully obtain data is negatively impacting our investigations and compromising public safety. The FBI has developed a "Lawful Access" Initiative to educate the public and private sector of the potential safety risks that arise from the challenge.

(U) The illicit use of virtual/cryptocurrency creates an additional challenge for law enforcement that would benefit from consistent regulation. TCOs utilize virtual/cryptocurrency for money laundering, the circumvention of sanctions, anonymous financial transactions and illicit financial gain. The FBI recognizes the importance of working with interagency and international partners to enhance a vigorous enforcement plan, regulatory scheme, and policy framework to thwart the opportunities created by virtual/cryptocurrency for TCOs, terrorist organizations, and other bad actors.

28. With respect to information sharing, can you provide my office with the last five intelligence products produced by the FBI for sharing terrorism related data, foreign and domestic, with your Arizona State, Local, and Tribal partners? My office is happy to receive these products in a classified setting as appropriate.

Response: (U) While our standard practice is to not comment on specific intelligence products, FBI field offices routinely share information with their local law enforcement partners to assist in protecting the communities they serve.

From Senator Jacky Rosen

ANTI-SEMITIC AND WHITE SUPREMACIST VIOLENCE: The Anti-Defamation League recently noted that the number of anti-Semitic incidents in the United States DOUBLED between 2015 and 2018. We know from history that anti-Semitism can lead to violent hatred against many other groups, and like all hate, anti-Semitism is rooted in myths, falsehoods, and vicious propaganda.

Unclassified (U)/For Official Use Only (FOUO)

In few ways is this clearer than in Holocaust denial, which we see on the internet, in white supremacist writings, and sometimes even in our schools. I even see it in the comments on my own social media page. Combating this ignorance-fueled hatred, preventing anti-Semitic violence, and stopping hate before it starts are some of the goals of the new Senate Bipartisan Task Force for Combating Anti-Semitism that Senator Lankford and I launched last month. And we are hoping to work with the FBI and others in law enforcement and in the executive branch to enhance your existing efforts to combat hate.

29. Director Wray, can you talk to us about the FBI's efforts to root out anti-Semitic and white supremacist hate and prevent violent attacks on our communities by those steeped in hatred?

Response: (U) Preventing violent attacks in the Homeland is the FBI's number one priority. The FBI works proactively to disrupt terrorist plots motivated by diverse ideologies that connect to Anti-Semitic beliefs. This includes investigative work to build out networks and identify associates of known extremists, and analytical work to understand this evolving threat. In the Domestic Terrorism realm, Domestic Violent Extremists (DVEs) who are Racially or Ethnically Motivated Violent Extremists (RMVEs) are the primary actors who pose an Anti-Semitic threat. Anti-Semitic attacks have been perpetrated by RMVEs who advocate for the superiority of the white race, as well as by those with an ideology that believes western hemisphere-based minorities are the true Jewish race and are empowered to eradicate those not in their belief system. Additionally, in April 2019, the FBI established the Domestic Terrorism-Hate Crimes Fusion Cell to address the intersection of the complementary FBI missions to combat Domestic Terrorism and provide justice to those who are victims of Hate Crimes. In the International Terrorism realm, Homegrown Violent Extremists (HVEs) who are global jihad-inspired, Foreign Terrorist Organizations (FTOs) such as ISIS and Hizballah, and state sponsors of terrorism such as Iran, have also demonstrated and acted upon a desire to target Jewish houses of worship and the Jewish community in the United States.

(U) The FBI actively engages in outreach and education on threats to help communities work with us to prevent terrorism. The FBI's most valuable tool in the Counterterrorism fight is our relationships with local and religious communities and the public, who are best positioned to notice a change in individuals' behavior and alert the FBI to threats that endanger members and congregants. We work regularly with our partners in faith-based communities to share information about threats and best practices. This includes convening calls and meetings with the heads of Jewish security organizations, sharing our unclassified intelligence products, and presenting at an All Faith Roundtable on the Homeland threat. FBI Field Offices conduct outreach with faith-based leaders in their areas of responsibility to host interfaith working groups and training in an effort to ensure communities are kept abreast of the current threat picture and are in the best position to prevent and mitigate acts of terrorism when they arise.

30. What resources do you need from Congress, and how can we best partner with you, to accomplish this mission?

Response: (U) The FBI respectfully defers to the Department of Justice regarding specific legislative proposals. The FBI welcomes any resources Congress chooses to provide.

ONLINE EXTREMISM: Last year we saw the deadliest attack on the Jewish community in modern American history, when eleven people were killed at the Tree of Life Synagogue in Pittsburgh. Perhaps unsurprisingly, the shooter was linked to numerous anti-Semitic postings on a fringe social networking site called Gab. And hours after a gunman opened fire at a synagogue in Poway, California, a violently anti-Semitic letter from the shooter appeared on 8chan and Facebook, with links to the letter later showing up on Twitter and other social media sites, spreading his hateful ideas across the world.

31. Director Wray, online forums such as 8chan and Gab do very little to police their sites from hateful and violent speech. What is the FBI doing to ensure that disturbing and hate-filled posts on these websites don't incite violence or serve as the precursor for the poster taking violent action themselves?

Response: (U) The FBI has ongoing relationships with many social media providers and technology companies in support of their efforts to combat and prevent extremist and violent speech on their platforms. FBI interactions with social media and technology companies focus on education and capacity building. This includes conversations regarding social media and other technology companies developing and voluntarily enforcing Terms of Service. To date, the FBI has engaged with multiple private sector companies through the establishment of corporate outreach programs to offer both unclassified and classified briefings regarding terrorist and criminal use of the internet. Along with our interagency partners, the FBI maintains a relationship with the Global Internet Forum to Counter Terrorism (GIFCT). FBI threat briefings assist companies in developing or enhancing voluntary measures to address the use of their platforms for hosting terrorist content, while respecting the rights guaranteed to all Americans in the United States Constitution.

(U) The FBI does not conduct any investigative activity solely on the basis of First Amendment-protected activities, or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject. Investigations of individuals are predicated on an allegation or information indicating that a federal crime or threat to national security has or may occur.

32. In the immediate aftermath of deadly attacks motivated by hate, how should mainstream social networks interact with these fringe sites to stop the spread of manifestos, letters, and other hateful writings? Is the FBI working in this space?

Response: (U) The internet continues to provide an environment for the sharing of violent extremist material and a safe haven to connect like-minded individuals through social networking sites, forums, and chat rooms. The proliferation of social media has increased the speed, efficiency, and accessibility of violent extremist ideologies while also facilitating a greater decentralized connectivity among violent extremist supporters. The FBI is increasingly concerned about violent extremists livestreaming attacks, as was employed during the attacks in New Zealand and was attempted in Poway, California. The FBI is engaged with social media companies regarding the spread of this information in the immediate aftermath of attacks. Our hope is that by offering training and engagement on the latest threats, the FBI is facilitating the

industry's ability to combat and prevent the dissemination of extremist and violent speech. Additionally, the FBI works to educate the public and specific at-risk communities about warning signs and indicators of mobilization to violence, including those found on social media and elsewhere online.

SECURING THE ELECTRIC GRID & CRITICAL INFRASTRUCTURE: As you know, our electric grid has numerous potential cybersecurity vulnerabilities. For example, malware has been discovered inside electrical components used to operate the power grid *prior* to their purchase. The FY2018 NDAA included a reporting requirement based on bipartisan legislation I introduced to require the Secretaries of Defense, Homeland Security, and Energy, and the Director of National Intelligence, to report to Congress on significant risks to the national electric grid, the effect those risks pose to military readiness, and measures to mitigate those risks.

It also asked for an evaluation of the strategic benefits from, and challenges with, isolating military infrastructure from the bulk electric grid and the benefits of the use of microgrids.

33. Director Travers, on the civilian side, what is needed to properly secure American critical infrastructure, such as the energy grid, from malicious cyber activity, including by non-state terrorist actors? Also, what do you assess to be the greatest risks to the national electric grid and the effect those risks pose to national security?

Response: (U) Properly securing the American energy grid requires robust partnerships and information sharing between the FBI, its partners, and the private sector—which owns and operates the majority of the energy infrastructure in the United States. Proper security requires energy utilities to use best practices when implementing physical or cyber security measures. Securing the supply chain remains the greatest challenge and the greatest threat to the U.S. energy sector due to the vast number of possible intrusion vectors. Many companies simply do not have the capacity to fully vet the software and equipment they use in energy infrastructure sites, such as electrical substations or natural gas processing plants. Regarding the threat of cyber terrorism to the U.S. energy sector, nation states remain the greatest threat to the U.S. electric grid due to their expertise, resources, and historical targeting patterns. Cyber criminals continue to use methods such as ransomware to cripple the IT networks of their victims and, in some cases, infect the industrial control environment.

34. How about threats to other critical infrastructure? What about private sector infrastructure like data storage centers?

Response: (U) Cyber-attacks against U.S. critical infrastructure have targeted organizations in multiple sectors, including energy, nuclear, commercial facilities, water, aviation, and critical manufacturing. The FBI is constantly identifying threat actor tactics, techniques, and procedures (TTP) to identify the actors and share with stakeholders. The threat actors targeting U.S. critical infrastructure are comprised of both nation state and criminal actors. Nation state and illicit cyber enterprises may be interested in mapping out sector networks to further their influence, collect PII, or deploy ransomware for financial gain. Malicious actors are using a number of techniques to target critical infrastructure, including conducting ransomware attacks, using

Unclassified (U)/For Official Use Only (FOUO)

botnets, and exploiting vulnerabilities in Internet of Things (IoT) devices. Increasingly, ransomware attacks against U.S. systems have been used, encrypting data and rendering systems unusable until a ransom is paid and decryption keys are provided. In order to address this threat, the FBI has collaborated with other agencies to engage with critical infrastructure entities on cyber threats by sharing indicators of compromise, TTPs, and strategic threat information with partners, including Chief Information Security Officers and corporate General Counsels.

(U) The FBI respectfully defers to the Department of Homeland Security regarding protecting critical infrastructure assets.

**Post-Hearing Questions for the Record
Submitted to Russell Travers
From Senator Jacky Rosen**

**“Threats to the Homeland”
November 5, 2019**

1. **SECURING THE ELECTRIC GRID & CRITICAL INFRASTRUCTURE:** As you know, our electric grid has numerous potential cybersecurity vulnerabilities. For example, malware has been discovered inside electrical components used to operate the power grid *prior* to their purchase. The FY2018 NDAA included a reporting requirement based on bipartisan legislation I introduced to require the Secretaries of Defense, Homeland Security, and Energy, and the Director of National Intelligence, to report to Congress on significant risks to the national electric grid, the effect those risks pose to military readiness, and measures to mitigate those risks.

It also asked for an evaluation of the strategic benefits from, and challenges with, isolating military infrastructure from the bulk electric grid and the benefits of the use of microgrids.

- a. Director Travers, on the civilian side, what is needed to properly secure American critical infrastructure, such as the energy grid, from malicious cyber activity, including by non-state terrorist actors? Also, what do you assess to be the greatest risks to the national electric grid and the effect those risks pose to national security?
- b. How about threats to other critical infrastructure? What about private sector infrastructure like data storage centers?

UNCLASSIFIED

What is needed to properly secure American critical infrastructure, such as the energy grid, from malicious cyber activity from terrorist actors?

Terrorists typically possess less sophisticated cyber capabilities than nation state actors, engaging in nuisance-level cyberattacks such as opportunistic denial-of-service attacks and defacements of poorly secured websites. Their intent is to spread propaganda and instill fear in the public. Although some probably aspire to carry out more damaging cyberattacks against the US, the IC continues to assess that terrorists lack the technical capabilities to do so. (b)(7)(C)

The IC remains concerned that poorly secured facility networks and employees with low cybersecurity awareness could provide vectors for unsophisticated cyberattacks that impact services at critical infrastructure facilities. Approximately 85 percent of US critical infrastructure is privately owned and operated. Public-private sector partnerships are essential to ensure comprehensive security of US critical infrastructure, and we consider the private sector part as the first line of defense in detection, prevention, mitigation, and response to terrorist incidents. (b)(7)(C)

Improved industry access to classified information probably would aid in the timely communication of actionable and tailored threat information to improve security and response times to an emerging crisis. The lack of a central depository for private industry clearances, high industry turnover rates, and no requirements to read personnel out when they move to new positions all hamper information flow, according to an NCTC review of information sharing with the private industry. (b)(7)(C)

What do you assess to be the greatest risks to the national electric grid from terrorist entities and the effect those risks pose to national security?

The IC has not received any credible reporting of terrorist plans to target the US electricity infrastructure and we assess that if such attacks were to occur, they would be in the form of small-scale kinetic attacks that would cause only localized or brief disruptions because most extremists lack the technical knowledge and access needed to reliably inflict greater damage. (b)(7)(C)

- The IC believes that across ideologies, lone actors pose the primary terrorist threat to the United States. Since the beginning of 2018, self-radicalized individuals not in direct contact with extremist organizations have killed 53 people in 11 attacks. (b)(7)(C)
- Most lone actors have shown a preference for soft targets that may have personal significance and the majority use simple and readily available weapons such as firearms and knives. These methods require no specialized training and minimal surveillance, which diminishes law enforcement's ability to detect operational planning and readiness. (b)(7)(C)
- Lightly protected and easily accessible energy targets, such as pipelines and electric power transmission lines, are vulnerable to terrorist attacks but do not typically cause significant damage or disruption because most groups lack the capability and knowledge to attack more robust infrastructure. (b)(7)(C)

UNCLASSIFIED

UNCLASSIFIED

- A less sophisticated attack could inadvertently cascade to cause broader outages in remote areas or challenging terrain. (U)

Attacks on energy infrastructure abroad have increased in the last decade, a trend that is correlated with the growing political and economic instability in hydrocarbon-producing regions, suggesting a rise in terrorists' interest in energy targets. (U)

- Extremists and militants frequently attack electricity infrastructure overseas, but most strikes do not cause significant damage or power disruptions because the most accessible targets- such as high and low voltage transmission towers- can be easily repaired or bypassed. However, we continue to be concerned with the potential economic impact coordinated targeting of the energy sector could cause based on previous criminal incidents in the United States. For example, from August to October 2013, USPER Jason Woodring conducted three separate attacks against electrical infrastructure in Arkansas. During one of the attacks, Woodring set fire to an electrical station in Scott, Arkansas causing more than \$4 million in damages and left anti-government messages at two of the crimes scenes. (U)

We cannot rule out the possibility of a terrorist-inspired insider kinetic or cyber attack on power facilities in the Homeland. An NCTC review of several overseas insider kinetic attacks this decade against oil and gas sector targets indicates that these types of operations often happen with no warning and pose the most significant terrorist threat to hardened energy infrastructure because employees can help attackers bypass security, identify critical components to damage, and provide maps and insights into pattern of life, judging from press reporting. (U)

- An NCTC review of six insider attacks from 2006-16 indicates that attackers need four elements to be successful: knowledge of facility security, including gaps, to gain entry, up-to date maps of the facility to navigate once inside, pattern-of-life information to identify shift changes and personnel movements, and the locations of critical components or large gatherings of personnel to maximize damage. (U)

What about terrorist threats to other critical infrastructure, including private sector infrastructure?

Terrorist groups and homegrown violent extremists (HVEs) probably lack the capability and leadership oversight to conduct complex attacks against critical infrastructure in the US. However, we remain concerned because of continued evidence of terrorist group attacks against facilities abroad and extremist messaging indicating infrastructure targets in terrorist propaganda. (U)

Cyberattacks like ransomware, which typically hold a target system hostage in return for payment, will probably continue to affect US critical infrastructure. Last year a ransomware attack, perpetrated by technically proficient criminal cyber actors, caused more than \$30 million in damages to multiple US critical infrastructure sectors. Although ransomware attacks more than doubled worldwide in 2019, we have not observed any terrorist cyber actors successfully launch such attacks. (U)

UNCLASSIFIED

UNCLASSIFIED

We continue to monitor trends in terrorist intent and capability to conduct attacks against energy sector infrastructure in the Homeland, including the following factors: global attack trends, terrorist propaganda and extremist messaging, and how extremists could leverage emerging technology or insider access to sensitive sites to conduct a complex attack. (U)

UNCLASSIFIED

