WORLDWIDE THREATS TO THE HOMELAND

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

NOVEMBER 15, 2022

Serial No. 117–73

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE
50–981 PDF WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
DONALD M. PAYNE, JR., New Jersey
J. LUIS CORREA, California
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
ERIC SWALWELL, California
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
TOM MALINOWSKI, New Jersey
RITCHIE TORRES, New York, Vice Chairman
JOHN KATKO, New York
MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, New Jersey
MARIANNETTE MILLER-MEEKS, Iowa
DIANA HARSHBARGER, Tennessee
ANDREW S. CLYDE, Georgia
CARLOS A. GIMENEZ, Florida
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
KAT CAMMACK, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MAYRA FLORES, Texas

HOPE GOINS, *Staff Director*
DANIEL KROESE, *Minority Staff Director*
NATALIE NIXON, *Clerk*

CONTENTS

WORLDWIDE THREATS TO THE HOMELAND

Tuesday, November 15, 2022

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to notice, at 9:31 a.m., in room 310, Cannon House Office Building, Hon. Bennie G. Thompson [Chairman of the committee] presiding.

Present: Representatives Thompson, Jackson Lee, Langevin, Payne, Correa, Slotkin, Green, Clarke, Swalwell, Titus, Watson Coleman, Rice, Demings, Barragán, Gottheimer, Torres, Katko, McCaul, Higgins, Guest, Bishop, Van Drew, Miller-Meeks, Harshbarger, Gimenez, LaTurner, Meijer, Cammack, Pfluger, Garbarino, and Flores.

Chairman THOMPSON. Good morning. Today, the committee is holding its annual hearing to examine "Worldwide Threats to the Homeland." We are pleased to have Secretary of Homeland Security Alejandro Mayorkas, FBI Director Christopher Wray, and NCTC Director Christine Abizaid before the committee once again.

Two years ago, the committee convened its Worldwide Threats hearing during some of the darkest days of the pandemic. Last year, the panel testified before the committee in the immediate aftermath of the attack on the U.S. Capitol. No matter the circumstances, the committee and the American people have benefited from the witnesses' frank assessment of the threats facing the homeland, both foreign and domestic. More than 20 years after the terrorist attacks of September 11, 2001, and 20 years this month since the Department of Homeland Security was established in law, we recognize the witnesses, their predecessors, and men and women of their agencies for their tireless efforts to prevent another 9/11-style attack. That said, we know that the threat posed by foreign terrorist organizations has not gone away. It has evolved and persisted, just as our efforts to combat it have. At the same time, domestic violent extremists now pose the greatest threat to our homeland. The Biden administration has put new focus on combatting this rising threat, issuing the first-ever National Strategy for Countering Domestic Terrorism, establishing a domestic terrorism analytic branch within DHS's Office of Intelligence and Analysis, and designating domestic violent extremism as a "National Priority Area" for homeland security grants.

More work remains, as extremists are increasingly willing to engage in targeted violence, whether at a synagogue in Pittsburgh, a Walmart in El Paso, or a supermarket in Buffalo. I hope to speak to our witnesses today about their assessment of the current threat

from terrorism and targeted violence and what their agencies are doing to protect the homeland.

Beyond terrorism, I remain concerned about cyber threats, particularly from Russia, China, and Iran. In response to these threats, the Biden administration has raised our cybersecurity posture by issuing an Executive Order on Improving the Nation's Cyber Security, leading global efforts to confront ransomware threats, and launching a groundbreaking public-private collaboration to help secure industrial control systems. I want to hear from our witnesses about how they assess the current threat to cyber and critical infrastructure, what progress we have made, and what more we can do.

Meanwhile, other homeland security challenges remain, like preparing for natural disasters, dealing with climate change, responding to the pandemic, securing our skies and waterways, addressing the increased number of migrants arriving at our borders, and protecting our very democracy and its institutions. Our discussion will undoubtedly touch on many of these issues today, and I look forward to a robust but respectful dialog.

As the 117th Congress draws to a close, I want to take a moment to reflect on the committee's work over the last 2 years, because together we have accomplished a great deal. Today marks our 25th full committee hearing this Congress, and our subcommittees have held more than 50 hearings, conducting oversight of some of the most pressing homeland security issues facing our Nation. We enacted critical legislation, particularly in the area of cybersecurity, creating a mandatory cyber incident reporting framework, providing cybersecurity grants to State and local governments, and improving the Federal Government's visibility into malicious activity on industrial control systems.

Historically, much of this committee's best work and many of its greatest successes have been the result of strong bipartisan effort. That has certainly been true this Congress with the gentleman from New York, Mr. Katko, as Ranking Member. Early in his time on this committee, Ranking Member Katko became a leader and innovator on aviation security, and more recently, he has made his mark on the committee's cybersecurity work. Perhaps most importantly, he was a true partner on efforts to stand up a commission to examine the January 6th attack on the Capitol, putting country before politics. The Ranking Member and I did not always agree, but we agreed when we could. When we disagreed, we tried not to be disagreeable about it. As he departs Congress, I want to thank him for his important work over the years on this committee and, on a personal note, for his friendship. I wish him the very best in the new year and beyond.

Likewise, I want to extend my thanks to all Members for their work in the 117th Congress, and especially those who are moving on to other endeavors next year: The gentleman from Rhode Island, Mr. Langevin, the gentlewoman from New York, Ms. Rice, the gentlewoman from Florida, Mrs. Demings, the gentleman from New Jersey, Mr. Malinowski, the gentlewoman from Virginia, Mrs. Luria, the gentleman from Michigan, Mr. Meijer, and the gentlewoman from Texas, Mrs. Flores. Your contributions to the commit-

tee's work this Congress and throughout your tenure are recognized and appreciated.

Again, I thank the witnesses for being here and I look forward to the hearing.

With that, I recognize the Ranking Member, the gentleman from New York, Mr. Katko, for an opening statement.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

NOVEMBER 15, 2022

Today, the committee is holding its annual hearing to examine world-wide threats to the homeland. We are pleased to have Secretary of Homeland Security Alejandro Mayorkas, FBI Director Christopher Wray, and NCTC Director Christine Abizaid before the committee once again.

Two years ago, the committee convened its world-wide threats hearing during some of the darkest days of the pandemic. Last year, this panel testified before the committee in the immediate aftermath of the attack on the U.S. Capitol. No matter the circumstances, the committee and the American people have benefited from the witnesses' frank assessment of the threats facing the homeland, both foreign and domestic.

More than 20 years after the terrorist attacks of September 11, 2001—and 20 years this month since the Department of Homeland Security was established in law—we recognize the witnesses, their predecessors, and men and women of their agencies for their tireless efforts to prevent another 9/11-style attack. That said, we know that the threat posed by foreign terrorist organizations has not gone away. It has evolved and persisted, just as our efforts to combat it have. At the same time, domestic violent extremists now pose the greatest threat to our homeland.

The Biden administration has put new focus on combatting this rising threat, issuing the first-ever National Strategy for Countering Domestic Terrorism, establishing a domestic terrorism analytic branch within DHS's Office of Intelligence and Analysis, and designating domestic violent extremism as a "National Priority Area" for homeland security grants. More work remains, as extremists are increasingly willing to engage in targeted violence, whether at a synagogue in Pittsburgh, a Walmart in El Paso, or a supermarket in Buffalo. I hope to speak to our witnesses today about their assessment of the current threat from terrorism and targeted violence and what their agencies are doing to protect the homeland.

Beyond terrorism, I remain concerned about cyber threats, particularly from Russia, China, and Iran. In response to these threats, the Biden administration has raised our cybersecurity posture by issuing an Executive Order on Improving the Nation's Cyber Security, leading global efforts to confront ransomware threats, and launching a ground-breaking public-private collaboration to help secure industrial control systems. I want to hear from our witnesses about how they assess the current threat to cyber and critical infrastructure, what progress we have made, and what more we can do.

Meanwhile, other homeland security challenges remain, like preparing for natural disasters, dealing with climate change, responding to the pandemic, securing our skies and waterways, addressing the increased number of migrants arriving at our borders, and protecting our very democracy and its institutions. Our discussion will undoubtedly touch on many of these issues today, and I look forward to a robust but respectful dialog.

As the 117th Congress draws to a close, I also want to take a moment to reflect on the committee's work over the last 2 years, because together we have accomplished a great deal. Today marks our 25th full committee hearing this Congress, and our subcommittees have held more than 50 hearings—conducting oversight of some of the most pressing homeland security issues facing our Nation.

We enacted critical legislation—particularly in the area of cybersecurity—creating a mandatory cyber incident reporting framework, providing cybersecurity grants to State and local governments, and improving the Federal Government's visibility into malicious activity on industrial control systems. Historically, much of this committee's best work and many of its greatest successes have been the result of strong bipartisan effort. That has certainly been true this Congress with the gentleman from New York, Mr. Katko, as Ranking Member.

Early in his time on this committee, Ranking Member Katko became a leader and innovator on aviation security, and more recently, he has made his mark on the

Committee's cybersecurity work. Perhaps most importantly, he was a true partner on efforts to stand up a commission to examine the January 6th Attack on the Capitol, putting country before politics. The Ranking Member and I did not always agree, but we agreed when we could. When we disagreed, we tried not to be disagreeable about it. As he departs Congress, I want to thank him for his important work over the years on this committee and, on a personal note, for his friendship. I wish him the very best in the new year and beyond.

Likewise, I want to extend my thanks to all Members for their work in the 117th Congress, and especially those who are moving on to other endeavors next year: The gentleman from Rhode Island, Mr. Langevin; the gentlewoman from New York, Miss Rice; the gentlewoman from Florida, Mrs. Demings; the gentleman from New Jersey, Mr. Malinowski; the gentlewoman from Virginia, Mrs. Luria; the gentleman from Michigan, Mr. Meijer; and the gentlewoman from Texas, Mrs. Flores. Your contributions to the committee's work this Congress and throughout your tenure are recognized and appreciated.

Mr. KATKO. Thank you, Mr. Chairman. I am pleased that the committee is holding this important hearing. I think it is vitally important to look at these issues on a routine basis and we have always done that as our Nation faces these growing and continuous changing threats posed by foreign adversaries, criminal and terror organizations, and the crisis at the Southwest Border, to name a few.

In the first 2 years of the Biden administration, we have seen a disturbing trend become a catastrophic humanitarian crisis at the border. In 2020, CBP had 500,000 migrant encounters at the Southwest Border. In 2021, the first year of the Biden administration, in pull magnets they created, these migrants encounters have tripled to well over 1.7 million. In the last fiscal year, Customs and Border Protection reported a record-breaking 2.3 million migrant encounters. Mr. Wray, I know you at FBI, that has got to be a concern for you.

While the vast majority of these migrants may be coming to find work or more prosperous opportunities, we cannot ignore the evident security threat that looms beneath the surface of that crisis.

CBP reported over 29,000 illegal immigrants who have known criminal records and 751 documented gang members, including the 312 affiliated with the notorious MS–13 gang, among those accounted at the Southwest Border. Those are the ones we know about, not the ones we don't.

Even more troubling is that these numbers only account for those that were located by law enforcement, not the 600,000 that are estimated to have evaded officers at the border in 2022 alone. How many dangerous criminals and gang members entered undetected? How many were smuggling deadly drugs, like fentanyl, into our communities? The truth is we have no way of knowing, but these reports demonstrate it is almost certainly an elevated and fast-growing number.

In addition, a still darker threat lies within the data, in something that is central to our mission here at Homeland Security. In 2020 CBP located 3 individuals—3—who were on the terrorist screening data set or watch list attempting to enter the United States along the Southwest Border points of entry. These were deemed to be a potential threat to our homeland, including known or suspected terrorists or their affiliates. In 2021 the number grew to 15. In the last reported year, 98 potential terrorists or affiliates were discovered between our ports of entry attempting to evade law

enforcement and enter the country. Again, that is just the ones we know about.

Sadly, the increased risk to our Nation's security is not the only consequence of this crisis. The migrants attempting passage are also experiencing brutal conditions that I saw first-hand, including child exploitation, rape, and death. The U.N. International Organization for Migration has labeled the Southwest Border as "the deadliest land crossing in the world" and migrant deaths from 2022 are reported to be over 850, breaking the grim record for deaths set just last year.

There are counties in Texas and in Arizona and California where they have had to cut their budgets to deal with the number of dead bodies they encounter on the border. I don't understand that.

We are reminded of these tragedies almost daily with reports of families drowning in the Rio Grande River or dying of heat exhaustion crossing the inhospitable desert, often abandoned by smugglers who care only about profits.

I would like to recognize the brave men and women who stand guard at our Nation's borders constantly under siege by drug cartels, human smugglers, and this ever-increasing humanitarian crisis. These honorable brave Americans work day and night, holidays and weekends, in some of the most unforgiving environments. I know, Secretary Mayorkas, you know that for sure. They routinely face danger and even death, all while being villainized by some for fulfilling their duties to protect our homeland from those that wish us harm. In this difficult position, it is truly tragic but unsurprising that many of them bear scars, both mental and physical, from the burden that they shoulder. My heart goes out to the families of the heroic men and women that have given all protecting our country, as well as those that suffer the mental toll of prolonged exposure to this crisis, including the alarming rise in the number of suicides amongst the agents who are despondent.

Another threat to our country illuminated by the Inspector General last year was a vetting shortfall experienced during the evacuation and resettlement of more than 79,000 Afghans as part of Operation Allies Refuge and Operation Allies Welcome. It has now become even ever clearer that the Biden administration facilitated the transfer and relocation in the United States of many Afghans that were known at the time to have potentially significant security concerns. Both Homeland Security and the Department of Defense IGs found that information used to vet evacuees was not complete, reliable, or always accurate. We understand it was a fire drill, we understand we had to protect those who helped us, but we have to do better with vetting refugees. I am a very strong supporter of having refugees coming into our country because I think they are properly vetted by and large.

We must also not lose sight of the challenges to our virtual borders. State-sponsored cyber actors continue to utilize a cyber environment to penetrate computer networks for espionage, suppression campaigns, the spread of disinformation, and to steal intellectual property and technology, to bolster their own defenses at the expense of industry, government, and everyday Americans. We must remain vigilant to the efforts of China, Russia, Iran, North

Korea, to name a few, who seek advantage in tactical capabilities in the virtual environment that bring risk to our security.

In addition to state-sponsored adversaries, organized criminal cyber thieves devise formidable attacks and fraud schemes. Ransomware attacks were up 188 percent in 2021, costing businesses an estimated $1.2 billion and were focused on schools and health care organizations primarily, including many in my district.

I look forward to the collective insight of our witnesses today on how we can further address the most prevalent and concerning cyber threats impacting both our communities and National security.

Additionally, along with many Americans, I am sad to say that I am very concerned about reporting that an FBI agent, Timothy Thibault—if I said that correctly—may have depressed derogatory information relevant to on-going investigations relating to Hunter Biden. He has a long history of partisanship and he was quickly—left the agency when these allegations came to light. As a career law enforcement professional, I know I found these revelations to be deeply troubling, as did many others in law enforcement.

Similarly, Mr. Wray, you have publicly acknowledged, and I applaud you for that, that you were troubled by the allegations at a recent Senate Judiciary hearing. While today's hearing is focused primarily on threats to the homeland security, I have to say I am concerned about the overall state of the Bureau and increasingly partisan perception, right or wrong, of the Bureau. I say that from someone, who for 20 years worked day and night on the highest and most violent and dangerous criminals in the world as a Federal organized crime prosecutor in El Paso, Texas and San Juan, Puerto Rico and up-State New York. Every time I had FBI agents by my side, they did the best wire taps, they did the best organized crime cases, they were by far what I considered to be the A Team when you did those major cases. I know those agents, because they are still friends of mine, are heartbroken by the perception of the FBI today. I hope in the days and years going forward that you can turn that ship around because our Nation deserves it. When our Nation loses faith in law enforcement, that is a terrible thing. You are the premier law enforcement agency and I hope you can turn this ship around.

Mr. Chairman, as you alluded to, this is in all likelihood my last full committee with this hearing. Of all the decisions I have had to make about whether to retire or not, this was the toughest one by far because I have had more joy and more satisfaction with this agency because it was like a bastion of bipartisanship. We don't conduct a lot of the antics and the cheap theatrics a lot of the other committees do. We get our job done because we care about this Nation, whether a Republican or a Democrat, and we love our Nation and we want to keep it safe. I commend you for the time that you have been Chairman and the way you have conducted yourself and the way we have become friends and the way we have been able to keep our eyes focused on the mission despite all of the partisan rancor that seems to be higher than ever these days.

So good for you for what you have done for this committee and good for all of you Members here who have put your partisanship

aside when we come in this room and do what is right for this country. That to me is a very important thing.

We may often disagree, and sometimes even strongly, Mr. Chairman, but I believe this committee has demonstrated our passion for securing the country's bipartisan steadfast.

I want to thank my committee staff who has spent countless hours developing oversight legislation and policy to secure the United States from all manner of threats. I am incredibly grateful for their service and dedication to the mission. Many of them are with me here today. I am not going to single them all out, but there is one I will single out. This person has been with me from the beginning, is now my staff director. The entire 8 years I have been in Congress I have worked with him side by side on homeland security matters, and that is Kyle Klein who is right behind me. I want to say thank you to him. He has been a true professional. He is a bipartisan person. He cares about this country and loves this country and wants to keep it safe. So, Kyle, thank you very much and I just want to say thank you to you.

With that happy note, I yield back.

Thank you, Mr. Chairman.

[The statement of Ranking Member Katko follows:]

STATEMENT OF RANKING MEMBER JOHN KATKO

Thank you, Mr. Chairman. I am pleased that the committee is holding this important hearing today, as our Nation faces growing and continuously-changing threats posed by foreign adversaries, criminal and terror organizations, and the crisis at the Southwest Border.

In the first 2 years of the Biden administration, we have seen a disturbing trend become a catastrophic humanitarian crisis at the border. In 2020, CBP had 500,000 migrant encounters at the Southwest Border. In 2021, the first year of the Biden administration, these migrant encounters tripled to well over 1.7 million, and in this last fiscal year, CBP reported a record-breaking 2.3 million migrants encounters.

While the vast majority of these migrants may be coming to find work or more prosperous opportunities, we cannot ignore the evident security threat that looms beneath the surface of this crisis. CBP reported over 29,000 illegal migrants who had known criminal records and 751 documented gang members, including 312 affiliated with the notorious MS–13 gang, were among those encountered at our Southwest Border.

Even more troubling is that these numbers only account for those that were located by law enforcement, not the 600,000 that are estimated to have evaded officers at the border in 2022. How many dangerous criminals and gang members entered undetected? How many were smuggling deadly drugs like Fentanyl into our communities? The truth is we have no way of knowing, but these reports demonstrate it is almost certainly an elevated and fast-growing number.

In addition, a still darker threat lies within the data. In 2020 CBP located three individuals who were on the Terrorist Screening Dataset or "watch list" attempting to enter the United States along the Southwest Border between ports of entry. These were people deemed to be a potential threat to our homeland, including Known or Suspected Terrorists or their affiliates. In 2021, the number grew to 15. In the latest reporting for 2022, 98 potential terrorists or affiliates were discovered between our ports of entry in attempting to evade law enforcement and enter the country.

Sadly, the increased risk to our Nation's security is not the only consequence of this crisis, the migrants attempting passage are also experiencing brutal conditions including child exploitation, rape, and death. The U.N. International Organization for Migration has labeled the Southwest Border as the "deadliest land crossing in the world" and migrant deaths for 2022 are reported to be over 850, breaking the grim record for deaths set just last year. We are reminded of these tragedies almost daily with reports of families drowning in the Rio Grande River or dying of heat exhaustion crossing the inhospitable desert, often abandoned by smugglers who care only about profits.

I would like to recognize the brave men and women who stand guard at our Nation's borders, constantly under siege by drug cartels, human smugglers, and this ever-increasing humanitarian crisis. These honorable Americans work day and night, holidays and weekends, in some of the most unforgiving environments. They routinely face danger and even death, all while being villainized by some for fulfilling their duties to protect our homeland from those that wish us harm. In this difficult position, it is tragic but unsurprising, that many of them bear scars both mental and physical from the burden that they shoulder. My heart goes out to the families of the heroic men and women that given all protecting our country as well as to those that suffer the mental toll of prolonged exposure to this crisis.

Another threat to our country, illuminated by Inspector General reporting this year, was the vetting shortfall experienced during the evacuation and resettlement of more than 79,000 Afghans as part of Operation Allies Refuge and Operation Allies Welcome. It is now becoming ever clearer that the Biden administration facilitated the transfer and relocation into the United States of many Afghans that were known at the time to have potentially significant security concerns. Both the DHS and DoD IGs found that information used to vet evacuees was not complete, reliable, or always accurate.

We must also not lose sight of the challenges to our virtual borders. State-sponsored cyber actors continue to utilize the cyber environment to penetrate computer networks for espionage, suppression campaigns, the spread of disinformation, and to steal intellectual property and technology to bolster their own defenses at the expense of industry, Government, and everyday Americans. We must remain vigilant to the efforts of China, Russia, Iran, and North Korea, who seek advantage and tactical capabilities in the virtual environment that bring risk to our security.

In addition to state-sponsored adversaries, organized criminal cyber thieves devise formidable attacks and fraud schemes. Ransomware attacks were up 188 percent in 2021 costing U.S. businesses over $1.2 billion dollars and were focused on schools and health care organizations. I look forward to the collective insight of our witnesses today on how we can further address the most prevalent and concerning cyber threats impacting both our communities and national security.

Additionally, along with many Americans, I am concerned by reporting that an FBI agent, Timothy Thibalt, may have suppressed derogatory information relevant to on-going investigations related to Hunter Biden, and has a long history of partisanship. As a career law enforcement professional, I know I found these revelations to be deeply troubling, as did many others in law enforcement. Similarly, you have publicly acknowledged that you were troubled by the allegations at a recent Senate Judiciary hearing. Director Wray, while today's hearing is focused primarily on threats to homeland security, I have to I am concerned about the overall state of the Bureau and the increasingly partisan perception of the agency.

Mr. Chairman, in all likelihood, this will be the last full committee hearing of the Congress and, for me, as Ranking Member. Serving alongside you and all of our colleagues has been the honor of my career, and I am forever grateful to the service and dedication to our national security by you and Members of this committee on both sides of the aisle. While we may often disagree—even strongly disagree—I believe this committee has demonstrated that our passion for securing the country is bipartisan and steadfast. I also want to thank my committee staff, who have spent countless hours developing oversight, legislation, and policy to secure the United States from all manner of threats. I'm incredibly grateful for their service and dedication to the mission.

And with that, Mr. Chairman, I yield back.

Chairman THOMPSON. The gentleman yields back. Honestly, I already expressed my thoughts on your leadership as well as the Members who will be departing, and thank you much.

Mr. KATKO. We are on the same page.

Chairman THOMPSON. Other Members of the committee are reminded that under committee rules opening statements may be submitted for the record.

[The statement of Honorable Jackson Lee follows:]

STATEMENT OF HONORABLE SHEILA JACKSON LEE

NOVEMBER 14, 2022

Thank you, Chairman Thompson and Ranking Member Katko, for convening this hearing and affording us, the Homeland Security Committee, the opportunity to hear testimony on "Worldwide Threats to the Homeland."

I welcome today's witnesses and look forward to their testimony:

- The Honorable Alejandro Mayorkas, Secretary, U.S. Department of Homeland Security;
- The Honorable Christopher A. Wray, Director, Federal Bureau of Investigation, U.S. Department of Justice; and
- The Honorable Christine Abizaid, Director, National Counterterrorism Center, Office of the Director of National Intelligence.

This hearing is the committee's annual opportunity to examine threats to the U.S. homeland, both foreign and domestic, with leaders of the Department of the Homeland Security (DHS), Federal Bureau of Investigation (FBI), and National Counterterrorism Center (NCTC).

The committee is holding this hearing not only to examine existing and emerging homeland threats, but also to reflect on the progress that has been made to secure the homeland over the last two decades and assess challenges that remain.

No matter what other challenges might emerge, we must never forget that one of our Nation's greatest threats comes from our struggle against violent extremism that began on September 11, 2001 and has extended to violent extremists living among us who use political affiliation as a justification for acts of terror.

These risks to our homeland have been compounded in recent years by the agitation and incitement of domestic extremists who in many cases have resorted to violence to manifest their delusional ideologies.

September 11, 2001, remains a tragedy that defines our Nation's history, but the final chapter will be written by those who are charged with keeping our Nation and its people safe while preserving the way of life that terrorists sought to change.

Today, the loved ones of the victims continue to grieve over the deaths of so many of our fellow citizens who were their fathers, mothers, grandparents, children, grandchildren, aunts, uncles, cousins, co-workers, friends, and neighbors.

Initially after September 11, 2001, it was a priority of our Nation to prevent terrorists who would do Americans harm from boarding flights that could lead to another 9/11 catastrophe. The Transportation Security Administration, or TSA, was created in that era for that purpose, and has been indispensable ever since.

Over the 20 years since enactment of the Homeland Security Act, the mission of the Department of Homeland Security has expanded to include cyber defense of civilian, governmental, and private-sector networks; protecting critical infrastructure in the form of the Nation's electric grid, water delivery systems, transportation networks and Federal election systems; and, most recently managing and protecting assets, operations, and personnel during the COVID–19 pandemic.

The committee's annual hearings on Worldwide Threats to Homeland Security have covered a range of topics from activities of foreign terrorist organizations like al-Qaeda and ISIS, to home-grown violent extremism perpetrated by lone wolves and white supremicists.

Today's government witnesses will provide insight into terrorism threats and how the Federal Government is addressing those threats to protect the homeland.

The nearly 3,000 people who died on September 11, 2001 who were the initial driving force of our committee will always be central to our focus and actions, so as to prevent another attack on United States soil.

This hearing provides Members of the committee with the opportunity to reflect on the past, and to take a hard look at the present day, to acknowledge the real threats we face from domestic terrorism.

My primary domestic security concerns are how to protect the Nation by:

- preventing foreign fighters and foreign-trained fighters from entering the United States undetected;
- countering domestic and home-grown violent extremism;
- preserving Constitutional rights and due process for all persons;
- addressing the uncontrolled proliferation of assault weapons;
- sensible gun legislation to prevent mass shootings;
- protecting critical infrastructure from physical and cyber attack;
- creating equity and fairness in our Nation's immigration policies; and
- strengthening the capacity of the Department of Homeland Security and the Department of Justice to meet the challenges posed by weapons of mass destruction.

The list of 2022 threats to the homeland is further expanded to include:
- emerging threats of viral pandemics;
- rapid onset of the effects of climate change;
- political violence fueled by misinformation and disinformation;
- the rise of extremist right-wing militia groups like QAnon and Boogaloo—that act on misinformation, disinformation, and conspiracy theories; and
- efforts by terrorist groups to reemerge or reorganize following our Nation's efforts in battling ISIS and al-Qaeda.

EMERGING VIRAL THREATS

As you recall, Chairman Thompson, on March 11, 2020, the World Health Organization declared that COVID–19 was a pandemic, which had by that date reached at least 114 countries, sickening over 100,000 people, and killing more than 4,000 people.

We have traveled a long road since that time, developing vaccines, treatments, and strategies to stop the spread of the virus. Tragically, prior to the innovation and implementation of remedial measures, the coronavirus claimed over 1 million American lives and over 6 million lives globally.

Today, over 220 million Americans, or 68 percent of the U.S. population, are considered fully vaccinated, enabling life to return to close to normal pre-pandemic conditions. This success has proven that, by working together, we can protect ourselves from viral threats.

However, we cannot let our guard down.

We must continue to present the public with opportunities—and encourage them—to take the booster vaccines and to urge people with co-morbidities to continue to wear masks and to use social distance.

We must implement the lessons learned from the COVID–19 pandemic and put them into action to prevent future epidemics.

There are other viral threats like monkeypox, that if left unchecked, threaten to become the next pandemic.

In addition to monkeypox, this year's flu season is expected to be one of the worst on record because people are coming out of quarantine without getting a flu shot.

We must continue to develop vaccines and treatments, and work together to stop the spread of these and other diseases.

It's important that we also remain vigilant against emerging viral threats.

THREATS TO DEMOCRACY: PARAMILITARY GROUPS, THREATS AND ACTS OF VIOLENCE

There is no question that threats to democracy in the United States continue to grow.

Since the 2016 Presidential election, there has been a dramatic increase in the number of conspiracy theories circulating on-line. Many of these theories have been promulgated by groups like QAnon that prey on the uninformed, trade in fabrications, and are fueled by paranoia.

In 2019, the FBI issued an Intelligence Bulletin that designated QAnon as a "domestic terror threat" because of its potential to incite extremist violence.

On January 6, 2021, a violent mob of rioters stormed the U.S. Capitol in an attempt to overturn the results of the 2020 Presidential election. In the midst of the chaos, House Speaker Nancy Pelosi was targeted by the mob. They broke into her office, vandalized it, and defiled the Capitol.

In the past few weeks, Paul Pelosi, the husband of Speaker Nancy Pelosi, was violently attacked by an assailant who stated that he viewed Speaker Pelosi as "'leader of the pack of lies told by the Democratic Party" and that he wanted "to use Nancy to lure another individual".

This violence and the threats of violence against elected officials and their families are a heinous attempt to hold democracy hostage.

Violence is intended to suppress participation in the democratic process, but we can never allow it to negate the voice of the people.

In recent years, there have been a number of paramilitary groups have been stockpiling weapons and preparing for violence.

The New York Times reports that of the more than 440 extremism-related murders committed in the past decade, more than 75 percent were committed by right-wing extremists, white supremacists, or anti-Government extremists.

The threats against Members of Congress are more than 10 times as numerous as they were just 5 years ago.

These incidents are a stark reminder that conspiracy theories can have very real and—very dangerous consequences. If left unchecked, they could pose a serious threat to democracy in the United States.

Other brands of ideological extremism are being proliferated by groups that call themselves Oath Keepers, the Proud Boys, the Boogaloo Bois, the Three Percenters, the Wolverine Watchmen.

Some of these groups equate themselves. to militias, reminiscent of the Ku Klux Klan that used diabolical deceit and self-glorification to terrorize Black Americans and others to achieve oppressive ends.

GEOPOLITICAL THREATS: RUSSIA'S WAR AGAINST UKRAINE, COMPETITION FROM CHINA, CYBER HACKS

Not only must we remain cognizant of domestic threats, we must also recognize that several geopolitical threats are urgent.

In particular, peer competition from China and the Russian war with Ukraine pose serious challenges to our security.

Russia increasingly shows its unwillingness to accept global norms, not only militarily but also by its cyber intrusions. Russia is well-known to have repeatedly interfered with elections and democratic processes in many countries, perhaps most obviously by their cyber hack of the Democratic National Committee.

This attack not only exposed sensitive information, but it also undermined public trust in our Government and elections.

China has been especially notorious for its cyber hacking of corporate America, and stealing trade secrets with which it reverse-engineers our products and leverages an unfair economic edge in global trade.

Both countries have sophisticated cyber hacking capabilities.

Once in our systems, Russian and China can remain in the systems for years expanding their access and going undetected.

We must be vigilant in defending our homeland against these threats.

We must continue to invest in our cybersecurity infrastructure.

GLOBAL CLIMATE CHANGE: WINTER STORM URI AND INFRASTRUCTURE

Global climate change continues to cause extreme weather events that highlight the urgent need for action.

"Winter Storm Uri" is a stark reminder of the devastation that extreme weather can cause. Not only did the storm lead to wide-spread power outages and water shortages, it also caused billions of dollars in damage to infrastructure.

Winter Storm Uri was one of the most severe winter storms to hit Texas in recent memory. From February 13–17, 2021, the storm caused wide-spread damage and power outages across the State. In some areas, temperatures dropped below freezing for extended periods of time, causing pipes to freeze and burst.

I have seen first-hand, and hear from my constituents, the devastating effects caused by flooding from major hurricanes, and their destruction of whole homes and neighborhoods, as inflicted by Hurricane Harvey.

While the physical and economic damage caused by Hurricane Harvey was staggering, nearly the emotional toll of the storm was equally severe. Many people are still struggling to cope with the loss of loved ones and homes.

We must invest in more resilient infrastructure and develop smarter strategies to confront climate change, which intensifies each of the natural disasters that occur. Only by taking these steps can we hope to minimize the damage caused by future storms.

BATTLE TO DEFEAT ISIS AND AL-QAEDA

We must never forget this committee's origins: September 11, when 2,977 men, women, and children were murdered by 19 hijackers. Those of us serving in Congress then did not know if there was another plane heading our way.

Yet, in the true spirit of Americans, we stood on the East Front steps of the Capitol later that day—150 Members of Congress—singing, with unity and purpose, "God Bless America."

The American people needed to know that their Government was still here ready to serve and protect them from harm.

We did not have a President of the United States dividing Americans and pitting us against each other with wild conspiracies or aggravating old wounds based upon race, ethnicity, or religion.

We needed unity and we received it. It made us stronger together.

Over the past two decades, we have learned a great deal . . . and have also forgotten much of what we, as a Nation, learned. The United States is stronger when unified, and this committee's mandate includes rooting out the forces that divide us.

Those who wish to do us harm can come from any race, religion, ethnicity, or political persuasion.

We are better when we are one nation prepared to face these challenges against a common foe.

That sense of unity has been under assault by forces within and outside of the country.

I look forward to the testimony of today's witnesses and the question and answer opportunity that will follow.

Thank you. I yield back the remainder of my time.

Chairman THOMPSON. Members are also reminded that the committee will operate according to the guidelines laid out by the Chairman and Ranking Member in our February 3, 2021 colloquy regarding remote procedures.

I welcome our panel of witnesses.

Our first witness is Alejandro Mayorkas, Secretary of Homeland Security. Our next witness will be Christopher Wray, director of the Federal Bureau of Investigation. Our third and final witness will be Christine Abiziad, director of the National Counterterrorism Center.

Without objection, the witnesses' full statement will be included in the record.

I now ask Secretary Mayorkas to summarize his statement for 5 minutes.

STATEMENT OF ALEJANDRO MAYORKAS, SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Secretary MAYORKAS. Chairman Thompson, Ranking Member Katko, distinguished Members of this committee, thank you for inviting me to join you today.

Next week marks the 20th anniversary of the Homeland Security Act being signed into law. This Act brought together many components of the Federal Government to safeguard the United States against foreign terrorism in the wake of the devastation wrought on September 11, 2001. It remains the largest reorganization of the Federal Government's national security establishment since 1947. It is a testament to the great threat we faced as a Nation from terrorism brought to our shores by foreign actors and foreign terrorist organizations.

Congress created a department that has significantly reduced the foreign terrorism threat posed to the homeland.

Chairman THOMPSON. Mr. Secretary, will you pull your mic a little closer to you?

Secretary MAYORKAS. How is that?

Chairman THOMPSON. Well—all right. Let us hear how that goes.

Secretary MAYORKAS. Congress created a department that has significantly reduced the risk foreign terrorism poses to the homeland by increasing our capacity to prepare for and respond to those events.

Foreign terrorist organizations remain committed to attacking the United States from within and beyond our borders. They use social media platforms to amplify messaging intended to inspire attacks in the homeland. They have adapted to changing security environments, seeking new and innovative ways to target the United States. The evolving terrorism threat to the homeland now includes lone actors fueled by a wide range of violent extremist ideologies and grievances, including domestic violent extremists, U.S.-based individuals who seek to further political or social goals wholly or

in part through violence, without direction or inspiration from a foreign terrorist group or foreign power.

From cyber attacks on our critical infrastructure to increasing destabilizing efforts by hostile nation-states, the threats facing the homeland have never been greater or more complex. Flouting internationally-accepted norms of responsible behavior in cyber space, our adversaries, hostile nations and non nation-state cyber criminals, continue to advance in capability and sophistication. Their methods vary, but their goals of doing harm are the same. Hostile nations like Russia, the People's Republic of China, Iran, and North Korea, and cyber criminals around the world, continue to sharpen their tactics and create more adverse consequences. Their ransomware attacks target our financial institutions, hospitals, pipelines, electric grids, and water treatment plants attempting to wreak havoc on our daily lives. They exploit the integrated global cyber ecosystem to sow discord, undermine democracy, and erode trust in our institutions, public and private.

These cyber operations threaten the economic and national security of every American and many others around the world. In particular, China is using its technology to tilt the global playing field to its benefit. They leverage sophisticated cyber capabilities to gain access to the intellectual property, data, and infrastructure of American individuals and businesses. Russia's unprovoked invasion of Ukraine intensified the risk of a cyber attack impacting our critical infrastructure earlier this year. Nation-state aggression is creating a heightened risk of chemical, biological, radiological, and nuclear-related threats to Americans as well.

While fast-emerging technologies, like unmanned aerial systems, artificial intelligence, internet communications, and cryptocurrencies are helping societies be more productive, creative, and entrepreneurial, they also are introducing new risks. Transnational criminal organizations are deploying these technologies to commit a wide array of crimes as they continue to grow in size, scale, sophistication, and lethality.

With respect to unmanned aerial systems in particular, it is vital that Congress act before the end of this year to extend our C–UAS authorities in order to protect the American people from malicious drone activity.

The risk of targeted violence perpetrated by actors abroad and at home is substantial. Emerging technology platforms allow individuals and nation-states to fan the flames of hate and personal grievances to large audiences and are encouraging people to commit violent acts. Those driven to violence are targeting critical infrastructure, soft targets, faith-based institutions, institutions of higher education, racial and religious minorities, government facilities and personnel, including law enforcement and the military and perceived ideological opponents.

Addressing these threats requires a whole-of-society approach across Federal, State, and local governments, the private sector, nonprofits, academia, and most importantly, every citizen.

Congress may not have predicted the extent of today's threat environment when our department was created 20 years ago, but our mission has never been more vital, our components have never collaborated more closely, our extraordinary work force has never

been more capable, and our Nation has never been more prepared. We must harness the same deliberative and bipartisan spirit in which this department was created to combat the vast threats Americans face today.

I look forward to answering your questions.

[The prepared statement of Secretary Majorkas follows:]

PREPARED STATEMENT OF HON. ALEJANDRO N. MAYORKAS

NOVEMBER 15, 2022

Chairman Thompson, Ranking Member Katko, and distinguished Members of this committee: Thank you for inviting me to join you today. Next week marks the 20th anniversary of the Homeland Security Act being signed into law, which brought together many components of the Federal Government in a determined National effort to safeguard the United States against foreign terrorism in the wake of the devastation wrought on September 11, 2001. It remains the largest reorganization of the Federal Government's National security establishment since 1947 and a testament to the grave threat we faced as a Nation from terrorism brought to our shores by foreign actors and foreign terrorist organizations.

Thanks to extensive deliberation and cooperation from both sides of the aisle, Congress created a department that significantly reduced the risk foreign terrorism poses to the homeland by increasing our capacity to prepare for and respond to those events. However, foreign terrorism remains a persistent threat that DHS combats every day. Foreign terrorist organizations remain committed to attacking the United States from within and beyond our borders. They use social media platforms to amplify messaging intended to inspire attacks in the homeland and have adapted to changing security environments, seeking new and innovative ways to target the United States. Foreign terrorists will continue to expand their networks, cross international borders, raise funds, and organize to improve their ability to target the homeland.

Rapidly emerging technologies, evolving cyber capabilities, and increasing economic and political instability around the world are contributing to a heightened threat environment at home. From cyber attacks on our critical infrastructure and increasing destabilizing efforts by hostile nation-states, to the rise of domestic violent extremism, the threats facing the homeland have never been greater or more complex.

Flouting internationally-accepted norms of responsible behavior, transparency, and accountability in cyber space, our adversaries—hostile nations and non-nation-state cyber criminals—continue to advance in capability and sophistication. Their methods vary, but their goals of doing harm are the same. Hostile nations like Russia, the People's Republic of China (PRC), Iran, North Korea, and cyber criminals around the world continue to sharpen their tactics and create more adverse consequences. Their ransomware attacks target our financial institutions, hospitals, pipelines, electric grids, and water treatment plants to wreak havoc on our daily lives. They exploit the integrated global cyber ecosystem to sow discord, undermine liberal democracy, and erode trust in our institutions, public and private. These cyber operations threaten the economic and National security of every American, and many others around the world.

In particular, the PRC is using its technology to tilt the global playing field to its benefit. They leverage sophisticated cyber capabilities to gain access to the intellectual property, data, and infrastructure of American individuals and businesses. Russia's unprovoked invasion of Ukraine intensified the risk of a cyber attack, impacting our critical infrastructure earlier this year. Nation-state aggression is creating a heightened risk of chemical, biological, radiological, and nuclear-related threats to Americans as well.

Fast-emerging technologies like unmanned aerial systems, artificial intelligence, internet communications, and cryptocurrencies are helping societies be more productive, creative, and entrepreneurial. They also are introducing new risks. Transnational criminal organizations are deploying these technologies to commit a wide array of crimes as they continue to grow in size, scale, sophistication, and lethality.

The risk of targeted violence, perpetrated by actors abroad and at home, is substantial. Emerging technology platforms allow individuals and nation-states to fan the flames of hate and personal grievances to large audiences and are encouraging people to commit violent acts. Those driven to violence are targeting critical infrastructure; soft targets such as sports venues, shopping malls, and other mass gath-

erings; faith-based institutions, such as churches, synagogues, and mosques; institutions of higher education; racial and religious minorities; Government facilities and personnel, including law enforcement and the military; and perceived ideological opponents.

Addressing these threats requires a whole-of-society approach across Federal, State, and local governments, the private sector, nonprofits, academia, and—most importantly—every citizen. Congress may not have predicted the extent of today's threat environment when our Department was created 20 years ago, but our mission has never been more vital, our components have never collaborated more closely, and our Nation has never been more prepared. We must harness the same deliberative and bipartisan spirit in which this Department was created to combat the vast threats Americans face today.

COMBATING TERRORISM AND TARGETED VIOLENCE

Foreign Terrorism Threats

Since the inception of this Department, the threat landscape has evolved dramatically, and DHS has remained vigilant against all terrorism-related threats to the homeland. In the years immediately following the September 11 terrorist attacks, the Department focused on foreign terrorists located overseas who sought to harm us within our borders and threaten our interests abroad. This focus evolved to include home-grown violent extremists (HVEs): Individuals in America whose ideologically-motivated terrorist activities are primarily inspired by Foreign Terrorist Organization's (FTOs) political or social objectives.

Our assessments indicate that FTOs will maintain a highly-visible presence online and prioritize messaging focused on inspiring HVEs to conduct attacks in the United States. Media branches of al-Qaeda and the Islamic State of Iraq and ash-Sham (ISIS) have continued to celebrate perceived victories over the United States pointing to the September 11, 2001 terrorist attacks on their anniversaries and the U.S. military withdrawal from Afghanistan to encourage the use of violence by their supporters. ISIS media and its supporters have also sought to revitalize ISIS's image as a global enterprise and to portray the group as the true vanguard of resistance against the United States and its allies. ISIS and its supporters continue to call for attacks in the United States, and supporters often share on-line tactics and techniques for reducing the likelihood of being detected by law enforcement.

Some terrorist-associated individuals maintain a presence in the Western Hemisphere, and could be leveraged to support extremist activities, possibly involving the homeland. For example, al-Qaeda-associated individuals in Brazil are involved in financial support through businesses they manage in the country, transferring funds in support of extremist-related activities, and involved in the printing and purchasing of counterfeit currencies in support of al-Qaeda's global efforts.

We continue to see Iran and its partner, Lebanese Hezbollah, pose an enduring threat to the homeland, evidenced by Iran's public statements threatening retaliation in the United States for Islamic Revolutionary Guard Corps Quds Force (IRGC–QF) Commander Qasem Soleimani's death and historical arrests of IRGC and Hezbollah members plotting operations in the United States. In the past several years, U.S. law enforcement has arrested numerous individuals for spying on Iranian dissidents in the United States and for acting as agents of influence for the Iranian Government. In August, Federal prosecutors unsealed charges against an IRGC member for plotting to assassinate a former U.S. official. Given its capabilities, Iran could advance an attack plot targeted at the United States with little to no warning. DHS continues to work closely with other law enforcement agencies and the intelligence community to stay aware of on-going threat streams and take preventative actions as appropriate.

DHS works closely with our law enforcement, National security, and intelligence community partners to improve our ability to identify individuals who pose a National security or public safety threat and who seek to travel to the United States or receive an immigration benefit. In fiscal year 2022, the National Vetting Center (NVC), managed by DHS, enhanced its ability to support vetting for DHS and Department of State. Through technology advancements, the NVC has increased efficiencies in vetting processes, improving our ability to identify potential threats. We continue to build partnerships with foreign governments, to include increasing our information sharing and vetting capabilities. DHS is increasing our ability to engage in biometric comparison with our foreign partners, and most recently amended requirements for the Visa Waiver Program (VWP) to require participation in the Enhanced Border Security Partnership (EBSP). Under EBSP, DHS will be able to conduct biometric checks against VWP member countries' biometric data to authen-

ticate VWP travelers' identities to quickly receive immigration and criminal history information.

As a key part of the interagency approach to countering these threats, DHS provides timely and accurate intelligence to the broadest audience at the lowest classification level possible. DHS will continue to leverage our deployed intelligence professionals to ensure the timely sharing of information and intelligence with our State, local, Tribal, and territorial (SLTT) partners, including the National Network of Fusion Centers, in accordance with applicable law and DHS privacy, civil rights, civil liberties, and intelligence oversight policies.

Domestic Violent Extremism and Targeted Violence

The evolving terrorism threat to the homeland now also includes those fueled by a wide range of violent extremist ideologies and grievances, including domestic violent extremists (DVEs). DVEs are U.S.-based individuals who seek to further political or social goals wholly or in part through violence, without direction or inspiration from a foreign terrorist group or foreign power. These actors are motivated by various factors, including biases against racial and religious minorities, perceived Government overreach, conspiracy theories promoting violence, and false or misleading narratives often spread on-line. Today, these U.S.-based individuals, who are inspired by a broad range of violent ideologies, pose the most significant and persistent terrorism-related threat to the homeland.

The intelligence community assesses that racially or ethnically motivated violent extremists (RMVEs), who advocate for the superiority of the white race, and militia violent extremists (MVEs), a component of the anti-Government/anti-authority violent extremism threat category, present the most lethal DVE threat in the homeland. In many cases, DVE actors have spent inordinate amounts of time on-line viewing extremist, violent materials and engaging with like-minded individuals. RMVEs are the DVE actors with the most persistent and concerning transnational connections, because individuals with similar ideological beliefs exist outside of the United States. These RMVEs communicate with and seek to influence each other. Such connectivity with overseas violent extremists might lead to a greater risk of U.S. RMVEs mobilizing to violence.

A June 2022 DVE assessment[1] by DHS, the Federal Bureau of Investigation (FBI), and the National Counterterrorism Center (NCTC) determined that the threat from DVEs is likely to persist for the coming months, with heightened tensions surrounding the 2022 elections, continued perceptions of Government overreach, and immigration-related developments or potential new legislation and court rulings; all presenting potential flashpoints that could serve to encourage or inspire acts of violence.

To prepare for this threat, the Department has embraced a community-based approach to prevent terrorism and targeted violence by building trust, partnerships, and collaboration across every level of government, the private sector, non-governmental organizations, and the communities we serve, while respecting First Amendment protections. We focus on reducing the threat of violence. We must make it harder to carry out an attack and reduce the potential for loss of life by preventing mobilization to violence.

DHS's Center for Prevention Programs and Partnerships (CP3) is at the forefront of the Federal Government's prevention efforts. Established in 2021, CP3 provides technical, financial, and educational assistance to help communities build local prevention capabilities. In addition to supporting State-level prevention strategies, CP3 supports local efforts to establish community support systems—bringing together mental health providers, educators, faith leaders, public health officials, social service providers, nonprofits, public safety officials, and others—to create programs that connect individuals with the help they need. CP3 relies on the expertise of DHS's Privacy and Office for Civil Rights and Civil Liberties professionals to ensure all public-facing prevention resources, web content, and training materials are protective of Americans' privacy rights and civil rights and civil liberties.

As part of this effort, DHS has invested more than $50 million over the past 3 years in communities across the United States, to help prevent acts of targeted violence and terrorism through the Targeted Violence and Terrorism Prevention (TVTP) Grant Program. DHS recently announced 43 TVTP grant awards to entities in 20 States, totaling $20 million, for fiscal year 2022. Managed by CP3 and the Federal Emergency Management Agency (FEMA), the TVTP Grant program provides funding for State, local, Tribal, and territorial (SLTT) governments, nonprofits, and institutions of higher education, to establish or enhance capabilities to prevent

[1] DHS, NCTC, FBI, June 17, 2022 *(U) Wide-Ranging Domestic Violent Extremism Threat to Persist.*

targeted violence and terrorism. This year's awards fulfill the grant program's focus on prioritizing the prevention of domestic violent extremism, as well as efforts to counter mobilization to violence that occurs on-line, while respecting privacy, civil rights, and civil liberties.

DHS provides security funding to support facility hardening and other operational and physical security enhancements for nonprofit organizations at risk of terrorist attacks through the Nonprofit Security Grant Program (NSGP). I am grateful that this critically important program has seen a funding increase this past fiscal year of $70 million from fiscal year 2021 levels, for a total of $250 million. The fiscal year 2023 President's Budget request proposes another increase to $360 million.

These funds are in addition to the resources provided by DHS to our State and local partners through the Homeland Security Grant Program (HSGP), in which DHS has designated "Combating Domestic Violent Extremism" as a "National Priority Area" for both fiscal year 2021 and fiscal year 2022. This means that between fiscal year 2021 and fiscal year 2022, States and local governments across our Nation will spend over $111 million in grant funding on capabilities to detect and protect against these threats.

Through the Presidential Threat Protection Act of 2000, Congress formally authorized the U.S. Secret Service (USSS) to establish the National Threat Assessment Center (NTAC) to conduct research, training, and consultation on threat assessment and the prevention of targeted violence. NTAC leads the field of targeted violence prevention by producing world-class research examining all forms of targeted violence, including domestic terrorism, mass-casualty attacks, and attacks against K–12 schools. NTAC's experts provide training and guidance for professionals from a wide range of agencies and institutions on establishing threat assessment frameworks and targeted violence prevention programs unique to their organization's missions and needs. In fiscal year 2022, NTAC delivered over 280 trainings and briefings to over 28,000 participants, including State and local law enforcement, government officials, educators, mental health professionals, faith-based leaders, and workplace security managers. The number of events and participants reached by NTAC in fiscal year 2022 represent the highest totals in the Center's history.

DHS's Cybersecurity and Infrastructure Security Agency (CISA) works closely with public and private-sector partners to build security capacity to mitigate cyber and physical risks, including threats posed by terrorism and targeted violence. Through trainings, tools, exercises, and best practices, CISA supports organizations in enhancing security holistically and in countering the most prevalent threats, including active shooters. Protective Security Advisors—a cadre of more than 140 security subject-matter experts located across the country—provide direct and tangible support to facilities by conducting security assessments and advising on enhanced protective measures.

Gender-Based Violence

Gender-based violence (GBV) is any harmful threat or act directed at an individual or group based on their actual or perceived biological sex, gender identity, gender expression, sexual orientation, or difference from social norms related to masculinity or femininity. Gender-based violence is rooted in structural gender inequalities and power imbalances. The DHS Council for Combatting Gender-Based Violence (CCGBV) works to identify and build consensus and best practices around combatting GBV, including initiatives focused on domestic violence, forced marriage, female genital mutilation/cutting (FGM/C), on-line abuse and harassment, and trafficking in persons. The work of the CCGBV comes at an inflection point for the health, safety, and well-being of women and girls, as the COVID–19 pandemic has exacerbated a pre-existing "shadow pandemic" of gender-based violence, as well as economic, health, and caregiving crises that disproportionately impacted women and girls long before the pandemic struck.

Women and girls are particularly vulnerable and may be specifically targeted for acts of gender-based violence (GBV) as a part of terrorist activities, requiring specific protection measures. This includes safeguarding women's human rights during disaster and crisis situations, displacement, and other scenarios, in order to counter the effects of extremist violence. The USSS's NTAC has also identified the specific threat posed by misogynistic extremism, men who identify themselves as involuntary celibates or "incels" and target women for violence.

CYBER THREATS

Our interconnectedness and the technology that enables it—the cyber ecosystem—exposes us to a dynamic and evolving threat environment, one that is not contained by borders or limited to centralized actors, one that impacts governments, the private sector, civil society, and every individual. As a result, cyber threats from for-

eign governments and transnational criminals remain among the most prominent threats facing our Nation. Hostile nations like Russia, the PRC, Iran, and North Korea, as well as cyber criminals around the world, continually grow more sophisticated and create more adverse consequences.

Within the past 2 years, we have seen numerous cybersecurity incidents impacting organizations of all sizes and disrupting critical services, from the SolarWinds supply chain compromise to the wide-spread exploitation of vulnerabilities found in Microsoft Exchange Servers. Further, ransomware incidents—like those affecting a major pipeline company, JBS Foods, Kaseya, and CommonSpirit hospital system—continue to increase. As of February 2022, CISA, the FBI, and the National Security Agency observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, and victims in the first half of 2021 paid an estimated $590 million in ransoms, compared to $416 million over all of 2020. We continue to believe there is significant under-reporting of ransomware incidents.

Russia will likely remain a significant threat to U.S. networks, data, and critical infrastructure as it refines and employs sophisticated cyber espionage, influence, and attack capabilities, particularly in response to international pressure following its invasion of Ukraine. Russia has previously targeted critical infrastructure in the United States and allied countries to hone—and in some cases demonstrate—its ability to inflict damage during a crisis. Last February, Russia conducted a cyber attack against commercial satellite communications, impacting families and businesses across Europe.

The PRC poses a highly advanced cyber threat to the homeland. The PRC continues to leverage increasingly sophisticated, large-scale cyber espionage operations against a range of industries, organizations, and dissidents in the United States. The PRC uses cyber means to illicitly obtain U.S. intellectual property, personally identifiable information, and export-controlled information. The PRC launches cyber espionage operations against the United States via People's Liberation Army and Ministry of State Security cyber actors. PRC-backed hackers are among the most active groups targeting governments and critical infrastructure this year—including across Southeast Asia. They are the most active group targeting businesses around the globe. Just one PRC hacking group, known as APT41, has stolen intellectual property from at least 30 multinational companies in the pharmaceutical, energy, and manufacturing sectors, resulting in hundreds of billions of dollars of lost revenue.

Iran has a robust cyber program that targets networks in nearly every sector, and conducts offensive cyber operations in the United States, Israel, Saudi Arabia, and via other regional adversaries. Iranian cyber attacks recently caused severe harm to government networks in Albania, limiting access to essential services. These attacks include disruptive and destructive cyber attacks such as website defacements and data deletion. Iranian cyber espionage is a high-frequency, wide-spread threat, and Iran may choose to leverage its cyber access for disruptive or destructive attacks.

In the last 2 years alone, North Korea has largely funded its weapons of mass destruction programs through cyber heists of cryptocurrencies and hard currencies totaling more than $1 billion.

We assess that ransomware attacks targeting U.S. networks will increase in the near and long term because cyber criminals have developed effective business models to increase their financial gain, likelihood for success, and anonymity. In recent years, ransomware incidents have become increasingly prevalent among U.S. SLTT government entities, and critical infrastructure organizations, with ransom demands in 2020 exceeding $1.4 billion in the United States. The Healthcare and Public Health Sector was also a popular target for ransomware threat actors.

The Department is committed to keeping Americans safe from the devastating effects of cyber crimes. Cyber criminals' primary motivation is financial gain and criminals show little regard for whom they target. DHS's investigative components, the USSS and Homeland Security Investigations (HSI), are dedicated to stopping criminal acts, identifying and arresting the criminals, and working to seize and return stolen funds to the victims. Cyber crimes are often transnational with the criminal actors, their infrastructure, and their victims, spread across the globe. The USSS and HSI partner with Federal and SLTT law enforcement and with international and foreign law enforcement in combating cyber crimes.

It is the Department's responsibility to help protect our Nation's critical infrastructure from these attacks. The private sector, which owns and operates most of the Nation's critical infrastructure, plays a vital role in working with CISA to ensure that we are aware of new campaigns and intrusions. That awareness in turn helps CISA advise other potential victims—increasing the Nation's collective cyber defenses through our collaborative efforts.

In March 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) into law. CIRCIA marks an important milestone in improving America's cybersecurity. The information received from our private-sector partners' reports will enable CISA, along with other Federal agencies such as the FBI, to build a common understanding of how our adversaries are targeting U.S. networks and critical infrastructure. This information will fill critical information gaps and allow us to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims. We are grateful to Congress for passing this historic bipartisan legislation, marking a critical step forward in the collective cybersecurity of our Nation.

Cyber Threat Mitigation and Resilience

To respond to evolving cyber threats and increase our Nation's cybersecurity and resilience, DHS has taken several steps, including:

- In July 2021, with the Department of Justice (DOJ) and other Federal partners, DHS launched *StopRansomware.gov*—the first whole-of-Government website that pools Federal resources to combat ransomware and helps private and public organizations of all sizes mitigate cyber risk and increase their resilience.
- In August 2021, CISA announced the creation of the Joint Cyber Defense Collaborative (JCDC) to develop and execute joint cyber defense planning with partners at all levels of government and the private sector, to prevent and reduce the impacts of cyber intrusions, and to ensure a unified response when they occur.
- In February 2022, DHS launched the Cyber Safety Review Board (CSRB), a groundbreaking public-private partnership dedicated to after-action review of significant cyber threats. The CSRB published its first report this summer addressing the risk posed by vulnerabilities in the widely-used "Log4j" open-source software library.
- In February 2022, recognizing the heightened risk of malicious cyber activity related to the Russia-Ukraine conflict, CISA launched a new campaign called "Shields Up" to amplify free cybersecurity resources and guidance for how organizations of every size and across every sector can increase their cybersecurity preparedness.
- In accordance with CIRCIA, DHS established the Cyber Incident Reporting Council (CIRC) this past summer. The CIRC, which includes approximately 30 representatives from Sector Risk Management Agencies (SRMAs) and independent regulators, has convened several times to discuss opportunities to coordinate, deconflict, and harmonize Federal cyber incident reporting requirements, including those issued through regulation. To facilitate this effort, DHS has inventoried all Federal cyber incident reporting requirements and held one-on-one consultations with over 20 CIRC members.
- In September 2022, CISA and FBI launched the Joint Ransomware Task Force (JRTF) to coordinate a whole-of-Government effort to combat the threat of ransomware. A major objective of the JRTF is to coordinate efforts among Federal agencies and private-sector and SLTT partners to improve our Nation's response to ransomware incidents, including efforts to increase our Nation's cyber resiliency.
- In September 2022, the Department announced the State and Local Cybersecurity Grant Program (SLCGP) to help States, local governments, rural areas, and territories address cybersecurity risks and cybersecurity threats to information systems. In fiscal year 2022, $183.5 million was made available under the SLCGP, with varying funding amounts allocated over 4 years from the Infrastructure Investment and Jobs Act.
- In October 2022, the Department released the Cybersecurity Performance Goals (CPGs), voluntary practices that outline the highest-priority baseline measures businesses and critical infrastructure owners of all sizes can take to protect themselves against cyber threats. By clearly outlining measurable goals based on easily understandable criteria such as cost, complexity, and impact, the CPGs are designed to be applicable to organizations of all sizes.
- The disruptive ransomware attack on a major pipeline company in May 2021 revealed a continuing significant National security risk with critical vulnerabilities in the transportation sector that previous voluntary efforts did not sufficiently mitigate. Since the attack in 2021, the Transportation Security Administration (TSA) has issued security directives mandating that surface transportation owners and operators implement several critically important and urgently-needed cybersecurity measures such as designating a cybersecurity coordinator, reporting cybersecurity incidents, implementing a cybersecurity re-

sponse plan, completing a cybersecurity vulnerability assessment, and identifying cybersecurity gaps. TSA recently updated these directives to focus requirements on achieving security outcomes, rather than on prescriptive measures. Through security program amendments, TSA issued several similar requirements to larger airports and air carriers, with additional measures under consideration. DHS continues to consider what additional directive action might be necessary to address urgent cyber threats in transportation and other critical infrastructure sectors and will continue to work closely with the U.S. Department of Transportation (DOT), the U.S. Department of Energy, and other Sector Risk Management Agencies.

EMERGING TECHNOLOGY THREATS

Unmanned Aircraft System (UAS) Threats

The rapid proliferation of drones and their expanded utilization by hobbyists, professionals, and threat actors have required DHS to shift its response efforts to mitigate smaller, more agile, and less attributable dangers across all its mission areas, while still supporting the lawful use of these advanced technologies within our Nation. Drones have conducted kinetic attacks with payloads of explosives or firearms, caused dangerous interference with manned aviation, disrupted airport operations (causing significant economic harm), disrupted and damaged critical infrastructure, and nearly every day, transnational organized criminal organizations (TCOs) use drones to convey illicit narcotics (including fentanyl) and contraband across U.S. borders and conduct hostile surveillance of law enforcement.

Congress extended the law that provides DHS's current counter-UAS (C–UAS) authority through December 16, 2022, under the continuing resolution. Ensuring that the existing authority does not lapse, and the C–UAS activities currently being performed by DHS do not cease, are critically important to our missions protecting the President and Vice President, along the Southwest Border, securing sensitive Federal facilities, and safeguarding the public. DHS has successfully executed C–UAS operations at mass gatherings and Special Security Assessment Rating (SEAR) and National Special Security Events (NSSEs), including the 2022 World Series, the Super Bowl, the Indianapolis 500, the U.N. General Assembly, the Democratic and Republican National Conventions, and the State of the Union address. At all times, DHS engages in these activities in a manner that protects individuals' privacy, civil rights, and civil liberties consistent with the requirements of the current law and DHS policy.

To ensure that the Department can continue its C–UAS activities, the administration has requested that Congress pass a 2-year, clean extension of existing C–UAS authorities in the NDAA or another legislative vehicle before these authorities expire. Any lapse in or narrowing of DHS's C–UAS authority would entail serious risks for homeland security, as DHS would have to cease or curtail existing C–UAS operations that protect the homeland, including at the Southern Border where drones are being used to traffic fentanyl and other dangerous contraband. Rather, the authority should be expanded to address critical gaps in the current law, such as a lack of protection for U.S. airports from drones, the lack of authority for DHS to partner with State, local, Tribal, and territorial law enforcement, enabling them to detect and mitigate threats themselves, and the inability of critical infrastructure owners and operators to detect drones operating near their facilities or request Federal mitigation assistance.

Congressional action is urgently required, as DHS's authority to detect and counter drone threats will expire on December 16, 2022. A lapse in this authority could have catastrophic implications for homeland security.

5G/6G

In the cyber ecosystem—which underpins the unprecedented interconnectedness we've achieved as a Nation and across the globe—emerging technology and innovation can also expose us to a dynamic and evolving threat environment. For example, communications advancements in 5G and 6G technology continue to be a high security priority for the Department.

The PRC is using its technology to tilt the global playing field to its benefit, capitalizing on the world-wide demand for communications technology and luring customers with improved telecommunications networks at a low cost. However, Beijing often requires large PRC-based companies to share and store data from their networks in-country and to provide that data to the Government when requested by authorities. It is our belief that our essential telecommunications networks should not be owned or operated by companies who will either sell or provide information to a foreign government, and we are championing to international partners that

cheap telecommunications technology is not worth the price of citizens' privacy, their national security, or their sovereignty.

For several years, DHS has worked closely with the interagency efforts to secure 5G and to mitigate possible malicious use by PRC technology. At CISA, our 5G team provided supply chain risk analyses that were a significant contribution to the Federal Government's response to this issue. However, today we are looking beyond 5G to the next frontier in 6G. 6G is still around 8–10 years away but the process to create the standards for 6G roll out is beginning today. This is a technology standardization process that has geopolitical implications as Beijing is already positioning itself to dominate the standards process. We see this as a potential threat to our homeland and economic security and are taking steps to educate our partners about the importance of this issue.

Cryptocurrency

While most cryptocurrency is used legitimately, cryptocurrency has attributes that have already been exploited by criminals, terrorists, and adversaries to facilitate their operations. Most notably, as it has become easier to access and more widely used in general commerce, many transnational ransomware operations are using the cryptocurrency ecosystem to obfuscate illicit requests and receipt of ransoms.

Many components within DHS are focused on the rising illicit use of digital assets, developing and providing training, investigating, collaborating with interagency partners, and conducting research. Pursuant to the President's Executive Order 14067, Responsible Development of Digital Assets, the Department contributed to the whole-of-Government effort to address concerns with respect to digital assets.

For example, with domestic and international law enforcement partners, the U.S. Secret Service has achieved notable successes in combatting cyber-enabled financial crimes, including dismantling two centralized virtual currency providers that supported extensive criminal activity and successfully investigating a Russia-based criminal scheme attempting to defraud cryptocurrency exchange customers of $16.8 million.

U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) has offices in over 50 countries and works to combat cyber crimes, including through training to international partners and analytical assistance in tracing digital assets. HSI investigations related to virtual assets have risen from one criminal investigation in 2011 to over 530 criminal investigations in fiscal year 2022—seizing over $4 billion in virtual assets this last fiscal year. HSI has also trained law enforcement partners in more than 20 countries on dark web and cryptocurrency investigations, and regularly works with victims to remediate vulnerabilities before they are exploited.

Artificial Intelligence (AI)

AI encompasses several different technologies, notably natural language processing, computer vision, generative AI, and more. It is imperative for DHS to take a proactive role in the use of AI systems and to contribute to the National conversation on the secure use of this transformative technology. Malicious actors are using increasingly advanced AI, powered by more data, increasingly accessible computing resources, and advancements in machine learning algorithms. Our own prudent use of AI can help us more effectively and efficiently accomplish our mission to secure the homeland.

- Over the past several years, DHS has been engaged in AI conversations across the Federal Government on AI ethics, governance, and use policies.
- We are taking a strategic approach to mitigate and counter adversary AI efforts by tracking evolving adversary AI capabilities that could be used to exploit or overcome security measures at our physical borders, in cyber space, in election systems, and beyond.
- We are working with other responsible partners—domestically and internationally—on sharing best practices and developing standards.

Quantum

The future development of quantum computers capable of breaking current cryptography presents a tremendous threat to the way we store and move sensitive Government, critical infrastructure, financial, and personal data. DHS recognized this threat and established a productive partnership with the National Institute for Standards and Technology (NIST) within the Department of Commerce to produce actionable steps that our critical infrastructure and State, local, Tribal, and territorial (SLTT) partners can take to prepare themselves for the coming transition to new post-quantum cryptographic algorithms. DHS played a leading role in reflecting this work—and complementary efforts—in the whole-of-Government and whole-of-

society effort on quantum computing captured in the President's recent National Security Memorandum on quantum computing.

Smart Cities and Connected Communities

The convergence of a number of emerging technologies such as 5G, Internet of Things, AI, and cloud computing in our municipalities is creating exciting opportunities for efficient transportation, equitable delivery of Government services, and energy efficiency in the form of "connected communities." This issue presents a unique cybersecurity challenge for critical infrastructure, with the introduction of potentially tens of thousands of new internet-connected devices. DHS has been working this issue for over a year to ensure that our municipalities, large and small, can capitalize on this impressive technology in a safe and secure manner.

TRANSNATIONAL CRIMINAL ORGANIZATIONS

Transnational Criminal Organizations (TCOs) continue to pose a threat to the United States, particularly U.S. public health, as well as our economic and National security. Over recent years, they have grown in size, scale, sophistication, and lethality. According to a 2018 estimate, the U.S. Treasury Department estimated drug-related crime alone generated over $100 billion in proceeds in the United States. These profits also come with a high toll on human life; the opioid drugs these TCOs traffic were responsible for the majority of the over 100,000 U.S. overdose deaths between April 2020 and April 2021, according to CDC reporting. Mexico-based TCO criminal activity is not limited to drug trafficking; they engage in wide variety of other criminal activity. TCOs also facilitated and profited from smuggling migrants into the United States and their illicit trade activity led to the seizure of over $2.14 billion in Intellectual Property violations in fiscal year 2021. TCOs are adept at changing their illicit drug supply chains, shifting human smuggling routes and tactics, and using various money-laundering techniques to evade law enforcement. TCOs operating in Mexico, specifically the Sinaloa Cartel and New Generation Jalisco Cartel, almost certainly will continue to dominate illegal drug trafficking—including trafficking of methamphetamine, fentanyl, cocaine, and heroin—into the United States.

Other TCOs, some working with Mexico-based TCOs, also pose a growing threat to the homeland. TCOs in the PRC launder money for or sell precursor chemicals to TCOs in Mexico, while Central American gangs, such as Mara Salvatrucha (MS–13) and the 18th Street Gang, largely serve as cross-border couriers, smuggling drugs and people for Mexico-based TCOs. Asia-, Africa-, and Balkans-based TCOs are involved in a range of criminal activities that affect the homeland, such as money laundering, financial fraud, human smuggling, and racketeering.

To confront TCOs and other threat networks, DHS has embraced an approach that leverages U.S. Customs and Border Protection (CBP)'s unique authorities, data holdings, Intelligence Enterprise, and interagency partnerships to illuminate, disrupt, degrade, and dismantle networks that pose a threat to the homeland and its interests. CBP's international collaboration and integration with the interagency optimizes the collective global effort, which identifies options for intelligence-driven, risk-mitigating responses. Our success at identifying, degrading, and disrupting transnational networks relies on CBP front-line agents, officers, trade, and intelligence professionals working hand-in-hand with the whole of Government, as well as international partners. Developing these relationships and capabilities enables CBP to proactively identify and stop threats before they arrive at U.S. borders.

Counternarcotics

DHS employs a multi-layered approach to countering narcotics trafficking. The shift in the illicit drug market toward synthetic drugs, primarily fentanyl, its analogues, and other opioids, led CBP to develop and implement the CBP Strategy to Combat Opioids. With the support of Congress, CBP continues to make significant investments and improvements in drug detection and interdiction technology to detect the presence of illicit drugs, including illicit opioids, in all operating environments. CBP's extended border and foreign operations mission involves collaborating with U.S. and international partners to conduct joint maritime operations in the source, transit, and arrival zones of the Western Hemisphere. In collaboration with Joint Interagency Task Force South (JIATF–S), CBP operates aircraft throughout North and Central America, conducting counter-narcotics missions to detect and interdict bulk quantities of illicit narcotics. CBP seized 11,200 pounds of fentanyl in fiscal year 2021 and 14,700 pounds in fiscal year 2022. This compares to 2,804 pounds in fiscal year 2019. CBP's National Targeting Center uses advanced analytics and targeting capabilities to identify critical logistics, financial, and communication nodes and exploit areas of weakness in opioid trafficking networks.

CBP seeks to prevent drug trafficking through ports of entry, which is where most drugs enter the United States. Personal vehicles remain the primary method of conveyance encountered for illicit drugs entering the country by volume over land, with notable increases within commercial truck conveyances for methamphetamine. The Non-Intrusive Inspection (NII) Systems Program deploys technologies to inspect and screen conveyances or cars, trucks, railcars, sea containers, as well as personal luggage, packages, parcels, and flat mail through either X-ray or gamma-ray imaging systems. CBP Officers use NII systems to help them effectively and efficiently detect and prevent contraband, including drugs, unreported currency, guns, ammunition, and other illegal merchandise, as well as inadmissible persons, from being smuggled into the United States, while having a minimal impact on the flow of legitimate travel and commerce.

CBP also robustly enforces the Synthetics Trafficking and Overdose Prevention (STOP) Act to prevent trafficking by mail. CBP operates within major international mail facilities to inspect international mail and parcels arriving from more than 180 countries. Additionally, CBP and the U.S. Postal Service are working to increase the amount of advance electronic data (AED) received on international mail. This advance information enables ICE and other agencies to identify networks of foreign suppliers and domestic importers that are responsible for smuggling fentanyl into the United States.

HSI also plays a critical role in countering narcotics trafficking by exchanging information, coordinating investigations, and facilitating enforcement actions with law enforcement partners abroad to deter the ability of TCOs to smuggle drugs, people, and contraband into and out of the United States. Preliminary fiscal year 2022 statistics reveal HSI conducted 11,535 criminal arrests and seized roughly 1.87 million pounds of narcotics, which included 20,980 pounds of fentanyl, in fiscal year 2022. Additionally, in fiscal year 2022, HSI agents seized more than $210 million in total currency and assets through their narcotics enforcement efforts.

One of HSI's most significant tools to combat TCOs engaged in fentanyl trafficking are the Border Enforcement Security Task Forces (BESTs). BESTs eliminate the barriers between Federal and local investigations and close the gap with international partners in multinational criminal investigations. BESTs continue to be a primary vehicle used to carry out HSI's comprehensive, multi-layered strategy to address the National opioid epidemic.

The U.S. Coast Guard (USCG) leads maritime interdictions of narcotics in the Western Hemisphere. The USCG disrupts illicit trafficking where it is most vulnerable: At sea in the transit zones, often far from U.S. shores before bulk quantities are divided for distribution. The Coast Guard is continuing to expand cooperation with partner nations in South and Central America to combat the flow of narcotics before they reach U.S. shores. In fiscal year 2022, the USCG removed approximately 140 metric tons of cocaine, 60,000 pounds of marijuana and 8 metric tons of other narcotics, including methamphetamines, fentanyl, heroin, and hashish.

The Department welcomes Congress' support for extending the statutory authority to establish and operate Joint Task Forces (JTFs). JTFs provide a direct operational coordination layer to enhance the multi-faceted challenges facing DHS. Today, JTF-East is responsible for ensuring Departmental unity of effort in the southern maritime approach to the United States and demonstrates the tangible, positive impacts that JTFs can have on enhancing DHS coordinated operations.

Human Smuggling

Migration is a hemispheric challenge, one not limited to the United States. Displacement and migration are higher than at any time since World War II. At our Southwest Border, we are experiencing historic levels of encounters. The demographics of the population have also changed, with more than triple the number of Venezuelans, Cubans, and Nicaraguans than last year, as people flee repressive governments and lack of economic opportunity. In September 2022, Venezuelans, Cubans, and Nicaraguans accounted for almost half of unique encounters at the Southwest Border—triple their share from 1 year ago. Reporting from the U.S. Agency for International Development (USAID) suggests that nearly 1 in 4 Venezuelans have fled their home since 2014, approximately 7 million people. At least 1 in 3 of those who have fled from Venezuela have settled in Colombia. Additionally, the Office of the United Nations High Commissioner for Refugees (UNHCR) has reported that Costa Rica is hosting more than 200,000 Nicaraguan migrants, equal to nearly 4 percent of their total population.

We assess that global food and water shortages, poor economic conditions, and other socio-political factors will continue to drive an increase in cross-border migration. TCOs that specialize in human smuggling increasingly exploit and financially benefit from the continued growth in global migration trends. TCOs in Mexico play

an influential role in human smuggling, increasingly facilitating illicit migration to and across the border. These groups control large sections of territory just south of the U.S. border and have traditionally taxed human smugglers to move migrants through their areas of operation.

Disrupting human smuggling is a top priority for our Department, and we have invested significant time and resources in the effort to disrupt and dismantle the TCOs that support human smuggling. In April 2022, DHS launched a first-of-its-kind effort, unprecedented in scale, to disrupt and dismantle human smuggling networks. So far, this campaign has resulted in the arrest of over 6,400 smugglers and the disruption of over 6,750 smuggling operations. This work includes raiding stash houses, impounding tractor-trailers that are used to smuggle migrants, and confiscating smugglers' communications technology.

On October 16, I wrote to the United States Sentencing Commission, urging that the guidelines for smuggling offenses be updated to address the seriousness of the offenses. According to the Sentencing Commission's own data, in fiscal year 2021, the average sentence smuggling drugs (average 74 months) was almost 5 times longer than for smuggling human beings (average of just 15 months). These lower sentences negatively affect prosecutors' ability to negotiate plea agreements and obtain co-operation of co-conspirators; as a result, human smuggling organizations survive and thrive, as key members are rarely severely penalized for their heinous crimes.

The United States cannot do this work alone; hemispheric challenges require hemispheric solutions. We are strengthening our relationships with partners in Mexico and Central and South America and taking unprecedented actions as a result. In October 2022, DHS announced joint actions with the government of Mexico, reinforcing our coordinated enforcement operations to target human smuggling organizations and bring them to justice. That campaign includes new migration checkpoints, additional resources and personnel, joint targeting of human smuggling organizations, and expanded information sharing related to transit nodes, hotels, stash houses, and staging locations.

We are matching the unprecedented migration challenge we face with unprecedented and innovative solutions to secure the border. We are surging resources and increasing efficiency, prioritizing smart border security solutions, making historic investments in technology, taking the fight to cartels and smugglers, and doing more with our regional partners than ever before. CBP has 23,000 agents and officers working along the Southwest Border and is seeking another 300 agents in the fiscal year 2023 budget request.

We have hired and contracted for over 1,000 Border Patrol Processing Coordinators to get agents back into the field to perform their essential law enforcement mission. Through the Southwest Border Coordination Center, established in February 2022, we are coordinating a whole-of-Government approach to humanely prevent and respond to increases in irregular migration by surging and coordinating our border security and law enforcement resources. We are also supporting border communities as well as interior cities—both local governments and NGO's—that are responding to a surge in migration, including through the Emergency Food and Shelter Program.

We are prioritizing smart border security solutions, grounded in evidence rather than rhetoric, and making historic investments in technology. We have incorporated mobile intake and en route processing to begin processing non-citizens in the field; integrated digital case review saving over 70,000 hours of agent time; and advanced capacity by leveraging virtual processing capabilities.

In addition to our digitization efforts, we are also installing effective technology like linear ground detection systems and automated surveillance towers. We have also made historic investments in non-intrusive inspection technology to be deployed at ports of entry to increase our interdiction of illicit drugs, because we know that traffickers seek to smuggle drugs through the ports of entry in all modes of transportation.

Trade in Counterfeit Goods and Theft of Intellectual Property

The Department continues to facilitate legitimate trade by investigating TCOs that profit from the sale of counterfeit goods and the theft of Intellectual Property (IP). To this end, HSI's Intellectual Property Rights Coordination Center (IPR Center) brings together 30 Federal and international agencies to combat IP theft. In fiscal year 2022, HSI initiated more IP theft cases; affected more criminal arrests, indictments, and convictions; and seized a higher value of counterfeit goods, more than $1.1 billion worth, than in fiscal year 2021.

HSI's Operation Chain Reaction targets counterfeit goods entering the U.S. Government supply chain, including that of the Armed Services. As an example of HSI's

impact, the agency recently indicted one of the largest importers of counterfeit network routers. These routers, worth more than $1 billion had they been genuine, were destined to sensitive end-users, including in the Department of Defense, the FBI, government aerospace contractors, and medical facilities. In another example, HSI recently secured a guilty plea from an importer of counterfeit military uniforms destined to be sold to the Department of Defense. These counterfeit uniforms failed fire-resistance testing and failed to hide the wearer's radiation levels, making them detectible to enemy optics. Had these counterfeit goods not been seized, they would have imperiled the safety of our warfighters and exposed our service members to harm.

Human Trafficking and Child Sexual Exploitation

Combatting the abhorrent crimes of human trafficking and child sexual exploitation and abuse is a top priority for the Department. These crimes target the most vulnerable among us, offend our most basic values, and threaten our personal and public safety. Nearly every component within DHS is involved in combating human trafficking. We employ a victim-centered approach across our policies and programs, striving to support and protect victims. We lead criminal investigations into sex trafficking and forced labor, with HSI initiating nearly 1,400 investigations in fiscal year 2022 alone and helping achieve hundreds of Federal and State-level convictions each year against traffickers. We develop leading-edge technologies to identify and locate victims and perpetrators. We shine a light on these dark crimes through the Blue Campaign, our signature public awareness and education effort. We train our personnel to recognize and respond to human trafficking in the course of their daily responsibilities, delivering 53 training and outreach events to 5,927 participants in fiscal year 2022. These efforts are streamlined and strengthened through the DHS Center for Countering Human Trafficking, the first Department-wide operational coordination center for combating human trafficking and the importation of goods produced with forced labor.

Combating trade in illicit goods produced with forced labor is also a critical part of our counter-trafficking mission. Recent studies estimate that upwards of 27 million people around the world are trapped in forced labor bondage, many of whom are members of racial, religious, and ethnic minority groups. Working to end these horrific practices not only promotes respect for human rights and dignity, but also benefits U.S. National security and other interests overseas. CBP is charged with rooting out forced-labor-made goods from our supply chains by preventing the entry of these illegal goods into the U.S. market. CBP carries out this mission by investigating allegations of forced labor in supply chains and, where allegations are corroborated, issuing Withhold Release Orders (WROs) and forced labor findings.

This year, DHS led the interagency Forced Labor Enforcement Task Force (FLETF) in its successful implementation of the Uyghur Forced Labor Prevention Act (UFLPA), which was enacted by Congress and signed into law at the end of 2021. Going forward, CBP will continue to enforce the new law, and DHS, as FLETF Chair, will continue to lead the interagency in updating the UFLPA enforcement strategy, including the list of entities subject to the UFLPA's rebuttable presumption.

The scope and severity of on-line child sexual exploitation and abuse (CSEA) has increased dramatically in recent years. Reports of on-line child sexual abuse material (CSAM) to the National Center for Missing and Exploited Children, the Nation's clearinghouse for CSAM, increased by more than 35 percent between 2020 and 2021 (to nearly 30 million reports), and 2022 year-to-date numbers foreshadow an even greater increase this year. Increasingly, the victims of these horrific crimes are infants and toddlers, and the abuse has become more violent. New forms of CSEA have also emerged and grown exponentially, including the live streaming of child sexual abuse and sophisticated sextortion and grooming schemes.

That is why I am redoubling the Department's efforts in this space. We are strengthening our Cyber Crimes Center (C3), including HSI's Child Exploitation Investigations Unit (CEIU), a global leader in counter-CSEA law enforcement operations. Every day, the extraordinary men and women of C3 and HSI field offices around the country and the globe work tirelessly to locate and apprehend offenders, identify and rescue victims, and share information with our partners in this fight. In fiscal year 2021, CEIU identified and/or rescued 1,177 child victims in child exploitation investigations. During this same period, CEIU arrested 3,776 individuals for crimes involving the sexual exploitation of children and helped to secure more than 1,500 convictions. In fiscal year 2022, HSI Victim Assistance Specialists assisted 3,326 victims of crimes, of which 1,138 were child exploitation victims. HSI Forensic Interview Specialists conducted 1,836 trauma-informed forensic interviews,

of which 1,238 were in support of bringing perpetrators of child exploitation crimes to justice.

We are also building policy, public-education, and strategic-engagement infrastructure to elevate and enhance the Department's counter-CSEA capabilities. DHS remains steadfast in advancing and leveraging its full breadth of authorities and resources to end these heinous crimes, and we urge you to support our efforts to expand our work to fight all forms of human trafficking and child sexual abuse.

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND EXPLOSIVES THREATS

The overall chemical, biological, radiological, nuclear and explosives (CBRNE)-related threat environment in the homeland will likely remain unpredictable over the next 12 months. Terrorists remain interested in acquiring and using WMD in attacks against U.S. interests and the U.S. homeland. Separately, factors including the spread of dual-use CBRNE-related technologies, materials, environmental change, advances in computer and related technology that lower technical barriers, and global expansion in the number and sophistication of biological laboratories will likely continue to influence threat trends in the coming years, especially the proliferation of CBRNE threats by non-state actors.

The United States assesses that Russia maintains an offensive biological weapons program and that other potential state adversaries engage in activities that raise concerns regarding compliance with the Biological Weapons Convention. Having seen the human and economic devastation resulting from the COVID–19 pandemic, our adversaries are more aware of the significance of biological threats. Additionally, a global desire to mitigate the consequences of future pandemics is likely to expand global interest in leveraging and advancing biological technology capabilities, including technologies used for biosafety and biosecurity. The dual-use nature of these capabilities complicates the ability to discern civil medical research from malign biological weapons development and heightens the risks of accidental release of biological hazards due to lacking biosafety and biosecurity.

DHS continues to monitor chemical-related threats, including the development and use of chemical weapons and the potential for non-state actors, lone actors, and criminals to pursue a range of chemical substances to use domestically. The use of chemical agents by Russia and North Korea in targeted attacks outside their borders in recent years reaffirms our commitment to monitor for and defend against similar attempts in the homeland. Similarly, chemical accidents of varying severity remain common and of enduring concern. Over time, these trends could manifest as an increased domestic threat.

Traditional radiological and nuclear threats to the homeland remain low. Due to material security and other factors, the likelihood of a large-scale radiological attack in the homeland is very low. Nevertheless, we cannot rule out the risk of unsecured or vulnerable fissile and other source materials in the United States. While the United States has expressed concern with Russian nuclear saber-rattling, we do NOT anticipate that a nuclear detonation in Europe would have any direct health consequences on the homeland.

The Countering Weapons of Mass Destruction Office (CWMD) leads the Department's efforts to safeguard the United States against CBRNE threats by collecting and analyzing CBRNE threat data, conducting risk analysis, and enhancing and implementing capabilities to prevent, detect, prepare for, and respond to the range of CBRNE incidents. This includes collaborating with Federal entities to monitor biological threats in cities across the country, providing radiological and nuclear detection equipment to SLTTC partners in urban areas, providing surge support to protect special events, and equipping DHS operational components with radiological and nuclear detection equipment to prevent smuggling at the border. Additionally, CWMD works closely with campus jurisdictions to enhance their capabilities to address these threats and ensure a coordinated, National response.

The Office of Health Security (OHS) promotes a unified approach through partnerships that protect the health of our workforce and the health security of the homeland. In the face of an ever-expanding and complex National health security mission, OHS enhances integration of Federal and SLTTC public safety and health security partners, leads the Department's engagements related to medical countermeasures prioritization and policy development, and coordinates food, agriculture, and veterinary defense activities. Recent domestic and global threats such as pandemics, supply chain disruptions, resurgence of zoonotic and transboundary diseases, climate change impacts, and cybersecurity incidents all underscore the important nexus between agro-defense, food protection, and food security with the National security, National economic security, and National public health and safety of the United States.

EXTREME WEATHER EVENTS AND CLIMATE CHANGE RESILIENCE

The impacts of climate change pose an acute and systemic threat to the safety, security, and prosperity of the United States, and have already led to changes in the environment, such as rising ocean temperatures, shrinking sea ice, rising sea levels, and ocean acidification. As our climate continues to warm, the United States will experience more climate-related disasters such as heat waves, droughts, wildfires, coastal storms, and inland flooding. This year, we have already seen the devastating impacts from Hurricane Fiona in Puerto Rico and Hurricane Ian in Florida, and Typhoon Merbok in Alaska. Natural disasters occur both seasonally and without warning, subjecting affected communities to insecurity, disruption, and economic loss. Natural disasters include all types of severe weather that have the potential to pose a significant threat to human health and safety, property, and critical infrastructure.

Preparedness and Resilience

Under the Biden-Harris administration, DHS is engaged in climate change adaptation and mitigation efforts to make the Department and the Nation more prepared, more secure, and more resilient:

- In 2021, DHS established a Climate Change Action Group (CCAG) to coordinate DHS response to climate-related Executive Orders and track implementation of actions and progress toward DHS climate change priorities. During the first year, the group was critical in coordinating a Strategic Framework to Address Climate Change and hold the first Department-wide exercise on extreme heat.
- DHS is leading the charge among Federal agencies to transition its fleet vehicles from internal combustion engines to zero-emission electric vehicles and is the first Federal agency to upfit a battery electric vehicle for law enforcement use. As the Nation's third-largest Federal agency and largest law enforcement agency, DHS has an inventory of more than 50,000 vehicles, with law enforcement vehicles making up 60 percent of its fleet.
- DHS made available more than $3 billion for the fiscal year 2022 Building Resilient Infrastructure and Communities (BRIC) and Flood Mitigation Assistance (FMA) grant programs which seek to help SLTT governments address high-level future risks to natural disasters such as extreme heat, wildfires, drought, hurricanes, earthquakes, and increased flooding to foster greater community resilience and reduce disaster suffering.
- FEMA continues to evolve mitigation grant programs to be more equitable, reduce complexity, and address climate resilience. FEMA is focused on reducing barriers to access funding faced by those who need it the most and building capacity and capability to deliver mitigation grant programs.
- FEMA announced the expansion of BRIC non-financial Direct Technical Assistance (DTA), increasing the number of communities receiving this community resilience planning and project development assistance from 20 in fiscal year 2021 to 40 in fiscal year 2022, to help communities design transformational projects that address multiple hazards and accelerate community resilience.
- FEMA has also developed a Nature-Based Solutions Guide to help communities identify and engage the staff and resources that can be used to implement nature-based solutions to build resilience to natural hazards, which may be exacerbated by climate change. Nature-based solutions can help reduce the loss of life and property resulting from some of our Nation's most common natural hazards. These include flooding, storm surge, drought, and landslides. As future conditions, like climate change, intensify these hazards, nature-based solutions can help communities adapt and thrive.

NATION-STATE THREATS

The United States faces an evolving and increasingly complex threat from nation-state adversaries, including the PRC, Russia, Iran, and North Korea, each of which views the United States as a strategic adversary. These adversaries employ a combination of traditional and non-traditional intelligence tradecraft, predatory economic and cultural outreach, and cyber and traditional espionage to seek illicit access to U.S. critical infrastructure and steal sensitive information, technology, and industrial secrets. These governments—and a growing number of others who are learning from their tactics—conduct overt and covert influence campaigns spreading misinformation and disinformation to sow and exploit divisions in our society, undermine confidence in our democratic institutions, and weaken our alliances. In some cases, they surveil, harass, and otherwise seek to suppress perceived dissidents and regime opponents overseas, including those now living in the United States.

The global availability of technologies with intelligence applications—such as biometric devices, unmanned systems, high-resolution imagery, enhanced technical surveillance equipment, advanced encryption, and big data analytics—and the unauthorized disclosure of cyber tools have enabled a wider range of actors to obtain sophisticated intelligence capabilities. Threat actors are using these capabilities against an expanded set of targets and vulnerabilities. Foreign Intelligence Entities are targeting most U.S. Government departments and agencies, to include DHS, as well as National laboratories, the financial sector, the U.S. industrial base, and other private-sector and academic entities. These activities put at risk the homeland security enterprise, as well as State and local partners, and private-sector critical infrastructure providers.

We assess that the PRC will continue to exploit professors, scholars, and students visiting the United States from the PRC as nontraditional collectors to steal sensitive information and technology. Some collectors are unwittingly providing information back to the PRC, while others are aware of their roles and have admitted to stealing research from U.S. institutions to support Chinese military ambitions. We expect the threat from these actors will increase as international students return to U.S. universities after a hiatus due to the COVID–19 pandemic.

Russia embeds intelligence officers in its diplomatic posts inside the United States. While in the United States, Russia's intelligence officers try to establish front companies and recruit Russian emigres and American citizens to steal sensitive U.S. academic, Government, and business information. Russia continues to circumvent U.S.-imposed sanctions to acquire sensitive/dual-use technology for use in military weapons and aviation industry.

We assess that for the foreseeable future, Iran probably will present an enduring counterintelligence threat to the homeland as it seeks to advance its goals in the Middle East. During the past several years, U.S. law enforcement has arrested numerous individuals for spying on Iranian dissidents in the United States and for acting as agents of influence for the Iranian government.

Election Security

The security and resilience of our Nation's election infrastructure is one of the highest priorities for DHS. As demonstrated in recent election cycles, we continue to face a wide range of threats targeting U.S. election infrastructure and voters by sophisticated, State-sponsored cyber threat actors, such as the PRC, Russia, and Iran. In many cases, the foreign threat actors who are attempting to breach our election systems are the very same ones who are conducting influence operations that seek to sow discord in our country. Their influence operations often utilize information obtained illicitly through cyber activity, or they make false or exaggerated claims of cybersecurity breaches. These foreign threat actors advance their own disinformation narratives about U.S. elections, as well as amplify existing domestic disinformation narratives. Protecting election infrastructure is a whole-of-Government effort. DHS works closely with the U.S. Election Assistance Commission (EAC), DOJ, the intelligence community, and other agencies to help accomplish this goal.

Throughout the 2022 primary and general elections, DHS has worked to ensure that election officials and their private-sector partners have the necessary information and tools to successfully manage risk and build resilience into the Nation's election infrastructure. DHS works to protect and safeguard elections by:

- *Sharing Intelligence and Information*.—DHS shares timely and actionable intelligence and information with our Federal, State, local, Tribal, and territorial government and private-sector partners about threats and risks to election infrastructure, including foreign disinformation efforts concerning elections.
- *Providing Services and Resources*.—CISA maintains an Election Security Resource Library to equip State and local governments, election officials, and others with no-cost tools they can use to secure election-related assets, facilities, networks, and systems from cyber and physical risks. This includes Cybersecurity Advisors located throughout the country and more than 100 Protective Security Advisors in all 50 States who provide cybersecurity expertise, conduct physical security assessments, and share guidance and best practices. Through 2022, CISA facilitated multiple Classified and un-Classified threat briefings, engaged thousands of election officials and SLTT partners for cybersecurity and physical security services, assessments, trainings, and tabletop exercises, including CISA's 2022 Tabletop the Vote exercise, a 3-day exercise that engaged over 1,000 stakeholders across 40 States. CISA also provides funding to the Election Infrastructure Information Sharing and Analysis Center (EI–ISAC), which now includes all 50 States and more than 3,400 local jurisdictions. This

is the main mechanism for sharing alerts with the election's community. DHS also provides funding for enhancing election security through FEMA grants.

- *Combating Disinformation Around Elections*.—State, local, Tribal, and territorial officials are the most trusted sources of election information in communities across our Nation: DHS partners with them to help ensure that voters receive accurate information. DHS assists with addressing disinformation by being transparent about identified foreign malign influence campaigns, amplifying facts shared by State, local, Tribal, and territorial officials with the public, and encouraging individuals to maintain digital and media literacy to recognize and build resilience.

CONCLUSION

While DHS was created in response to a singular threat, in the 2 decades since 9/11 the Department has evolved to address multiple unforeseen complex challenges. Through it all, our workforce has demonstrated exceptional skill and an unwavering commitment to keeping our country safe.

I am grateful to this committee for your continued support of DHS, both from a resource perspective and the provision of key authorities that allow the Department to adapt to an ever-changing threat landscape. I look forward to our continued work together and to answering your questions. Thank you.

Chairman THOMPSON. Thank you very much.

The Chair recognizes Director Wray to summarize his statement for 5 minutes.

STATEMENT OF CHRISTOPHER A. WRAY, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Mr. WRAY. Good morning, Chairman Thompson, Ranking Member Katko, Members of the committee. I am honored to be here today on behalf of the FBI's 38,000 men and women to discuss some of the most pressing threats facing our homeland.

When it comes to our current threat landscape, what makes our current situation, at least in my career, unique is—and particularly serious, I would add—is the fact that we have so many different threat areas all elevated at the same time. I am proud of the work that the FBI's agents, analysts, and professional staff are doing all over the country and all over the world every single day to rise to those challenges and to protect the American people.

Protecting the American people from terrorist attack remains the FBI's No. 1 priority. As I have said before, the greatest threat we face on the terrorism front here in the homeland is from what are effectively lone actors, or small cells. Whether it is a domestic violent extremist acting in furtherance of some ideological goal or a home-grown violent extremist looking to advance the interest of a foreign terrorist organization, these actors often move quickly from radicalization to action and often use easily obtainable weapons—think a gun, a knife, a car, a crude IED—against soft targets, which is just intelligence community speak for everyday people living everyday lives.

Overseas ISIS and al-Qaeda still aim to inspire, to plan, and to launch attacks against the United States and our allies, both abroad and here at home. As the al-Zawahiri strike this summer in Kabul reinforces, the threat of foreign terrorist organizations like al-Qaeda attempting to reconstitute in Afghanistan following our withdrawal remains very real. Our ability to gather valuable intelligence on the ground inside Afghanistan has been reduced. That is just a reality. All of that places a premium on our continued collaboration with our partners, both within the U.S. Govern-

ment and internationally. We have got to stay on the balls of our feet and use all of the tools available to us.

On top of that, countries like China, Russia, Iran, and North Korea are growing more aggressive, brazen, and capable. They are coming at us from all angles to undermine our core democratic institutions, our national security, and our rule of law.

Of those countries, the greatest long-term threat to our Nation's ideas, innovation, and economic security, our national security, is that from China. The Chinese government aspires to equal or surpass the United States as a global superpower and influence the world with a value system shaped by undemocratic authoritarian ideals. We are confronting that threat head-on. Just 3 weeks ago, for example, we unsealed charges against 13 individuals, 10 of them Chinese intelligence officers and government officials, for a variety of criminal efforts to exert influence right here in the United States to benefit Beijing. The FBI has scores of investigations open into the China threat in all 56 of our field offices.

On the cyber front, China's vast hacking program is the world's largest and they have stolen more of American's personal and business data than every other nation combined. But, of course, China is not our only challenge in cyber space—not even close. The FBI's cyber investigations are growing in frequency, scale, and complexity consistent with the evolution of the threat. We are investigating over 100 different ransomware variants and each one of those with scores of victims, as well as a whole host of other novel threats posed by both cyber criminals and nation-states alike. It is becoming more and more difficult to discern where the cyber criminal activity ends and the nation-state activity begins, as the line between those two continues to blur.

Just last month, for example, we announced the indictment of three Iranian nationals for their roles in a multi-year scheme to compromise the networks of hundreds of organizations, many of which offer services Americans rely on every day. To those sorts of actors, nothing is off limits, not even, for example, Boston Children's Hospital, which they set their sights on in the summer of 2021. Now, fortunately, before they could successfully launch their attack, we received a tip from a partner and working closely with the hospital, we were able to identify and defeat the threat, protecting both the network and the sick children who depend on it.

Our opponents in this space are relentless, so we have got to keep responding in kind. I can assure you that we are going to continue to be aggressive and creative as we run joint sequenced operations with our partners against these adversaries, removing their malware, taking down their botnets, and hunting them down all over the world.

That is just a snapshot of some of the many threats we are tackling, and it doesn't even include things like our efforts to combat violent crime, where this summer, working with our State and local partners, we arrested on average 50 violent criminals every single day. Or our continued focus on human trafficking, where this August, through our annual Operation Cross County, for instance, the FBI and our partners located more than 200 victims of human trafficking, many of them little kids. Or the work of our transnational organized crime section that it is doing in partnership with agen-

cies like DHS to investigate the movement of people, drugs, guns, and money into the United States across our Southern Border.

The breadth and depth of the threats that the FBI's dedicated men and women are tackling each and every day is staggering. I continue to be inspired by their commitment to our mission of protecting the American people and upholding the Constitution. I know we will continue to answer the call.

So thank you again for having me here again today and I would be happy to address your questions.

[The prepared statement of Mr. Wray follows:]

PREPARED STATEMENT OF CHRISTOPHER A. WRAY

NOVEMBER 15, 2022

Good morning, Chairman Thompson, Ranking Member Katko, and Members of the committee. Today, I am honored to be here, representing the people of the Federal Bureau of Investigation ("FBI"), who tackle some of the most complex and most grave threats we face every day with perseverance, professionalism, and integrity. Sometimes at the greatest of costs. I am extremely proud of their service and commitment to the FBI's mission and to ensuring the safety and security of communities throughout our Nation. On their behalf, I would like to express my appreciation for the support you have given them in the past and ask for your continued support in the future.

Despite the many challenges our FBI workforce has faced, I am immensely proud of their dedication to protecting the American people and upholding the Constitution. Our country continues to face unimaginable challenges, yet, through it all, the women and men of the FBI have unwaveringly stood at the ready and taken it upon themselves to tackle any and all challenges thrown their way. The list of diverse threats we face underscores the complexity and breadth of the FBI's mission: To protect the American people and uphold the Constitution of the United States. I am prepared to discuss with you what the FBI is doing to address these threats and what the FBI is doing to ensure our people adhere to the highest of standards while it conducts its Mission. I am pleased to have received your invitation to appear today and am looking forward to engaging in a thorough, robust, and frank discussion regarding some of the most critical threats facing the FBI and the Nation as a whole.

KEY THREATS AND CHALLENGES

Our Nation continues to face a multitude of serious and evolving threats ranging from home-grown violent extremists to hostile foreign intelligence services and operatives, from sophisticated cyber-based attacks to internet-facilitated sexual exploitation of children, from violent gangs and criminal organizations to public corruption and corporate fraud. Keeping pace with these threats is a significant challenge for the FBI. As an organization, we must be able to stay current with constantly-evolving technologies. Our adversaries—terrorists, foreign intelligence services, and criminals—take advantage of modern technology, including the internet and social media, to facilitate illegal activities, recruit followers, encourage terrorist attacks and other illicit actions, to spread misinformation, and to disperse information on building improvised explosive devices and other means to attack the United States. The breadth of these threats and challenges are as complex as any time in our history. The consequences of not responding to and countering threats and challenges have never been greater.

The support of this committee in helping the FBI do its part in thwarting these threats and facing these challenges is greatly appreciated. That support is allowing us to establish strong capabilities and capacities to assess threats, share intelligence, leverage key technologies, and—in some respects, most importantly—hire some of the best to serve as special agents, intelligence analysts, and professional staff. We have built, and are continuously enhancing, a workforce that possesses the skills and knowledge to deal with the complex threats and challenges we face today and tomorrow. We are building a leadership cadre that views change and transformation as a positive tool for keeping the FBI focused on the key threats facing our Nation.

Today's FBI is a National security and law enforcement organization that uses, collects, and shares intelligence in everything we do. Each FBI employee under-

stands that, to defeat the key threats facing our Nation, we must constantly strive to be more efficient and more effective. Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of acute and persistent terrorist, nation-state, 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.

NATIONAL SECURITY

Terrorism Threats

Protecting the American people from terrorism—both international and domestic—remains the FBI's No. 1 priority. The threat from terrorism is as persistent and complex as ever. We are in an environment where the threats from international terrorism, domestic terrorism, and state-sponsored terrorism are all simultaneously elevated.

The greatest terrorism threat to our homeland is posed by lone actors or small cells of individuals who typically radicalize to violence on-line, and who primarily use easily accessible weapons to attack soft targets. We see the lone offender threat with both Domestic Violent Extremists ("DVEs") and Home-grown Violent Extremists ("HVEs"), two distinct threats, both of which are located primarily in the United States and typically radicalize and mobilize to violence on their own. Individuals based and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seek to further political or social goals, wholly or in part, through unlawful acts of force or violence are described as DVEs, whereas HVEs are individuals of any citizenship who have lived and/or operated primarily in the United States or its territories who advocate, are engaged in, or are preparing to engage in ideologically-motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization, but are acting independently of direction by a foreign terrorist organization ("FTO").

Domestic and Home-grown Violent Extremists are often motivated and inspired by a mix of social or political, ideological, and personal grievances against their targets, and more recently have focused on accessible targets to include civilians, law enforcement and the military, symbols or members of the U.S. Government, houses of worship, retail locations, and mass public gatherings. Lone actors present a particular challenge to law enforcement and intelligence agencies. These actors are difficult to identify, investigate, and disrupt before they take violent action, especially because of the insular nature of their radicalization and mobilization to violence and limited discussions with others regarding their plans.

The top domestic terrorism threat we face continues to be from DVEs we categorize as Racially or Ethnically Motivated Violent Extremists ("RMVEs") and Anti-Government or Anti-Authority Violent Extremists ("AGAAVEs"). While RMVEs, who advocate for the superiority of the white race were the primary source of lethal attacks perpetrated by DVEs in recent years, AGAAVEs, specifically Militia Violent Extremists and Anarchist Violent Extremists were responsible for 3 of the 4 lethal DVE attacks in 2020. Notably, 2020 included the first lethal attack committed by an Anarchist Violent Extremist in over 20 years. More recently, in 2021, DVEs committed at least 4 lethal attacks, resulting in 13 deaths. DVEs with mixed or personalized ideologies committed 2 of the 4 attacks. The other 2 lethal attacks were committed by RMVEs—one who advocated for the superiority of the white race and one who allegedly used his interpretations of religious teachings to justify the murder of a police officer. The number of FBI domestic terrorism investigations has more than doubled since the spring of 2020, and as of the end of fiscal year 2022, the FBI was conducting approximately 2,700 domestic terrorism investigations.

We are approaching the 2-year anniversary of the January 6 siege of the U.S. Capitol, which has led to unprecedented efforts by the Department of Justice, including the FBI, to investigate and hold accountable all who engaged in violence, destruction of property, and other criminal activity on that day. To date, the Department has arrested and charged more than 880 individuals who took part in the Capitol siege.

The FBI uses all tools available at its disposal to combat domestic terrorism. These efforts represent a critical part of the National Strategy for Countering Domestic Terrorism, which was released in June 2021, and which sets forth a comprehensive, whole-of-Government approach to address the many facets of the domestic terrorism threat.

The FBI assesses HVEs are the greatest, most immediate international terrorism threat to the homeland. HVEs are people located and radicalized to violence pri-

marily in the United States, who are not receiving individualized direction from FTOs but are inspired by FTOs, including the self-proclaimed Islamic State of Iraq and ash-Sham ("ISIS") and al-Qaeda and their affiliates, to commit violence. An HVE's lack of a direct connection with an FTO, ability to rapidly mobilize without detection, and use of encrypted communications pose significant challenges to our ability to proactively identify and disrupt potential violent attacks.

The FBI remains concerned about the Taliban takeover of Afghanistan and the that the intent of FTOs, such as ISIS and al-Qaeda and their affiliates, intend to carry out or inspire large-scale attacks in the United States. Despite its loss of physical territory in Iraq and Syria, ISIS remains relentless in its campaign of violence against the United States and our partners—both here at home and overseas. ISIS and its supporters continue to aggressively promote its hate-fueled rhetoric and attract like-minded violent extremists with a willingness to conduct attacks against the United States and our interests abroad. ISIS's successful use of social media and messaging applications to attract individuals is of continued concern to us. Like other foreign terrorist groups, ISIS advocates for lone-offender attacks in the United States and Western countries via videos and other English language propaganda that have, at times, specifically advocated for attacks against civilians, the military, law enforcement, and intelligence community personnel.

Al-Qaeda maintains its desire to both conduct and inspire large-scale, spectacular attacks. Because continued pressure has degraded some of the group's senior leadership, we assess that, in the near term, al-Qaeda is more likely to continue to focus on cultivating its international affiliates and supporting small-scale, readily achievable attacks in regions such as East and West Africa. Over the past year, propaganda from al-Qaeda leaders continued to seek to inspire individuals to conduct their own attacks in the United States and other Western nations.

Iran and its global proxies and partners, including Iraqi Shia militant groups, continue to attack and plot against the United States and our allies throughout the Middle East in response to U.S. pressure. Iran's Islamic Revolutionary Guard Corps-Qods Force ("IRGC–QF") continues to provide support to militant resistance groups and terrorist organizations. Iran also continues to support Lebanese Hizballah and other terrorist groups. Hizballah has sent operatives to build terrorist infrastructures world-wide. The arrests of individuals in the United States allegedly linked to Hizballah's main overseas terrorist arm, and their intelligence collection and procurement efforts, demonstrate Hizballah's interest in long-term contingency planning activities here in the homeland. Hizballah Secretary-General Hassan Nasrallah also has threatened retaliation for the death of IRGC–QF Commander Qassem Soleimani. This threat was exemplified in 2022, when the Department charged an Iranian national and member of the IRGC, working on behalf of the Qods Force, with a plot to murder a former National Security Advisor.

The terrorism threat continues to evolve, but the FBI resolve to counter that threat remains constant. As an organization, we continually adapt and rely heavily on the strength of our Federal, State, local, Tribal, territorial, and international partnerships to combat all terrorist threats to the United States and our interests. To that end, we use all available lawful investigative techniques and methods to combat these threats while continuing to collect, analyze, and share intelligence concerning the threat posed by violent extremists, in all their forms, who desire to harm Americans and U.S. interests. We will continue to share information and encourage the sharing of information among our numerous partners via our Joint Terrorism Task Forces across the country, and our Legal Attaché offices around the world.

Cyber

Throughout these last 2 years, the FBI has seen a wider-than-ever range of cyber actors threaten Americans' safety, security, and confidence in our digitally connected world. Cyber-criminal syndicates and nation-states keep innovating ways to compromise our networks and maximize the reach and impact of their operations, such as by selling malware as a service or by targeting vendors to access the networks of the vendors' customers.

These criminals and nation-states believe that they can compromise our networks, steal our property, extort us, and hold our critical infrastructure at risk without incurring any risk themselves. In the last few years, we have seen—and have publicly called out—the People's Republic of China ("PRC"), the Democratic People's Republic of Korea ("DPRK"), and Russia for using cyber operations to target U.S. COVID–19 vaccines and research. We have seen the far-reaching disruptive impact a serious supply chain compromise can have through the Solar Winds-related intrusions, conducted by the Russian SVR. We have seen the PRC working to obtain controlled dual-use technology and developing an arsenal of advanced cyber capabilities that

could be used against other countries in the event of a real-world conflict. As these adversaries become more sophisticated, we are increasingly concerned about our ability to detect and warn about specific cyber operations against U.S. organizations. One of the most worrisome facets is their focus on compromising U.S. critical infrastructure, especially during a crisis.

What makes things more difficult is that there is no bright line that separates where nation-state activity ends and cyber criminal activity begins. Some cyber criminals contract or sell services to nation-states; some nation-state actors moonlight as cyber criminals to fund personal activities; and nation-states are increasingly using tools typically used by criminal actors, such as ransomware.

So, as dangerous as nation-states are, we do not have the luxury of focusing on them alone. In the past year, we also have seen cyber criminals target hospitals, medical centers, educational institutions, and other critical infrastructure for theft or ransomware, causing massive disruption to our daily lives. Such incidents affecting medical centers in particular have led to the interruption of computer networks and systems that put patients' lives at an increased risk, at a time when America faces its most dire public health crisis in generations.

We have also seen the rise of an ecosystem of services dedicated to supporting cyber crime in exchange for cryptocurrency. The effect is that what were once unsophisticated criminals now have the tools to engage in destructive behavior—for example, deploying ransomware to paralyze entire hospitals, police departments, and businesses—and the means to better conceal their tracks. It is not that individual malicious cyber actors have become much more sophisticated, but—unlike previously—they are able to rent sophisticated capabilities.

We must make it harder and more painful for malicious cyber actors and criminals to carry on their malicious activities. The FBI, using its role as the lead Federal agency for threat response, with its law enforcement and intelligence responsibilities, works seamlessly with domestic and international partners to defend their networks, attribute malicious activity, sanction bad behavior, and take the fight to our adversaries overseas. We must impose consequences on cyber adversaries and use our collective law enforcement and intelligence capabilities to do so through joint and enabled operations sequenced for maximum impact. And we must continue to work with the Department of State and other key agencies to ensure that our foreign partners are able and willing to cooperate in our efforts to bring the perpetrators of cyber crime to justice or otherwise disrupt such perpetrators' activities.

An example of this approach is the international seizure in April 2022 of Hydra Market—the world's largest and longest-running darknet market. Hydra was an online criminal marketplace that enabled users in mainly Russian-speaking countries to buy and sell illicit goods and services, including illegal drugs, stolen financial information, fraudulent identification documents, and money laundering and mixing services, anonymously and outside the reach of law enforcement. Transactions on Hydra were conducted in cryptocurrency and Hydra's operators charged a commission for every such transaction. In 2021, Hydra accounted for an estimated 80 percent of all darknet market-related cryptocurrency transactions, and since 2015, the marketplace had received approximately $5.2 billion in cryptocurrency. The seizure of the Hydra servers and cryptocurrency wallets containing $25 million worth of bitcoin was made in Germany by the German Federal Criminal Police (the Bundeskriminalamt), in coordination with the FBI and our other Federal partners in the Drug Enforcement Administration, the Internal Revenue Service, U.S. Postal Inspection Service, Homeland Security Investigations, and Organized Crime Drug Enforcement Task Forces. The FBI used technical expertise and legal authorities, and, most importantly, our world-wide partnerships to significantly disrupt this illegal marketplace.

In March, the FBI conducted a successful court-authorized operation to remove botnet malware known as Cyclops Blink from the botnet's command and control devices, cutting off the Russian Main Intelligence Directorate's (GRU) control over thousands of infected devices—mainly in small to mid-sized businesses—world-wide. The GRU had been building this malicious botnet, which ultimately spanned the globe, as early as June 2019, as a replacement for the VPNFilter malware we exposed and disrupted in 2018. Over several months, the FBI worked closely with WatchGuard Technologies, the developer of many of the infected devices, to analyze the malware, and WatchGuard developed detection tools and remediation techniques. In February, before the FBI's technical disruption, the FBI, NSA, CISA, and the United Kingdom's National Cyber Security Centre proactively released an advisory identifying the Cyclops Blink malware. That same day, WatchGuard released the detection and remediation tools. This latest disruption, in addition to highlighting the benefits of close public-private partnerships, proves that success against cyber threats doesn't only involve arrests and convictions.

In total, we took over 1,100 actions against cyber adversaries last year, to include arrests, criminal charges, convictions, dismantlements, and disruptions, and enabled many more actions through our dedicated partnerships with the private sector, foreign partners, and with Federal, State, and local entities. We also provided thousands of individualized threat warnings and disseminated more than 100 public threat advisories by way of Joint Cybersecurity Advisories, FBI Liaison Alert System ("FLASH") reports, Private Industry Notifications ("PINs"), and Public Service Announcements ("PSAs")—many of which were jointly authored with other U.S. agencies and international partners.

With our partners in the interagency, we have been putting a lot of energy and resources into all those partnerships, especially with the private sector. We are working hard to push important threat information to network defenders, but we have also been making it as easy as possible for the private sector to share important information with us. For example, we are emphasizing to the private sector how we keep our presence unobtrusive in the wake of an incident; how we protect information that the private sector shares with us, including their identities. We are also committed to providing useful feedback and improving coordination with our government partners so that we are speaking with one voice. But we need the private sector to do its part, too. We need the private sector to come forward to warn us—and warn us quickly—when they see malicious cyber activity. We also need the private sector to work with us when we warn them that they are being targeted. The recent examples of significant cyber incidents—SolarWinds, Cyclops Blink, the Colonial pipeline incident—only emphasize what I have been saying for a long time: The Government cannot protect against cyber threats on its own. We need a whole-of-society approach that matches the scope of the danger. There is no other option for defending a country where nearly all of our critical infrastructure, personal data, intellectual property, and network infrastructure sits in private hands.

In summation, 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 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, disrupt, and hold accountable those who pose a threat in cyber space.

Foreign Intelligence Threats

Top Threats

We see nations such as China, Russia, and Iran becoming more aggressive and more capable in their nefarious activity than ever before. These nations seek to undermine our core democratic, economic, and scientific institutions. They employ a growing range of tactics to advance their interests and to harm the United States. Defending American institutions and values against these threats is a national security imperative and a priority for the FBI.

With that, the greatest long-term threat to our Nation's ideas, innovation, and economic security is the foreign intelligence and economic espionage threat from China. It's a threat to our economic security—and by extension—to our National security. The Chinese government aspires to equal or surpass the United States as a global superpower and influence the world with a value system shaped by undemocratic authoritarian ideals. The pursuit of these goals is often with little regard for international norms and laws.

When it comes to economic espionage, the PRC uses every means at its disposal against us, blending cyber, human intelligence, diplomacy, corporate transactions, and pressure on U.S. companies operating in China, to achieve its strategic goals to steal our companies' innovations. These efforts are consistent with China's expressed goal to become a national power, modernizing its military and creating innovative-driven economic growth.

To pursue this goal, China uses not only human intelligence officers, co-optees, and corrupt corporate insiders, but also sophisticated cyber intrusions, pressure on U.S. companies in China, shell-game corporate transactions, and joint-venture "partnerships" that are anything but a true partnership. There's also nothing traditional about the scale of their theft—it's unprecedented in the history of the FBI. American workers and companies are facing a greater, more complex danger than they've ever dealt with before. Stolen innovation means stolen jobs, stolen opportunities for American workers, stolen national power, and stolen leadership in the industries.

National Counterintelligence Task Force ("NCITF")

As the lead U.S. counterintelligence agency, the FBI is responsible for detecting and lawfully countering the actions of foreign intelligence services and organizations as they seek to adversely affect U.S. National interests. The FBI recognized the

need to coordinate similar efforts across all agencies, and therefore established the National Counterintelligence Task Force ("NCITF") to create a whole-of-Government approach to counterintelligence. The FBI established the National-level task force, or NCITF, in the National Capital Region to coordinate, facilitate, and focus these multi-agency counterintelligence operations, and to programmatically support local Counterintelligence Task Force ("CITF") operations. Combining the authorities and operational capabilities of the U.S. Intelligence Community; Federal, State, and local law enforcement; and local CITFs in each FBI field office, the NCITF coordinates and leads whole-of-Government efforts to defeat hostile intelligence activities targeting the United States.

The Department of Defense has been a key partner in the NCITF since its founding in 2019. While the FBI has had long-term collaborative relationships with DoD entities such as the Air Force Office of Special Investigations, Naval Criminal Investigative Service, and Army Counterintelligence, the NCITF has allowed us to enhance our collaboration with each other for greater impact. We plan to emphasize this whole-of-Government approach moving forward as a powerful formula to mitigate the modern counterintelligence threat.

Transnational Repression

In recent years, we have seen a rise in efforts by authoritarian regimes to interfere with freedom of expression and punish dissidents abroad. These acts of repression cross national borders, often reaching into the United States. It's important to note countries like China, Russia, and Iran, stalk, intimidate, and harass certain people in the United States. This is called transnational repression. It's illegal and the FBI is investigating it.

Transnational repression can occur in different forms, including assaults and attempted kidnapping. Governments use transnational repression tactics to silence the voices of their citizens, U.S. residents, or non-citizens connected to the home country. This sort of repressive behavior is antithetical to our values as Americans. People from all over the world are drawn to the United States by the promise of living in a free and open society—one that adheres to the rule of law. To ensure that this promise remains a reality, we must continue to use all of our tools to block authoritarian regimes that seek to extend their tactics of repression beyond their shores.

Foreign Malign Influence

Our Nation is confronting multifaceted foreign threats seeking to both influence our National policies and public opinion, and cause harm to our National dialog and debate. The FBI and our interagency partners remain concerned about, and focused on, foreign malign influence operations—which include subversive, undeclared, coercive, and criminal actions used by foreign governments in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic institutions and processes.

Foreign malign influence is 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. Foreign malign 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 amplify existing stories on social media in an attempt to discredit U.S. individuals and institutions.

The FBI is the lead Federal agency responsible for investigating foreign malign influence threats. Several years ago, we established the Foreign Influence Task Force ("FITF") to identify and counteract foreign malign influence operations targeting the United States. The FITF is led by the Counterintelligence Division and comprises agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions. It is specifically charged with identifying and combating foreign malign influence operations targeting democratic institutions and values inside the United States. In all instances, the FITF strives to protect democratic institutions, develop a common operating picture, raise adversaries' costs, and reduce their overall asymmetric advantage.

The FITF brings the FBI's National security and traditional criminal investigative expertise under one umbrella to prevent foreign influence in our elections. This better enables us to frame the threat, to identify connections across programs, to aggressively investigate as appropriate, and—importantly—to be more agile. Coordinating closely with our partners and leveraging relationships we have developed in the technology sector, we had several instances where we were able to quickly relay

threat indicators that those companies used to take swift action, blocking budding abuse of their platforms.

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

In addition, the domestic counterintelligence environment is more complex than ever. This Nation faces a persistent and pervasive National security threat from foreign adversaries, particularly Russia and China, conducting sophisticated intelligence operations using coercion, subversion, malign influence, disinformation, cyber and economic espionage, traditional spying and non-traditional human intelligence collection. Together, they pose a continuous threat to U.S. National security and its economy by targeting strategic technologies, industries, sectors, and critical infrastructures. Historically, these asymmetric National security threats involved foreign intelligence service officers seeking U.S. Government and U.S. intelligence community information. The FBI has observed foreign adversaries employing a wide range of nontraditional collection techniques, including the use of human collectors not affiliated with intelligence services, foreign investment in critical U.S. sectors, and infiltration of U.S. supply chains. The FBI continues to adjust its CI priorities and posture to address the evolving and multifaceted threat.

CRIMINAL THREATS

We continue to face many criminal threats, from complex white-collar fraud in the financial, health care, and housing sectors to transnational and regional organized criminal enterprises to violent crime and public corruption. Criminal organizations—domestic and international—and individual criminal activity represent a significant threat to our security and safety in communities across the Nation.

Violent Crime

Violent crimes and gang activities exact a high toll on individuals and communities. Many of today's gangs are sophisticated and well-organized and use violence to control neighborhoods, and boost their illegal money-making activities, which include robbery, drug and gun trafficking, fraud, extortion, and prostitution rings. These gangs do not limit their illegal activities to single jurisdictions or communities. The FBI is able to work across such lines, which is vital to the fight against violent crime in big cities and small towns across the Nation. Every day, FBI special agents work in partnership with Federal, State, local, territorial, and Tribal officers and deputies on joint task forces and individual investigations.

Like the FBI's work combatting gangs, the FBI also investigates the most serious crimes in Indian Country—such as murder, child sexual and physical abuse, violent assaults, domestic violence, drug trafficking, public corruption, financial crimes, and Indian gaming violations. As you are aware, there are 574 Federally-recognized American Indian Tribes in the United States, and the FBI has Federal law enforcement responsibility on 188 Indian reservations. The FBI coordinates and collaborates with the Bureau of Indian Affairs ("BIA"), Office of Justice Services; and other Federal, State, and Tribal partners across the United States to investigate crimes in Indian Country."

Over the past 2 years, the FBI's work in Indian Country increased significantly due to the July 9, 2020, Supreme Court ruling in *McGirt* v. *Oklahoma,* which determined that the original boundaries of the Muscogee Creek Nation ("MCN") were never disestablished. This decision had the practical effect of requiring all land within MCN's territorial boundaries to fall under Federal Indian Country jurisdiction, thus expanding the FBI's responsibility for investigating felony offenses committed by or against an Indian. The principles of the *McGirt* decision also apply to Cherokee, Chickasaw, Choctaw, Seminole, and Quapaw Tribal territories in Oklahoma. Combined, all 6 reservations encompass approximately 32,000 square miles, or 45 percent of the State of Oklahoma. The total population within the combined borders is roughly 1.9 million, of which approximately 420,000 are enrolled Tribal members.

This drastic increase in FBI jurisdiction has significant and long-term operational and public safety implications given the increased number of violent criminal cases now under Federal jurisdiction within Oklahoma's Indian Country. Since this decision, the FBI's Oklahoma City Field Office ("OC") has seen a drastic increase in the total number of Indian Country investigations and now has the FBI's largest inves-

tigative responsibility. Since the Federal court ruling in the *McGirt* case, the FBI's Oklahoma City field office, which previously investigated approximately 50 criminal cases a year involving Native Americans, has managed thousands of Indian Country cases, prioritizing cases involving the most violent offenders who pose the most serious risk to the public.

To effectively conduct these investigations, the FBI has conducted temporary duty ("TDY") rotations of Special Agents, Intelligence Analysts, Victim Specialists, and other professional staff to the Muskogee and Tulsa RAs, the offices most impacted by the decision. The FBI has also expanded State, local, and Tribal participation on task forces to assist with response and investigative efforts. To support the U.S. Attorney's effective prosecution of these crimes, the FBI must have the capability to sustain an enhanced presence in FBI OC.

The FBI is committed to its mission of protecting Tribal communities through its Indian Country investigative program. With more than 150 Special Agents and 23 Safe Trails Task Forces around the country, the FBI has demonstrated its commitment to the safety and security of indigenous people by vigorously investigating the most serious crimes facing their communities. The FBI works to enhance its effectiveness by leveraging its relationships with its State, local, and Federal partners, both on and off the reservations.

The 2020 *McGirt* decision significantly increased the FBI's investigative responsibilities in Oklahoma by dramatically increasing both its territorial jurisdiction and caseload requirements. Furthermore, the decision created a jurisdictional gap, in that a large number of general crimes affecting Native American victims became unaddressed. In response the FBI surged National resources to ensure it was able to address its mission requirements to investigate major crimes in the newly designated Tribal Territory. These surges subsequently caused resource strains on other investigative programs and threats. The *Castro-Huerta* decision began to relieve that pressure and has the future potential to reduce FBI caseloads by an estimated 15 percent–20 percent in Oklahoma, while bridging the jurisdictional gap by allowing State authorities to address certain general crimes. This would free FBI resources to return to other National threat issues, while still providing Tribal communities with the FBI law enforcement services they've historically relied on.

The FBI fully recognizes and supports Tribal sovereignty while still seeking innovative ways to service the law enforcement needs of indigenous communities. The FBI believes ensuring public safety is a top priority and *Castro-Huerta* provides an avenue of bolstering that safety with the addition of State law enforcement services, while relieving resource burdens on the FBI. The FBI therefore supports the underlying policy as established in *Castro-Huerta* and would be opposed to legislation to abrogate the decision.

Transnational Organized Crime ("TOC")

More than a decade ago, organized crime was characterized by hierarchical organizations, or families, that exerted influence over criminal activities in neighborhoods, cities, or States. But organized crime has changed dramatically. Today, international criminal enterprises run multi-national, multi-billion-dollar schemes from start to finish. Modern-day criminal enterprises are flat, fluid networks with global reach. While still engaged in many of the "traditional" organized crime activities of loan-sharking, extortion, and murder, modern criminal enterprises are targeting stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, drug trafficking, identity theft, human trafficking, money laundering, human smuggling, public corruption, weapons trafficking, extortion, kidnapping, wildlife and timber trafficking, illegal fishing, illegal mining, and other illegal activities. TOC networks exploit legitimate institutions for critical financial and business services that enable the storage or transfer of illicit proceeds. Preventing and combating transnational organized crime demands a concentrated effort by the FBI and Federal, State, local, Tribal, and international partners.

While the FBI continues to share intelligence about criminal groups with our partners and combines resources and expertise to gain a full understanding of each group, the threat of transnational crime remains a significant and growing threat to national and international security with implications for public safety, public health, democratic institutions, and economic stability across the globe. TOC groups increasingly exploit jurisdictional boundaries to conduct their criminal activities overseas. Furthermore, they are expanding their use of emerging technology to traffic illicit drugs and contraband across international borders and into the United States.

Crimes Against Children and Human Trafficking

It is unthinkable, but every year, thousands of children become victims of crimes, whether it is through kidnappings, violent attacks, sexual abuse, human trafficking, or on-line predators. The FBI is uniquely positioned to provide a rapid, proactive, and comprehensive response; identify, locate, and recover child victims; and strengthen relationships between the FBI and Federal, State, local, Tribal, and international law enforcement partners to identify, prioritize, investigate, and deter individuals and criminal networks from exploiting children.

But the FBI's ability to learn about and investigate child sexual exploitation is being threatened by the proliferation of sites on-line on the Darknet. For example, currently, there are at least 30 child pornography sites operating openly and notoriously on the Darknet, including the Tor network. Some of these child pornography sites are exclusively dedicated to the sexual abuse of infants and toddlers. The sites often expand rapidly, with one site obtaining 200,000 new members within its first 4 weeks of operation.

The FBI combats this pernicious crime problem through investigations such as Operation Pacifier, which targeted the administrators and users of a highly sophisticated, Tor-based global enterprise dedicated to the sexual exploitation of children. This multi-year operation led to the arrest of approximately 350 individuals based in the United States, the prosecution of 25 American child pornography producers and 51 American hands-on abusers, the rescue or identification of 55 American children, the arrest of 548 international individuals, and the identification or rescue of 296 children abroad.

The FBI has several programs in place to arrest child predators and to recover missing and endangered children. To this end, the FBI funds or participates in a variety of endeavors, including our Innocence Lost National Initiative, Innocent Images National Initiative, Operation Cross Country, Child Abduction Rapid Deployment Team, Victim Services, over 80 Child Exploitation and Human Trafficking Task Forces, over 50 International Violent Crimes Against Children Task Force Officers, as well as numerous community outreach programs to educate parents and children about safety measures they can follow. Through improved communications, the FBI also has the ability to quickly collaborate with partners throughout the world, which plays an integral role in crime prevention.

The Child Abduction Rapid Deployment Team is a rapid response team comprised of experienced investigators strategically located across the country to quickly respond to child abductions. Investigators are able to provide a full array of investigative and technical resources during the most critical time period following the abduction of a child, such as the collection and analysis of DNA, impression and trace evidence and the processing of digital forensic evidence.

In addition to programs combating child exploitation, the FBI also focuses efforts to stop human trafficking. The FBI works collaboratively with law enforcement partners to combat all forms of human trafficking through Human Trafficking Task Forces Nation-wide.

The majority of human trafficking victims recovered during FBI investigations are United States citizens, but traffickers are opportunists who will exploit any victim with a vulnerability, including foreign nationals and victims of all ages, by subjecting them to forced labor or sex trafficking. We take a victim-centered, trauma-informed approach to investigating these cases and strive to ensure the needs of victims are fully addressed at all stages. To accomplish this, the FBI works in conjunction with other law enforcement agencies and victim specialists on the local, State, Tribal, and Federal levels, as well as with a variety of vetted non-Governmental organizations. Even after the arrest and conviction of human traffickers, the FBI often continues to work with partner agencies and organizations to assist victims and survivors in moving beyond their exploitation.

Civil Rights

The FBI remains dedicated to protecting the cherished freedoms of all Americans. Civil rights crimes are among the most egregious violations of Federal law—they include color of law violations, hate crimes, Freedom of Access to Clinic Entrances ("FACE") Act violations, and voter suppression. These crimes cause long-term, enduring damage to communities and economic infrastructure, compromise law enforcement and judicial system capabilities, and provoke wide-spread fear and trauma. We also support the work and cases of our State and local partners, as needed.

The investigation of hate crimes is the No. 1 priority within the FBI's civil rights program due to the devastating effect these types of crimes can have not just on the victims and their families, but also on entire communities. A hate crime is a criminal offense against a person or property motivated in whole or in part by the perpetrator's bias against a race, religion, disability, ethnic/national origin, sexual

orientation, gender, or gender identity. While the First Amendment to the Constitution allows for the free expression of both offensive and hateful speech, this protection does not extend to criminal acts, even those done to express an idea or belief. The First Amendment also does not protect someone who issues a true threat to inflict physical harm on individuals or groups, or who intentionally solicits others to commit unlawful acts of violence on his or her behalf. The FBI remains dedicated to investigating these types of crimes.

Beyond investigative work, the FBI recognizes proper and thorough handling of civil rights crimes does not begin the moment they are reported—it begins before they occur, with a solid and trusting relationship between the community and law enforcement. Each FBI field office will be taking specific actions to combat civil rights crimes in their area of responsibility ("AOR") to encourage systemic change. These actions include identifying appropriate partner agencies and local groups to develop outreach relationships at all levels, especially those that will spark institutional change; increasing civil rights-focused working groups and task forces with Federal, State, local, private, public, and non-profit partners; and providing increased training for State and local agencies and community groups centered on color of law investigations and hate crimes statutes to provide education about civil rights violations, promote increased reporting of hate crimes, and rebuild community trust in law enforcement.

Furthermore, we are focused on working with our State and local partners to collectively do a better job of tracking and reporting hate crime and color of law violations to fully understand what is happening in our communities and how to stop it. Our ability to address significant National issues, such as the use of force and officer-involved shootings and jurisdictional increases in violent crime, depends on fuller statistical understanding of the underlying facts and circumstances. Some jurisdictions fail to report hate crime statistics, while others claim there are no hate crimes in their community—a fact that would be welcome, if true. We are dedicated to working vigorously with our State and local counterparts in every jurisdiction to better track and report hate crimes, in an accurate, timely, and publicly transparent manner.

Lawful Access

The FBI remains a strong advocate for the wide and consistent use of encryption. Protecting data and privacy in a digitally-connected world is a top priority for the FBI, and we believe that promoting encryption is a vital part of that mission. Encryption without lawful access, though, does have a negative effect on law enforcement's ability to protect the public. As I have testified previously, when the FBI discusses lawful access, we mean putting providers who manage encrypted data in a position to decrypt it and provide it to us in response to a legal process. We do not mean for encryption to be weakened or compromised so that it can be defeated from the outside by law enforcement or anyone else. Unfortunately, too much of the debate over lawful access has revolved around discussions of this concept that the FBI would not support.

The problems caused by law enforcement agencies' inability to easily access electronic evidence continue to grow. Increasingly, commercial device manufacturers have employed encryption in such a manner that only the device users can access the content of the devices. Similarly, more and more communications service providers are designing their platforms and apps such that only the parties to the communication can access the content. This is generally known as "end-to-end" encryption. The proliferation of end-to-end encryption is a serious issue that increasingly limits law enforcement's ability, even after obtaining a lawful warrant or court order, to access critical evidence and information needed to disrupt threats, protect the public, and bring perpetrators to justice.

For example, even with our substantial resources, accessing the content of known or suspected terrorists' data pursuant to court-authorized legal process is increasingly difficult. The often on-line nature of the terrorist radicalization process, along with the insular nature of most of today's attack plotters, leaves fewer dots for investigators to connect in time to stop an attack, and end-to-end encryption increasingly hide even those often precious few and fleeting dots.

In one instance, while planning—and right up until the eve of—the December 6, 2019, shooting at Naval Air Station Pensacola that killed 3 U.S. sailors and severely wounded 8 other Americans, deceased terrorist Mohammed Saeed Al-Shamrani communicated undetected with overseas al-Qaeda terrorists using an end-to-end encrypted app. Then, after the attack, encryption prevented the FBI from accessing information contained in his phones for several months. As a result, during the critical time period immediately following the shooting and despite obtaining search warrants for the deceased killer's devices, the FBI could not access the information

on those phones to identify co-conspirators or determine whether they may have been plotting additional attacks.

This problem spans international and domestic terrorism threats. For example, subjects of our investigation into the January 6 Capitol siege used end-to-end encrypted communications.

We face the same problem in protecting children against violent sexual exploitation. End-to-end encryption frequently prevent us from discovering and searching for victims, since the vital tips we receive from providers only arrive when those providers themselves are able to detect and report child exploitation being facilitated on their platforms and services.

When we are able to open investigations, end-to-end encryption make it much more difficult to bring perpetrators to justice. Much evidence of crimes against children, just like the evidence of many other kinds of crime today, exists primarily in electronic form. If we cannot obtain that critical electronic evidence, our efforts are frequently hamstrung.

This problem is not just limited to Federal investigations. Our State and local law enforcement partners have been consistently advising the FBI that they, too, are experiencing similar end-to-end encryption challenges, which are now being felt across the full range of State and local criminal law enforcement. Many report that even relatively unsophisticated criminal groups, like street gangs, are frequently using encrypted smartphones and end-to-end encrypted communications apps to shield their activities from detection or disruption. As this problem becomes more and more acute for State and local law enforcement, the advanced technical resources needed to address even a single investigation involving end-to-end encryption will continue to increase.

CONCLUSION

Finally, the strength of any organization is its people. The threats we face as a Nation have never been greater or more diverse and the expectations placed on the FBI have never been higher. Our fellow citizens look to the FBI to protect the United States from all threats, and the people of the FBI continue to meet and exceed those expectations, every day. I want to thank them for their dedicated service.

Chairman Thompson, Ranking Member Katko, and Members of the committee, thank you for the opportunity to testify today. I am happy to answer any questions you might have.

Chairman THOMPSON. The gentleman's time has expired.

The Chair now recognizes Director Abizaid to summarize her statement for 5 minutes.

STATEMENT OF CHRISTINE ABIZAID, DIRECTOR, NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Ms. ABIZAID. Chairman Thompson, Ranking Member Katko, Members of the committee, thank you for the opportunity to appear before you today to discuss the overall terrorism landscape.

Now, despite significant progress in diminishing the terrorist threat to the United States, the country continues to face a diversified transnational, and in many ways, unpredictable threat environment, both at home and abroad. An array of actors, whether foreign terrorist organizations, state sponsors of terrorism, or lone actors, are shaping the nature of today's threat. This changed environment exists amid an on-going transition for the counterterrorism community where CT, while critical, is one of many competing priorities that the U.S. national security community must be postured to address.

In today's testimony I will start by giving an overview of the terrorist threat to the homeland, I will turn to the overseas threat, and then end with some comments on the importance of our continued CT focus.

Regarding the threat to the United States homeland, terrorist organizations such as ISIS and al-Qaeda remain committed to attacking the United States. However, unlike 21 years ago, the threat today is more likely to take the form of an individual attacker inspired by these groups rather than a highly networked hierarchically-directed terrorist plot. In fact, since 9/11 37 of the 45 ISIS or al-Qaeda-linked attacks in the homeland have been inspired by these groups rather than centrally managed by them. This trend toward lone actor threats inside the United States extends beyond ISIS and al-Qaeda, it also characterizes the threat we face from domestic actors, such as racially or ethnically motivated violent extremists, militia violent extremists, or anarchist violent extremists.

In particular, the U.S.-based racially and ethnically motivated violent extremist, or REMVE threat, has the most obvious links to transnational actors whose plots and professed ideology encourage mobilization to violence by those vulnerable to their messaging. This threat is fluid, it is fragmented, it lacks in hierarchical structures, and it has proponents around the globe and in the United States framing actions around the concept of leaderless resistance.

Transitioning to the overseas environment, Sunni- and Shia-driven terrorist movements world-wide continue to dominate the threat to Americans. ISIS and al-Qaeda continue to aspire to attack the United States and other Western targets overseas, though they have been more effective at pursuing operations against regional and local adversaries. For its part, ISIS in Iraq and Syria remains an intact centrally-led organization that will most likely continue to pose both a global threat and a local one, despite the death of its Emir in February, Hajji Abdullah.

While significantly weaker than at its peak in 2015 through 2017, ISIS leaders from Iraq and Syria have been successful at spurning branches and networks across Africa and as far as South and East Asia with its two most effective branches currently operating out of West Africa and Afghanistan.

Likewise, al-Qaeda maintains its regional affiliate structure, positioned effectively in parts of North and East Africa, the Middle East, and to a lesser extent, South Asia. The July death of longtime al-Qaeda leader, Ayman al-Zawahiri, was a strategic and symbolic setback for al-Qaeda, but it does not put an end to the organization. In particular, in the Middle East, al-Qaeda in the Arabian Peninsula is a destabilizing actor in Yemen and remains among the most intrepid al-Qaeda affiliates intent on attacking the United States homeland.

Two other prominent al-Qaeda affiliates also stand out, both for their growing regional influence and their significant capabilities. The Sahel-based al-Qaeda affiliate, JNIM, and the Somalia-based affiliate, al-Shabaab.

Transitioning from Sunni terrorism to threats emanating from Iran, its partners and proxies, Iran continues to plan, encourage, and support plots against the United States, both at home and in the Middle East, where we have a significant U.S. military presence. Iran and its proxy, Lebanese Hezbollah, have sought to plot attacks against former U.S. officials to retaliate for the death of Islamic Revolutionary Guards Corps' Qods Force commander Qasum

Solomani, raising the threat both at home and abroad for those that Iran deems responsible.

In closing, I would just highlight that the complexity of the terrorism environment that I just outlined continues to demand a collaborative, agile, and sufficiently resourced CT effort to mitigate terrorist threats to the United States. It is clear that the significant CT pressure brought to bear against terrorist groups over the last 2 decades, along with investment in effective CT defenses here at home, has resulted in a diminished threat to the United States homeland.

NCTC and its CT partners across the Government are working toward a sustainable and enduring level of support to this mission that maintains that strategic success even as other National security priorities drive our National strategy.

Finally, I want to assure this committee that the interagency enterprise of CT practitioners remains committed to this mission and are working behind the scenes every day to protect the American people, both at home and abroad. I thank them for their service and their dedication to this country.

With that, I welcome your questions.

[The prepared statement of Ms. Abizaid follows:]

PREPARED STATEMENT OF CHRISTINE ABIZAID

NOVEMBER 15, 2022

Good morning, Chairman Thompson, Ranking Member Katko, and Members of the committee. Thank you for the opportunity to discuss the overall terrorism landscape, the threat posed to the homeland and U.S. persons and interests overseas, and the state of the U.S. counterterrorism (CT) enterprise.

U.S. FACES A PERSISTENT, EVOLVING TERRORIST THREAT

Despite significant progress in diminishing the terrorist threat to the United States, the country continues to face a diversified, transnational, and, in many ways, unpredictable threat environment both at home and abroad. An array of actors, whether foreign terrorist organizations (FTOs), state sponsors of terrorism, or lone actors, is shaping the nature of today's terrorism landscape. This persistent threat environment exists amid an on-going transition for the CT community where CT, while still critical, is one of many competing priorities the U.S. national security community must be postured to address.

Internationally, Russia's invasion of and war in Ukraine, China's growing economic and security assertiveness, Iran's destabilizing activities in the Middle East and beyond, North Korea's confrontational behavior, and the growing capabilities of a number of cyber actors, for example, are among the most consequential challenges to U.S. National security.

At the same time, violent extremism continues to fuel threats against the West from a growing swath of territory from the African Sahel to Southeast Asia and contributes to worsening humanitarian conditions in regions like Afghanistan, Somalia, and Yemen. Notably, this diffusion of the threat, while challenging, has resulted in a less concentrated and effective terrorist capability directed inside the homeland.

Terrorist organizations such as ISIS and al-Qaeda and other aligned violent extremists take advantage of developing nations, political instability, and undergoverned territory to entrench themselves in difficult operating environments and ingratiate themselves to local populations. These movements remain committed to attacking U.S. persons and facilities world-wide even as they balance those goals against local gains. These groups represent the most urgent threat to U.S. interests overseas.

In the homeland, we remain concerned about al-Qaeda and ISIS threats but assess the threat these groups pose here is less acute than at any other time since 9/11, a judgment consistent with what we expressed last year. In fact, the most likely threat in the United States is from lone actors, whether inspired by violent ex-

tremist narratives, racially or ethnically motivated drivers to violence, or other politically-motivated violence.

Against the backdrop of this threat landscape, whether overseas or at home, NCTC remains focused on uncovering and disrupting transnational networks from which threats to Americans and America are likely to emerge. Even as we monitor the threat, we also must evaluate the state of the CT community's ability to address it. This role is even more critical as resources shift away from CT and we need to account for the sustained ability to meet the threat, however it evolves.

THE MAIN THREAT INSIDE THE UNITED STATES

Unlike 21 years ago, the American public today is more likely to experience a terrorist attack by an individual attacker than a highly structured terrorist organization. Today's lone-actor threats can mobilize in unpredictable ways based on a variety of motivations. These individuals almost certainly mobilize to violence independently without direction from specific groups.

Since 9/11, there have been 37 attacks in the homeland inspired by al-Qaeda or ISIS, compared to 8 that involved a direct connection to these groups. Similarly, during the last 12 years, all of the 17 racially or ethnically motivated violent extremist (RMVE) attacks by actors espousing the superiority of the white race were by individuals who radicalized at least in part on-line and who mobilized to violence as lone actors.

FTOs inspiring lone actors

Even as our concern grows about the threat from U.S.-based RMVEs and other domestic violent extremists, we remain concerned and vigilant regarding the threat from lone actors and small groups inspired by FTOs. Since 2001, the threat emanating from these individuals has evolved from one defined by complex, large-scale attacks directed by an FTO to mostly simple, self-initiated attacks inspired by an FTO. Messaging directed at these individuals to conduct attacks has decreased, although they continue to draw inspiration from historical publications such as al-Qaeda in the Arabian Peninsula's (AQAP) *Inspire* magazine or ISIS's messaging directed at these individuals.

Domestic violent extremists

Since 2018, drawing on our significant knowledge of transnational terrorism, NCTC has regularly supported the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) to understand the threat in the homeland posed by domestic violent extremists. Within this category of threat actors, acts of violence by U.S.-based RMVEs, militia violent extremists (MVEs), and anarchist violent extremists (AVEs) stand out. The RMVE threat has the most obvious links to transnational actors whose plots and professed ideology encourage mobilization to violence by those vulnerable to their messaging. The RMVE threat is largely fluid, fragmented, and lacking in hierarchical structures, with proponents framing actions around the concept of leaderless resistance.

U.S.-based RMVEs' linkage to foreign counterparts mostly involves the bidirectional sharing of violent extremist messaging, mutual grievances, manifestos of successful attackers, and encouragement for lone-actor violence, such as by the alleged Buffalo shooter. As with other terrorism challenges, RMVEs anywhere can operate transnationally by exploiting a world connected by social media and other on-line platforms. Even as technology companies improve their capabilities to detect and respond to violent extremist content on-line, RMVEs and their supporters find new methods to spread their message.

Additionally, the lethal threat from MVEs remains elevated, primarily toward Government and law enforcement personnel. MVEs are willing to use violence to redress perceived Government overreach and other sociopolitical grievances, judging from an increase in MVE plotting, disruptions, and FBI investigations since 2020.

AVEs also present a threat of sporadic violent physical assaults and property crimes affecting critical infrastructure most often directed at people or institutions seen as representing authority, capitalism, and oppression. Developments that heighten perceptions of inequality or social injustice might further embolden AVEs to commit acts of violence.

Disrupting terrorist travel and securing the border

In addition to supporting DHS and FBI efforts to disrupt threats inside the United States NCTC also supports efforts to prevent terrorist's infiltration of the homeland. Identifying known or suspected terrorists or their affiliates who seek to infiltrate U.S. borders by land, sea, or air is central to the U.S. Government's CT strategy. NCTC collaborates regularly with its partners, and on their behalf, State

and local partners, to build a common threat picture to enable operating partners to protect the U.S. border. In particular, NCTC continues to support the U.S. Government's screening and vetting enterprise and plays a critical role in refugee and immigration processing by identifying any connections to international terrorism, not only for the applicant, but also appropriate members of the applicant's family.

THE TERRORIST THREAT OVERSEAS CONTINUES TO EVOLVE

Turning to the overseas environment, foreign terrorist movements world-wide continue to inspire followers and enable attack plotting against the United States, Americans, and other Western countries. ISIS and al-Qaeda, the two leading foreign terrorist threats to U.S. interests, continue to aspire to attack U.S. and other Western interests but have been more effective at pursuing operations against regional and local adversaries. CT pressure by the United States and foreign partners, during the last 15 years, has been critical in degrading the capability of these groups, particularly in disrupting experienced leaders and operatives and exacting sustained pressure against key networks.

ISIS's global enterprise

ISIS in Iraq and Syria remains an intact, centrally-led organization that will most likely continue to pose a global threat to U.S. and other Western interests as well as local populations. Despite losing more than a dozen senior leaders during the past 3 years, it continues to wage a low-level insurgency in Iraq and Syria since its territorial defeat in 2018 and commands a cohesive global network that has allowed the group to sustain its influence—and in some areas, such as in Africa, expand its recruitment and operations. We assess that in February, after a raid that killed its overall amir, ISIS transitioned seamlessly to a new amir. ISIS members readily accepted the new leader and we see no signs of fissures or splintering by the branches and networks despite limitations the group faces in Iraq and Syria.

Even under new leadership, ISIS remains committed to its long-term goal of establishing an Islamic caliphate and continues to exploit undergoverned areas in Iraq and Syria, where it currently operates as a clandestine insurgency. This year, ISIS prioritized and attacked a detention facility in northeastern Syria that housed key ISIS leaders and experienced fighters. While we assess most of the high-value detainees were either recaptured or killed as local forces responded to the attack, the operation itself signifies ISIS's ability to stage high-profile attacks and prioritize efforts to replenish its dwindling ranks. We have witnessed subsequent calls and efforts, including by ISIS branches as far away as West Africa, to free imprisoned members. ISIS's capabilities and trajectory will remain dependent upon the level of counterterrorism pressure it faces, particularly by CT actors who continue to routinely disrupt ISIS's facilitation networks and operations.

One of ISIS's primary mechanisms to threaten the West is through its media, even as the group's overall media capabilities have declined from the group's early years. Despite this decline, ISIS's most prolific threat to the United States or other Western countries is through inspired attackers who are vulnerable to influence by ISIS messaging. The group's ability to inspire violence was most recently demonstrated by an ISIS supporter who carried out an attack in Oslo in June, which killed 2 and injured 21. Pro-ISIS supporter groups have also helped augment ISIS's media presence by creating, archiving, translating, and disseminating multilingual propaganda on-line. One such group supporting ISIS-Khorasan published English-language media focused on delegitimizing the United States and denigrating the Taliban.

While we have seen a decline in the number of ISIS-inspired attacks in the West since peaking in 2017, such operations remain a priority for the organization. The group also still aspires to deploy operatives to the West, and we continue to monitor for threats against high-visibility, attractive regional targets that would have similarly high impact and provide propaganda value and publicity, such as the 2022 FIFA World Cup in Qatar. More broadly, ISIS has continued to grow its global enterprise, which now includes approximately 20 branches and networks, through which ISIS leaders' project strength and dispel the narrative of its defeat. In March, ISIS recognized its newest branch—ISIS in the Sahel—and, in July, the branch claimed responsibility for an attack on Nigeria's Kuje prison—located 27 miles away from the U.S. Embassy—in which almost 1,000 prisoners were released, including some terrorists.

ISIS has also used its branches and networks to choreograph global attack campaigns since 2019, the most recent of which was in April to avenge the death of the group's overall amir. ISIS in Iraq and Syria led in the number of attack claims and were boosted by ISIS-West Africa and ISIS-Khorasan, the branches we consider to be among the group's most capable.

This year, ISIS-Khorasan expanded its ambitions outside Afghanistan with a handful of cross-border rocket attacks against Tajikistan and Uzbekistan and a foiled plot in India. Its ambitions for attacking the West—possibly including the homeland—remains a top intelligence priority, notwithstanding the withdrawal of U.S. forces from Afghanistan last August.

ISIS is also exploiting uneven local CT pressure in Central, East, and Southern Africa to expand its presence, increase connectivity, and develop new capabilities beyond its traditional strongholds in North and West Africa. ISIS's expansion in Mozambique increasingly threatens Western-led energy projects there, while signs of ISIS's influence in the Democratic Republic of Congo, South Africa, and elsewhere in the region demonstrate the group's growing appeal across the continent.

Al-Qaeda post-Zawahiri

The death of al-Qaeda's longtime leader Ayman al-Zawahiri, this past July in Kabul, Afghanistan, dealt an important strategic and symbolic blow to the al-Qaeda network, which he led from relative isolation for more than a decade. Zawahiri was a respected ideological leader among the al-Qaeda global network who strove to enhance interconnectivity across al-Qaeda's dispersed regional affiliates. The network now finds itself without an obvious leader, but how quickly it will adapt to Zawahiri's loss remains to be seen.

Three months past the operation that killed him, the group has yet to publicly announce a successor. Among the remaining al-Qaeda veterans are several Iran-based senior leaders, most notably Sayf al-'Adl and Abd-al-Rahman al-Maghrebi, who probably continue to provide ideological and strategic guidance to the global network. We expect they both will continue to have important roles in the years ahead, despite the irony of their location in Iran, another of al-Qaeda's sworn enemies. Other, less prominent al-Qaeda leaders—who have been featured in globally- and regionally-focused media—are in charge of the regional affiliates and likely consult across a distributed leadership team about the direction of the al-Qaeda network.

Al-Qaeda's global network

Al-Qaeda's Iran-based senior leaders oversee the global network, which includes regional affiliates in Africa, the Middle East, and South Asia as well as various local networks that support the affiliates.

Starting in West Africa, al-Qaeda's Jama'at Nusrat al-Islam al-Muslimin (JNIM) is increasingly threatening capital cities in the Sahel while combatting local militaries, ISIS's Sahel province, and Russian paramilitary forces in Mali. In July of this year, the group attacked Mali's largest military camp, located just outside of Bamako, underscoring both its capabilities and growing boldness in the region. JNIM probably hopes to exploit the departure of French forces from Mali earlier this year to accelerate its growth and entrenchment, including into littoral West African states such as Benin, Cote d'Ivoire, and Togo. CT concerns in the region have further led to instability fueling nondemocratic transitions of power, most recently last month in Burkina Faso.

In the Horn of Africa, we remain concerned about the continued threat that al-Shabaab poses to U.S. citizens and Western interests. Al-Shabaab is the wealthiest and most lethal of all al-Qaeda affiliates, controls large portions of southern Somalia, and has demonstrated the capability to carry out successful operations across the region, including against U.S. service members.

In North Africa, al-Qaeda in the Islamic Maghreb (AQIM) has experienced setbacks from CT pressure since early 2018, but probably provides guidance to other al-Qaeda elements in the region, particularly JNIM. As of 2020, Algerian Yazid Mebrak was serving as AQIM's leader and was playing a key role in al-Qaeda's management of global operations, including the abductions and killing of Americans.

Turning to the Middle East and Yemen, AQAP is intent on conducting operations in the West and against U.S. and allied regional interests. It has proven itself to be among the al-Qaeda network's most creative branches but has faced significant CT pressure in recent years, creating hurdles for the group's external operations planning.

In June 2021, AQAP published its sixth issue of *Inspire Guide,* which provides operational guidance for would-be attackers in the homeland and suggests the group still maintains a viable media capability, despite the death last year of its key propagandist.

In Syria, al-Qaeda elements under the banner of Hurras al-Din have struggled to stabilize their footing and experienced numerous leadership losses and pressure from rival group Hay'at Tahrir al-Sham. However, these elements could use their

traditional safe haven in opposition-controlled territory to target U.S. and other Western interests in the region.

Finally, in Afghanistan, al-Qaeda's South Asia affiliate, al-Qaeda in the Indian Sub-continent (AQIS), is the weakest group in the organization's global network. Al-Qaeda remains intent on striking U.S. interests and inspiring its followers to do so but currently lacks a capability to direct attacks against the United States from Afghanistan. Separate from AQIS, there are probably fewer than a dozen al-Qaeda legacy members with historical ties to the group located in Afghanistan, and some may have been there prior to the fall of Kabul; we have no indication that these legacy members remaining in Afghanistan are involved in external attack plotting.

IRANIAN THREAT TO THE UNITED STATES

Transitioning to threats emanating from Iran and its partners and proxies, Iran continues to encourage and support plots against the United States at home and abroad, especially in the Middle East. Iran and Lebanese Hizballah have remained intent on retaliating for the death of Islamic Revolutionary Guard Corps-Qods Force (IRGC–QF) Commander Soleimani, with Iran plotting attacks against former U.S. officials.

Iran is pursuing a diverse campaign that employs legal, financial, and lethal action in pursuit of its revenge. Tehran has publicly threatened to conduct lethal operations including against former President Donald Trump and former Secretary of State Michael Pompeo, and has recently increased its threats of lethal action in the homeland. In August 2022, an Iran-based IRGC member was charged with attempting to arrange the murder of former National Security Advisor John Bolton in the United States.

Iran also pursues a campaign against anti-Iranian regime dissidents around the world, including in the United States. In July 2021, U.S. law enforcement charged an Iranian intelligence official and four others with attempting to kidnap an Iranian-American journalist in New York and forcibly returning her to Iran. At the end of July 2022, a man with a loaded assault weapon was arrested after behaving suspiciously outside the same journalist's home.

Iran has also demonstrated its willingness to engage in terrorism in the Middle East, as evidenced in June when Turkish authorities arrested members of an Iranian cell planning to kidnap and assassinate Israeli citizens in Istanbul. The plot was intended as retaliation for an alleged Israeli operation in Tehran. Separately, Iran-backed militants in Iraq and Syria target U.S. forces with unmanned aircraft systems and indirect fire attacks as they try to compel their withdrawal from the region.

EVOLVING THE CT ENTERPRISE

The complexity of the threat just outlined continues to demand a collaborative, agile, and appropriately-resourced CT effort to mitigate terrorist threats to the United States. In the 21 years since 9/11, the U.S. Government has developed just that: A highly integrated, innovative, and successful CT enterprise that continues to adapt to the nature of the threat. CT practitioners work behind the scenes every day to ensure that interconnected CT operations and programs are effectively used and employ a wide range of tools, including identity intelligence, diplomatic security, sanctions, law enforcement investigations, high-value target operations, and partner capacity-building efforts.

Even as other priorities demand attention from the U.S. National security community, CT remains foundational to our National security. The CT enterprise must preserve CT fundamentals—such as collection, warning, analysis, disruption, information sharing, and key partnerships—that ultimately give the National security community the time and space to focus on non-CT priorities. NCTC and its CT partners throughout the U.S. Government are working toward a sustainable and enduring level of support to this mission that maintains our strategic success and creates space for investments in other National security priorities.

CT in a time of competing priorities requires very purposeful and transparent decisions about when and where resource shifts can be made to retain as much of the hallmark interconnectivity and efficiency of the CT community as possible. The goal is to work with Congress to realize efficiencies while preserving the core capabilities required for the enduring mission. A key task for the CT community is ensuring those decisions are made deliberately and with a clear understanding as to the impact across the CT enterprise.

LOOKING AHEAD

Maintaining an efficient and effective CT architecture is an on-going mission, and our progress during the past 21 years has been a whole-of-Government effort, enabled by Congress' support. As we look to posture for evolving threats and National security priorities, we must ensure that we capitalize on the CT infrastructure and relationships built since 9/11 in support of other National security efforts. An interconnected threat environment fueled by great power competition, regional conflicts, and humanitarian emergencies has the potential to escalate threats quickly. We must ensure that our CT enterprise, including our international and U.S.-based partners, retains the ability to stop threats and to stay abreast of a continually-evolving threat picture.

Let me end by thanking the incredible community of intelligence, diplomatic, military, and law enforcement professionals whose dedication to the CT mission has done so much to protect this country and its citizens from a persistent and amorphous adversary. It is a privilege to be part of today's CT enterprise and to work on behalf of the American people.

Chairman THOMPSON. Thank you very much.

I thank the witnesses for their testimony.

I remind each Member that he or she will have 5 minutes to question the witnesses.

I will now recognize myself for questions.

Secretary Mayorkas, last year you said that "domestic violent extremism poses the most lethal and persistent terrorism-related threat to our country today." Is that still true?

Secretary MAYORKAS. Mr. Chairman, that continues to be our assessment in the Department of Homeland Security, that domestic violent extremism, particularly through lone actors or small groups loosely affiliated, are spurred to violence by ideologies of hate, anti-Government sentiments, personal grievances, and other narratives propagated on on-line platforms.

Chairman THOMPSON. Director Wray, what results on this domestic terrorism threat are you seeing from the lens of the FBI?

Mr. WRAY. Well, certainly we have seen over the last several years, really going back to maybe the summer of 2019, an increase in domestic violent extremism. We are concerned about the lethality, especially of racially motivated violent extremists, and then the spike that started in 2020 of anti-Government, anti-authority violent extremism. So we have very active investigations really all over the country through our joint terrorism task forces in all 56 field offices and it is a growing problem. You know, this committee is well aware of the whole phenomenon of connecting the dots and the importance of that. It is the very reason why agencies like NCTC and DHS exist in many ways. But with the lone actors and these small cells, the real problem there is there are not a lot of dots out there to connect and there is very little time in which to connect them. So that presents a whole new type of challenge for law enforcement and the intelligence community and puts a premium on our engagement with the public, with our State and local law enforcement partners in particular, who really become the eyes and ears that are so critical, because any one of them could have the one dot that we need.

Chairman THOMPSON. Ms. Abizaid, you talked about the pressure that we have applied to our international terrorist community and the results that have benefited from that pressure. Is it something that we need to increase the investment in that or increase

the relationships with other governments? How do you see that going forward?

Ms. ABIZAID. I think a sustained investment in our international counterterrorism enterprise is very important to be able to sustain the pressure against international groups going forward.

I agree with my colleagues' assessments here about the relative threat from domestic violent extremist actors here in the homeland versus international actors. Those international actors are continuing to plot and if they had an opportunity to infiltrate the United States, they would certainly look to exploit it. It is our international partners, our array of law enforcement, intelligence relationships and capabilities that enable us to stay on top of this international threat, even as we are dealing with some of those dynamics that Director Wray talked about here in the homeland that make it difficult for us to deal with a lone actor threat.

Chairman THOMPSON. Director Wray, about a third of the historically Black colleges in this country over the last year have received bomb threats. Can you enlighten us on the FBI's attempt to mitigate or capture those individuals responsible for those threats?

Mr. WRAY. Yes, Mr. Chairman.

Needless to say, we take these threats very seriously. Frankly the idea of causing the fear and disruption that they have caused is just really outrageous and unacceptable. We have joint terrorism task forces working on it, 30 field offices, multiple headquarters divisions. It is very much on-going. I think what I could say for purposes of today is that we have recently, with respect to the first big traunch of the threats, investigation has identified an underage juvenile subject and because of the Federal limitations on charging juveniles with Federal crimes, we have worked with State prosecutors to ensure that that individual is charged under various other State offenses which will ensure some level of restrictions and monitoring and disruption of his criminal behavior.

Since that big traunch that we believe that individual was responsible for, there have been two other traunches and we are very actively investigating those, but there is not much I can say on those on-going active investigations, those other investigations at this time. But we have been very engaged with HBCUs all over the country, we have done sort-of national conference calls and so forth with them to try to update them wherever we can. We recognize the fear and anger that this quite rightly causes in those communities and we are determined to see this through.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the Ranking Member.

Mr. KATKO. Thank you, Mr. Chairman, and thank you all for your testimony today. As you were speaking it just occurred to me how important this committee is and how important each of your respective work is. It is our job to do oversight and sometimes it is unpleasant. But the bottom line is we must never forget that you are at the head of keeping this country safe. I appreciate all the efforts of all of you. Sometimes you stumble like we all do, but it is also time to say thank you for what you do and how you do it.

You know, when you hear about all the threats, it is hard to really distinguish one as the ubiquitous threat, but it seems to me that one of the most pervasive threats that exists now that wasn't really

on our radar 8 years ago when I came in to Congress was a cyber issue. What we have done with respect to cyber with this committee is commendable, especially working with Chairman Thompson standing up CISA as an agency and making them at the—I like to call it the quarterback on the domestic front, and how well you have worked with the other agencies, like the FBI in that realm is great. But when you have cyber attacks, like on a water plant in Florida, which if successful would have killed thousands of people, you realize what a pervasive and probably the most ubiquitous threat we have in the United States is cyber.

So in that realm, I am very heartened to see how CISA has stepped up working in conjunction with the private sector as a partnership. It is not a regulatory-type setting, it is more of an exchange of information and how well you work with the other agencies, including the FBI as well. So that is great.

So, Chairman Mayorkas, I just want to ask you, what is your vision for CISA going forward, given the current threat environment and how important it is that we make sure CISA is strong and grows?

Secretary MAYORKAS. Ranking Member Katko, let me just thank you for your co-leadership of this committee and your service. I also want to express my thanks to this entire committee for its support of our cybersecurity mission, not only in the creation of the Cybersecurity and Infrastructure Security Agency, but also in the new legislation, the cyber incident reporting requirements, which I think are going to really strengthen the cybersecurity of this entire Nation.

I think, Ranking Member Katko, you set forth a very important blueprint for CISA and the Cybersecurity 2025. What we need to do is to strengthen—only strengthen the public-private partnership that really defines the cybersecurity ecosystem. The Joint Cyber Defense Collaborative that CISA has launched is really a tremendous success. It is not just domestic, but our JCDC, as it is known by its acronym, in our international relationships and the partnerships are going to be increasingly vital as adverse nation-states only seek to perpetuate harm through the virtual world.

Just a few weeks ago I was in Singapore for one of the world's preeminent cyber conferences and I spoke very starkly about the threat that China poses in the cybersecurity arena and how dangerous and perilous it is for countries to allow China to actually create their cyber infrastructure and how we need to combat that and create a level playing field. A competition of fairness is of course how we define ourselves, but to deal with a country that violates norms and does not act responsibly is something that we have to address.

So the public-private partnership, the international relationships, the sharing of information is so vital and that is really where we are headed.

Mr. KATKO. Thank you, Mr. Chairman, and Directors Wray and Abizaid.

Every day you wake up probably thinking the same thing I do and I look at my phone and see if there was an attack that evening or somewhere around the world, and often times, sadly, there has been. So the threat of terrorist groups, ISIS and al-Qaeda and all

the others, is still very real. I know you spent a lot of time with that.

Now, I just wish you could comment real quick and tell me if that threat matrix has changed since we left Afghanistan. Is Afghanistan becoming a breeding ground again? Is it more of a concern again?

I will start with Ms. Abizaid, please. Briefly.

Ms. ABIZAID. Yes, I would say that from Afghanistan the threat that I am most concerned about is actually from the ISIS affiliate, the ISIS Khorasan affiliate. That is a group that has demonstrated very significant capability against the Taliban in Afghanistan right now. They have conducted some attacks outside of Afghanistan and the immediate environs and I am worried about their ambition for greater and wider-spread attacks.

So it is a top priority for us.

Mr. KATKO. Director Wray.

Mr. WRAY. I would share Director Abizaid's concern about ISIS–K in the immediate term. I would just add that we are very concerned about al-Qaeda, the prospect of al-Qaeda reconstituting, given the relationship with the Taliban and that is the flip side of finding Zawahiri right in the middle of Kabul.

Mr. KATKO. Exactly.

Mr. WRAY. Then I would add to that, we are concerned about the possibility that either al-Qaeda or ISIS–K could inspire attacks here in the United States or against Americans elsewhere.

Mr. KATKO. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you. The gentleman yields back.

The Chair will now recognize other Members for questions they may wish to ask witnesses. The Chair will recognize Members in order of seniority, alternating between Majority and Minority. Members that are participating virtually are reminded to unmute themselves when recognized for questioning and then to mute themselves once they have finished speaking and to leave their cameras on so they are visible to the Chair.

The Chair recognizes for 5 minutes the gentlelady from Texas, Ms. Jackson Lee.

The Chair recognizes the gentleman from New Jersey, Mr. Payne, for 5 minutes.

Mr. PAYNE. I want to thank everybody for their testimony today.

Please bear with me a minute, I lost my——

Chairman THOMPSON. The gentleman—Mr. Payne, we hear you.

Mr. PAYNE. OK. Thank you.

Just a few weeks ago an armed man broke into the San Francisco home of Speaker Pelosi in what appeared to be an assassination attempt. Although Speaker Pelosi was not home, the intruder violently attacked the Speaker's 82-year-old husband, putting him in the hospital. This attack occurred at a tense time for our Nation with extreme rhetoric suggesting violence against public officials.

Director Wray, your own agency has also been subjected to such attacks after executing a search pursuant to a lawful warrant on the former President's residence as we saw with the incident outside an FBI office in Ohio.

To the panel, how do you assess the current threats against elected and Government officials and how do your agencies proactively protect against this violence?

Mr. WRAY. I will start off and see whether Secretary Mayorkas may want to chime in.

The phenomenon that you are describing, Congressman, I think has two pieces of it. The first is related toward violence toward all sorts of individuals in Government kind-of across the spectrum, and the second is law enforcement-specific.

On the first, we have seen a trend over the last several years of people more and more in this country when they are upset or angry about something turning to violence as the way to manifest it. That is a very, very dangerous trend. There is a right way under the First Amendment to express how angry and upset you are about something or with somebody, but violence and violence against Government officials is not it. But that is something that we have been seeing across the political spectrum now for quite a number of years.

Second, I mentioned law enforcement. It is a reality that the already dangerous profession, namely law enforcement, has become more dangerous. Last year was the highest number of law enforcement officers shot and killed in the line of duty since 9/11. I know personally because we have had agents shot and killed, we had a task force officer shot and killed, ambushed right outside one of our small offices in Terre Haute, Indiana. I call—one of the things I did when I started in this job was that I said I was going to call—every time an officer is shot and killed anywhere in the country in the line of duty, I was going to call the chief or the sheriff myself and express my condolences. I have made way north of 200 of those calls. It often is one a week and each one of those officers killed leaves behind a family, a department, and a community that will never be the same.

So the phenomenon that you described affects both Government officials as victims across the spectrum, but also law enforcement uniquely. It is a trend that we should all as Americans be concerned about.

Mr. PAYNE. Secretary Mayorkas.

Secretary MAYORKAS. Let me echo what the director said about what a tragically difficult year it has been for law enforcement.

I want to reference one additional statistic, which is this year has seen the greatest number of ambushes against law enforcement officers. There is no more noble profession than the law enforcement profession. I know a number of you on this committee have served in that capacity.

One of the areas of emphasis that the director and I have had is to be sure to disseminate timely and actionable information to State, local, Tribal, territorial, and campus law enforcement so that we equip our local communities to understand the threat landscape before them and prevent violent acts from occurring in the first instance.

Mr. PAYNE. Thank you. That was a quick 5 minutes and I will yield back.

Chairman THOMPSON. The gentleman's time has expired.

The Chair recognizes the gentleman from Texas for 5 minutes, Mr. McCaul.

Mr. MCCAUL. Thank you, Mr. Chairman. I want to thank all three of you for your service. As Mr, Katko mentioned, I know it is not an easy job.

I chaired this committee, you know, back in the day and I want to—you know, in my position being a leader now on foreign affairs, with the collapse of Afghanistan, what I have seen is a rise in our foreign nation adversary states. And the threat, quite honestly. The way it was done with the Taliban in charge of the evacuation, in charge of HKIA, a suicide bomber coming in and killing 13 service men and women, leaving Americans behind, leaving Afghan partners behind, getting Afghans on the planes that shouldn't have been on the airplanes, and got into the United States because it was so chaotic. Now, that doesn't really fall onto either of you-all's jurisdiction—perhaps Secretary Mayorkas to the extent of the screening coming in from the planes.

But then we saw Putin invade Ukraine and now we see a rising China, communist China threatening Taiwan. We see an Ayatolla close to a nuclear bomb and Kim Jong-un is firing rockets off again, now over Japan.

I argue that the world is getting more dangerous and I know that you are more domestic, but you have to look at the world and threats. It is a world-wide threat hearing to determine can those threats get into the homeland? That has always been the question, whether it be through ports and airports, which is the more typical way they do this, or what worries me now is the situation at the border. The fact that it is wide open. The combination of the Taliban taking over, Mr. Haqqani, a wanted terrorist, being their minister of interior, now minister—really of security is what he is, harboring Al-Zawahiri, who is Bin Laden's top lieutenant in his own house. I applaud the administration for targeting him and taking him out, but we don't have eyes and ears anymore. We have lost access to Bagram, and now China is in there with the lithium and we will probably get access to Bagram, that being the end result.

My question is maybe to the director of the FBI, what is your concern of the threat combination of this unmanaged wide-open border situation and the threat from al-Qaeda and ISIS coming out of Afghanistan, not to mention the fentanyl and all the other bad stuff? Then, last, the terror watch list, as I understand it, there was 98 of them. When I was Chair of this committee we would get briefed on those individuals. Not just the numbers. It is my understanding this committee is not getting the full briefing on who are these people that have attempted to get into the United States, much less the ones that already have.

Director Wray.

Mr. WRAY. Well, Congressman, you raised a number of I think very legitimate and important issues.

When it comes to the border in particular, it is a very significant and important challenge. There is a whole wide array of criminal threats that come in terms of drugs, money, guns, violence, and you mentioned some of that in your comments. There is also of course got concern from a national security perspective, any port of

entry is a possible vector that a terrorist organization could choose to exploit.

Now, historically—historically, foreign terrorist organizations have not chosen illegal immigration as the way to seed operatives, as they have usually preferred to either recruit somebody here or send somebody in legally, just because of the risks. But we have seen, you know, over the last 5 years, an increase in the number of KSTs who have been encountered who have attempted to cross. So that is obviously something we remain very concerned about. You may have seen last—early summer we announced the indictment of an individual who was trying to bring foreign nationals in in a plot to kill former President Bush.

Mr. MCCAUL. Thanks for bringing that up. That was one other thing. My time is getting ready to expire.

But I guess the point for this committee to really evaluate the threat to respond on a policy basis, we don't know who these 98 people are, where they are from. We don't really have any identifying information to know who they are, where they are coming from, how they—what was their motivation to get into the United States. So I would ask that maybe, Mr. Chairman, that we—I think this committee, as when you and I—when I was Chair and you were Ranking Member, we got that information.

Chairman THOMPSON. Yes. We will proceed to get it this time.

Mr. MCCAUL. Thank you.

Chairman THOMPSON. Thank you.

The Chair recognizes the gentleman from Rhode Island, Mr. Langevin, for 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank our witnesses for their testimony today and thank the Chairman for his kind words in his opening remarks on my leaving the committee at the end of this year. It has been a pleasure serving with everyone and I will miss the work and the people. But I thank our witnesses for being here.

So it has been 1 year since the Department submitted its report evaluating PPD 21 as required by Section 9002 of the 2021 NDAA. In a letter last week concurring with that review, President Biden acknowledged that the United States "lacks a comprehensive way to establish mandatory minimum cybersecurity requirements across our critical infrastructure and current approaches differ by sector". He also committed to working with Congress to fill gaps in statutory authorities.

So to all of our witnesses, what gaps should we be looking to fill related to improving the cybersecurity of critical infrastructure?

Then, Secretary Mayorkas, in particular the letter mentions a focused effort to help sector risk management agencies identify systemically important critical entities in their sector. How is DHS approaching this task?

Secretary MAYORKAS. Thank you very much, Congressman. I believe I caught the gist of your question.

We are doing quite a number of things to address cybersecurity and specifically in the critical infrastructure arena. Of course, the mandatory cyber incident reporting legislation that you and other Members of this committee championed is going to be so vitally important and quite frankly a model for other countries to follow.

TSA, the Transportation Security Administration, for the first time used its regulatory authority following the Colonial Pipeline attack to promulgate security directives to really require stakeholders in that sector to employ some of the more basic cyber hygiene mechanisms.

Just in the last few weeks, CISA, the Cybersecurity and Infrastructure Security Agency, promulgated its voluntary cybersecurity performance goals, which really make cyber hygiene far more understandable and accessible to a broad spectrum of industry leaders and industry participants where we recommend particular measures. We identify the cost of each measure, the prioritization of each measure, the complexity of implementation, and the benefits to be gained.

One of the areas—as I mentioned in response to Ranking Member Katko's question, one of the areas where we are also pressing very, very hard—and this touches upon Congressman McCaul's point—is the need for international collaboration, not only because of the increasingly global footprint of companies, but because of the fact that we are dealing more and more with adverse nation-states and their potential impact on the homeland.

Mr. LANGEVIN. All right. Thank you, Secretary.

Let me go to another area. The Russian invasion of the Ukraine was in some ways galvanized—it galvanized collaboration among CISA, FBI, and other Federal agencies to respond to the heightened cyber threats environment. In this case they quickly partnered with security firms and critical infrastructure stakeholders to help prepare for potential retaliatory Russian attacks.

Director Wray, how would you characterize the on-going threat of retaliatory Russian cyber attacks to U.S. critical infrastructure as the landscape of the war in Ukraine continues to change?

Secretary Mayorkas, how can we build on lessons learned earlier this year through efforts like Shields Up or the Joint Cyber Defense Collaborative to make critical infrastructure owners and operators continue to stay engaged and vigilant?

Mr. WRAY. Well, when it comes to critical infrastructure, I think I will say it has become an increasingly crowded field of threat actors targeting critical infrastructure, whether it is ransomware or some other kind of malicious cyber activity. One of the things we are particularly concerned about during the Russia-Ukraine conflict is the possibility that, for example, the Russian intelligence services, which have long targeted our critical infrastructure for espionage purposes, could choose to use the same access for more destructive purposes. It has put a premium on the kind of private-sector partnership that I know CISA, as well as the FBI, have engaged in very strongly. The private-sector partnership is the critical ingredient to defending critical infrastructure in this country. I think we have made very significant progress. There is also a lot more work to be done, but we are very much on the right path in my view.

Chairman THOMPSON. The gentleman's time has expired.

The Chair recognizes——

Mr. LANGEVIN. Thank you.

Chairman THOMPSON [continuing]. The gentleman from Louisiana, Mr. Higgins, for 5 minutes.

Mr. HIGGINS. Thank you Mr. Chairman.

Mr. Chairman, a major threat to our homeland is clearly the arterial bleed at our Southern Border and the disintegration of our sovereignty down there. The top threat to individual rights and freedoms of Americans from sea to shining sea, Mr. Wray, is the weaponization of the FBI against the American citizens that you have sworn to serve.

Secretary Mayorkas, for the record, are you aware or have you authorized CBP agents to release illegal aliens into American without identifying, screening, or vetting them properly? Or harvesting even basic biometric data, like fingerprints?

Secretary MAYORKAS. Congressman, our Nation's sovereignty stands strong and our brave men and women in the Border Patrol and throughout U.S. Customs——

Mr. HIGGINS. Are you aware or have you authorized CBP agents to release illegal aliens into America without having properly vetted, identifed them, or collected at least basic biometric data, like fingerprints?

Secretary MAYORKAS. Congressman——

Mr. HIGGINS. I mean you got millions coming across.

Secretary MAYORKAS. Congressman, our——

Chairman THOMPSON. The gentleman from—Mr. Higgins, allow the Secretary to answer.

Mr. HIGGINS. It is my time, Mr. Chairman.

Chairman THOMPSON. Well——

Mr. HIGGINS. If I want to reclaim my time, I will.

Chairman THOMPSON. Well——

Mr. HIGGINS. I am going to move on without an answer, Mr. Chairman, are you asking for me to yield you time?

Chairman THOMPSON. No, you—I am the Chair.

Mr. HIGGINS. Then I am going to reclaim my time.

Chairman THOMPSON. No.

Mr. HIGGINS. Look, we don't——

Chairman THOMPSON. Moving on now——

Mr. HIGGINS. Secretary Mayorkas——

Chairman THOMPSON. The gentleman from——

Mr. HIGGINS. Are you interrupting my time, Mr. Chairman? Or are you requesting me to yield you time?

Chairman THOMPSON. I am trying—I am trying to make sure that we conduct——

Mr. HIGGINS. You are interfering with my 5 minutes, Mr. Chairman.

Chairman THOMPSON. Well, then the gentleman will get——

Mr. HIGGINS. If you request me to yield you time, I will give you time.

Chairman THOMPSON. No, but that is not the procedure.

Mr. HIGGINS. But that is the procedure.

Chairman THOMPSON. It is not. It is not.

Mr. HIGGINS. Yes, it is.

Chairman THOMPSON. So——

Mr. HIGGINS. Of course it is.

Chairman THOMPSON. Look——

Mr. HIGGINS. I reclaim my time and I want this time back.

Secretary Mayorkas——

Chairman THOMPSON. Look——

Mr. HIGGINS. Have you used your authority to suppress exculpatory evidence——

Chairman THOMPSON. Mr. Secretary——

Mr. HIGGINS [continuing]. Presented——

Chairman THOMPSON. Mr. Secretary——

Mr. HIGGINS [continuing]. By CBP agents who have come under public attack and condemnation by DHS and the Biden administration? Have you used your authority to suppress exculpatory evidence presented by CBP agents who have come under public attack and condemnation by you and the Biden administration?

Secretary MAYORKAS. Two points, if I may, Congressman.

No. 1, in response to your second question, I don't even know what you are referring to. With respect to your first question——

Mr. HIGGINS. I will take that as that you are on the record as saying no.

Secretary MAYORKAS [continuing]. U.S. customs——

Mr. HIGGINS. That you have not——

Secretary MAYORKAS. U.S. customs——

Mr. HIGGINS [continuing]. Used your authority to suppress exculpatory evidence. If you are an honorable man, then obviously you should be able to say no to that. Who would suppress exculpatory evidence? Is your answer no?

Secretary MAYORKAS. I don't even know what you are referring to, Congressman.

Mr. HIGGINS. You will.

Secretary MAYORKAS. If I may, in response——

Mr. HIGGINS. Secretary Mayorkas, have you used your authority to retaliate against DHS agents who served on special details during the Trump administration, agents identified by your administration as conservatives or Trump supporters?

Secretary MAYORKAS. Once again, Congressman, I don't even know what you are referring to.

Mr. HIGGINS. You are before Congress. I am going to take that as a no.

Through your authority, Secretary Mayorkas, have you encouraged your chain of command to suppress basic law enforcement actions at the border and harass and victimize or intimidate experienced front-line law enforcement agents at the border using internal investigations and threats of disciplinary action or transfer in order to force those agents to comply with DHS policies that actually injure the security of our homeland and are contrary to the sworn oath of those agents? Is that the culture you have created?

Secretary MAYORKAS. Congressman, I don't even know what you are referring to.

Mr. HIGGINS. You will.

Secretary MAYORKAS. I am building a culture——

Mr. HIGGINS. Secretary Mayorkas, final question, good sir.

Secretary MAYORKAS [continuing]. Of honor and service and——

Mr. HIGGINS. It has been rumored——

Secretary MAYORKAS [continuing]. And nobility throughout the Department of Homeland Security. That is——

Mr. HIGGINS. You represent——

Secretary MAYORKAS. That is why——

Mr. HIGGINS [continuing]. Nobility, Secretary Mayorkas?

Secretary MAYORKAS. Congressman, that is what I am dedicated to.

Mr. HIGGINS. It has been rumored, Secretary, that you are going to resign prior to January 3. Is there any truth to those rumors?

Secretary MAYORKAS. That is a false rumor.

Mr. HIGGINS. All right. We look forward to seeing you in January.

Director Wray, does the FBI have confidential human sources—did the FBI have confidential human sources embedded within the January 6 protestors on January 6, 2021?

Mr. WRAY. Well, Congressman, as I am sure you can appreciate, I have to be very careful about what I can say about when——

Mr. HIGGINS. Even now—because that is what you told us 2 years ago.

Mr. WRAY. May I finish? May I finish? About when we do and do not and where we have and have not used confidential human sources.

But to the extent that there is a suggestion, for example, that the FBI's confidential human sources or FBI employees in some way instigated or orchestrated January 6, that is categorically false.

Mr. HIGGINS. Did you have confidential human sources dressed as Trump supporters inside the Capitol on January the 6th prior to the doors being open?

Mr. WRAY. Again, I have to be very careful of what I——

Mr. HIGGINS. It should be a no. Can you not tell the American people no, we did not have confidential human sources dressed as Trump supporters positioned inside the Capitol on January 6?

Chairman THOMPSON. The gentleman's time has expired.

Mr. WRAY. You should not read anything into my decision not to share information——

Chairman THOMPSON. Director Wray——

Mr. WRAY [continuing]. About confidential human sources.

Chairman THOMPSON [continuing]. The gentleman's time has expired.

Mr. HIGGINS. Thank you, Mr. Chairman.

Chairman THOMPSON. All of our witnesses are here today as guests of the committee to discuss threats to the homeland. As our guests, we owe our witnesses respect. The subject matter of today's hearing deserves thoughtfulness. The Chair encourages all Members to be polite and to take today's worldwide threats hearing seriously.

Mr. KATKO. Mr. Chairman, may I add from—I just have to—briefly.

Chairman THOMPSON. Yes.

Mr. KATKO. Just so I understand, my colleagues on my side of the aisle, if the Chairman speaks he has the authority to speak at any time he wants. If he speaks, we will make sure you get your time back. So going forward, just understand that, OK?

Thank you.

Chairman THOMPSON. Thank you, Mr. Ranking Member.

The Chair recognizes the gentleman from California, Mr. Correa.

Mr. CORREA. Thank you, Mr. Chairman. I want to thank our honored guests today for this most important discussion.

Mr. Wray, Mr. Mayorkas, Ms. Abizaid, thank you for being here.

Secretary Mayorkas, talking about counterterrorism threats to the homeland, really threats to Americans on a world-wide basis. We need strong allies around the world to protect the homeland. When Secretary Kelly was there in your position a number of years ago, I asked him about border security. We acknowledged, we agreed that border security does not begin and end at the border. If a threat gets to the border, we have got a problem.

So my question to you is do you feel like we have enough or do we need additional resources to be able to coordinate intel for the benefit of security of all Americans around the globe?

Secretary MAYORKAS. Congressman, we are working more closely than ever before with our partners——

Mr. CORREA. So if I may interrupt you, next week is World Cup—Qatar. Thousands of Americans will be there. I presume my questions to you and of course Mr. Wray, are we coordinating enough with the government of Qatar to make sure Americans will be safe there?

Secretary MAYORKAS. We certainly, Congressman, have been working with the Qataris in advising them with respect to how to enhance security to protect——

Mr. CORREA. Director Wray.

Secretary MAYORKAS [continuing]. Americans there.

Mr. WRAY. I would just agree with Secretary Mayorkas that we have been providing significant assistance and support to the Qataris in their efforts to secure the World Cup.

Mr. CORREA. You would disagree we have?

Mr. WRAY. No, I said I would agree with Secretary Mayorkas.

Mr. CORREA. You would agree. Thank you.

So I guess the next step is lessons learned. In 4 years we will have the World Cup in the United States. So any breach—I mean the government of Qatar, we hope, will have 100 percent in terms of defense there, no lapses. I hope we are there to learn their lessons because we are going to have to apply those in the United States in 4 years. Are we shadowing what they are doing?

Mr. WRAY. That is an important part of why we are providing the assistance and the support. It is not just because it is the right thing to do to help the Qataris and the——

Mr. CORREA. It is the right thing for American citizens around the world.

Mr. WRAY. It is also the right thing for America, because——

Mr. CORREA. To make sure we protect——

Mr. WRAY. Yes.

Mr. CORREA. Ms. Abizaid, any thoughts on how we can enhance security of Americans around the globe?

Ms. ABIZAID. So just on the World Cup point, I would say, you know, the Qataris are very good partners. It is a partnership that we are engaged in from an intelligence community side. We have a threat integration cell that is stationed there, as we do for all major events. The Qataris actually learned from us before we are going to be able to learn from them, when they came out during the Superbowl in Los Angeles to understand how we in the United States do security for major events like this.

So it is an on-going conversation, on-going partnership.

I would just say from an international perspective, those partnerships that you mentioned are absolutely critical to being able to secure the country here.

Mr. CORREA. Mr. Mayorkas.

Secretary MAYORKAS. I concur with that.

I should say, Congressman, that we have a very, very well exercised and trained methodology to address major events. That is throughout the interagency in the Federal Government, and we work very closely with State and local partners. This is a very evolved architecture that we have built that others learn from and we of course are in an on-going learning process.

Mr. CORREA. In my last 67 seconds I would ask all of you really that—I ask of you, which is what else can we do as a committee to make sure that we are coordinating with our allies and friends—and maybe even our unfriends around the world to make sure we stop catastrophic events like 9/11? You know, we talk about border security and 9/11, the terrorists that perpetrated 9/11 entered this country legally. We continue to focus on the border, on refugees, when the bigger issue is working with our allies around the world and other unfriends to make sure we stop those threats from happening again.

What do you need from us to make sure that that type of coordination exists and is enhanced moving forward?

Mr. WRAY. Well, one thing—obviously it would be a long list and we welcome the discussion, but the top thing on my list would be to urge Congress to reauthorize Section 702 when it comes up for renewal at the end of next year, because that is the critical tool to understanding foreign threats which may have—again, foreign threats that may have an impact on the United States.

Mr. CORREA. Mr. Mayorkas. My 6 seconds left.

Secretary MAYORKAS. We have one imminent reauthorization that is very much needed, and that is our countering unmanned aerial systems authority. I think that our budget is something that is very, very important to pass to provide us with the resources to advance our international partnerships.

Mr. CORREA. Thank you, Mr. Chair.

Chairman THOMPSON. The gentleman's time has expired.

The Chair recogizes the gentleman from Mississippi, for 5 minutes, Mr. Guest.

Mr. GUEST. Thank you, Mr. Chairman.

Secretary Mayorkas, as we here today speaking on threats to the homeland, these threats are magnified by our unsecure border. A few moments ago Director Wray in response to a question by Mr. McCaul stated the border is a challenge. He referred to drugs, money laundering, guns, and violence. You referenced some of the same information in your report. On page 13 you say that transnational criminal organizations continue to pose a threat to the United States. You speak of drug-related crime, money laundering, human smuggling. Then on page 15 in further detail, as it relates to human smuggling, you said at our Southwest Border we are experiencing historic levels of encounters. We know that those are numbers that you refer to are borne out by the statistics that your agency puts out each and every month.

Now, for the eighth straight month we have had more than 200,000 encounters along our Southwest Border. Physical year 2022, those number were more than 2,378,000, physical year 2021, 1,734,000. Compare those numbers to the last year of the prior administration, physical year 2020, those numbers were 458,000. So we see that during a 2-year period the number of encounters along our Southwest Border has increased over 520 percent.

Just taking 2022 and 2021 combined, those 2 years in which you have been in charge of this agency, we see a number that exceeds 4 million. To put that number in perspective, that is a number larger than 23 of the States that comprise the United States of America.

So looking at that, you have previously stated that the border is closed, the border is secure, and that we have not lost operational control of the border.

I ask you once again today, do you still stand by your statement based on those statistical figures, that the border is closed, the border is secure, and that we have not lost operational control?

Secretary MAYORKAS. Congressman Guest, let me share a few thoughts, because I think it is very important to put the challenge at our Southern Border—and it is a very serious challenge—in proper context.

It is a challenge that is not specific or exclusive to our Southern Border. This is a challenge that exists throughout the hemisphere.

Let me give a very powerful example.

Mr. GUEST. Mr. Mayorkas, I am not trying to interrupt you. I have very limited time and so I would like to focus my question on the Southwest Border. If we would like to meet outside this committee meeting when we have additional time—you and I have met before and I would be happy to meet with you again. But since I am now down to 2 minutes I want to focus my questioning specifically on the Southwest Border.

You have said when you have appeared before this committee that you need additional time—your agency needs additional time to get this crisis under control. We see—as Congress, we see no evidence that the situation along the Southwest Border is getting better. As a matter of fact, looking statistically, it seems like the border is getting worse. We can say these number of immigrants, we know that of these number of immigrants that we see here that have come across our border, we have statistics here that 98 people on that list—of those individuals were on the terrorist watch list.

So we as a committee, we as Congress, we as the American public, we want to have faith that you and your agency are seeking to get this challenge under control. But I am looking at statistics and statistics tell me that that is not the case. Statistics tell me that the border is only getting worse and that since this administration has taken control, that the policies that you have put in place have failed and that they have failed miserably. We know that Commissioner Magnus recently was forced to resign from office. I applaud you for removing him. I thought he did a terrible job. I hope that there are other people that you will remove and that you will work with a Republican-controlled Congress to find a way to secure the border.

So what I am hoping and what I am asking here—and I will give you the last 30 seconds of my time—is what will you do in your current position to help us secure the border? Because that is what we all want, Republicans, Democrats, we want a secure border, we clearly do not have that now. What will you help us do to make sure we get back to the levels that we saw in physical year 2020?

Secretary MAYORKAS. Congressman Guest, I very much look forward to working with you and this entire committee to enhance the security of our border.

Let me give two examples of things that we are doing and two things that I think Congress can do.

No. 1, we are taking it to the smugglers and the transnational criminal organizations at an unprecedented level. We have a disruption campaign, interagency disruption campaign that has led to more than 6,000 arrests, working not only in the itneragency, but with our international partners. We are taking it to them at an unprecedented level. No. 1.

No. 2, if one takes a look at the program that we recently implemented with respect to Venezuelan nationals, which were the highest number of encounters we were experiencing, the demographics at our Southern Border have changed dramatically over the last several years. If one takes a look at that program at its early phase, we were experiencing approximately 1,100 encounters of Venezuelan nationals a day, and since the implementation of the program, that is now approximately 300 per day. That is an example of the things that we are doing to enhance the security of our border.

Two things that Congress can do. No. 1 is pass our budget, which provides for additonal resources to the Department of Homeland Security and others to enhance our border security, including for the first time since 2011 300 more Border Patrol agents.

No. 2, once and for all, pass immigration reform, including, for example, much-needed reform to our asylum system. Everyone agrees the system is broken and we need it fixed.

Chairman THOMPSON. The gentleman's time has expired.

The Chair recognizes the gentlelady from Texas, Ms. Jackson Lee.

The Chair recognizes the gentlelady from Michigan, Ms. Slotkin.

Ms. SLOTKIN. Best State in the Union, Michigan.

Thanks for being here. I just—he has departed the room, but I just wanted to appreciate John Katko, my friend who is departing this committee, and the tone he has set in this committee. It is my fervrent hope that as the other side of the aisle seems poised to take over, that we keep this focused on homeland threats and not making this a place of political theater. That is my desperate hope and I think that is the message that was sent by the voters last week. I hope they hear it and continue in that spirit.

Second, I just want to talk a little bit about the threats that you all have talked about today, whether it is domestic terrorism and home-grown threats, the threats coming through our border, cybersecurity and the threats of ransomware, information and disinformation coming from, you know, places like Russia and China.

What has really struck me is how the threats that are most prominent for Americans today are really affecting civilians. They are not going after law enforcement agents, they are not going after our military, they are going after civilians in our K–12 shcools, in our hospitals, through our water treatment plants. The threats are much more personal and they are much more sort-of for the average American and they desperately want to know what we are doing to protect them.

Now, I was in the CIA and the Pentagon for many, many years and we are all—have to be careful not to fight the previous war and to make sure that we are adapting to today's threats.

Particularly on cyber, I am worried that we have had—you know, as we remember 9/11, we had the attacks in Kenya, we had the attacks on the *U.S.S. Cole,* and then we had 9/11. I feel like on our cyber attacks we have had our *U.S.S. Cole,* we have had the Colonial Pipeline, we have had our meat processing facility, we have had SolarWinds. So we all thought about what would we have done if we could have imagined the threat of 9/11, what would we have done to better prepare.

So, Secretary Mayorkas, please tell me the two or three things that you wish you could do—either you need the resources or you need the attention of the American people—to prevent a cyber 9/11.

Secretary MAYORKAS. Congresswoman, in my opening remarks I talked about the threat landscape and how in fact the goal of our adversaries is indeed to disrupt our way of life. I think you captured that very well in your opening remarks.

We have done a great deal to enhance the security of the cyber ecosystem. When I say we, it is not just the Department, but of course working very closely with our partners. That is No. 1, to equip the private sector with information and to educate them on the tools to advance cyber hygiene. We have done that for the civilian population as well.

If we take a look at some of the very accessible sites that we have created on the web, stopransomware.gov, CISA.gov, some of the very simply measures that people can take, whether it is multifactor authentication, backing up one's systems, using safe and secure passwords. These are the things that we need to do and continue to do. The more that we can amplify collectively—we in the Government, in Congress—the imperative of maintaining cyber hygiene, raising the alertness of the average citizen to the imperative, especially in the increasingly interconnected world, I think that is one critical goal.

Ms. SLOTKIN. Yes. I would offer, it would be useful if we had a list of specific things, your asks, right. We all want to prevent these cyber attacks. I think cyber issues are very bipartisan in this Congress and have been and hopefully will be in the future Congress. So please be assertive with what you need in order to protect the American people, because they feel like they don't know what is defending them.

Second, Director Wray, I was heartened to hear your story of calling all the families of fallen law enforcement that have been killed over the past year or time that you have been in service. I am very worried. Just coming out of campaign season, the number

of people who think that the FBI is a political tool, as we heard even raised in questions here today.

Can you please talk to the American people about the FBI and explain in your words why they should trust their Federal law enforcement?

Mr. WRAY. So there are a lot of opinions out there about the FBI, just like there are about everything. By my opinion, the window that I get to see into our work force is unique. I have visited all 56 of our field offices at least twice, I have spoken with law enforcement from all 50 States on countless occasions, I have met with judges, prosecutors, community leaders, victims and their families, and the FBI that I see every single day and that I hear about from all of them, is an FBI that does the right thing in the right way with rigor, with professionalism, with objectivity, with skill. I will stack our work force up against anywhere in the world any time. The Americans should have deep confidence in those people.

I will add that when it comes to perceptions of the FBI that the number of Americans all across this country applying to be special agents in the FBI has been going up—up significantly over the past 3 years, at a time when as I hear all the time, law enforcement all over this country is having the opposite experience. I think that speaks very well of Americans in every State represented on this committee.

Ms. SLOTKIN. Thank you.

I yield back.

Chairman THOMPSON. The gentlelady yields back.

The Chair recognzies the gentleman from North Carolina for 5 minutes, Mr. Bishop.

Mr. BISHOP. Thank you, Mr. Chairman.

Secretary Mayorkas, Mr. McCaul said the border is wide open, Director Wray testified about an elevated threat of guns and money and drugs across the border. Mr. Guest laid out a lot of the details about the record-breaking numbers. He ended up having to talk more than get an answer from you on something.

I just want to ask you—I have heard you in the Judiciary Committee recently in the summer testify that the border is secure. Secretary Mayorkas, do you continue to maintain that the border is secure?

Secretary MAYORKAS. Yes. We are working day in and day out to enhance its security, Congressman.

Mr. BISHOP. All right. Thank you, sir.

Secretary MAYORKAS. We have——

Mr. BISHOP. Sir, I——

Secretary MAYORKAS [continuing]. Remarkable——

Mr. BISHOP. I get it. I just wanted to make sure that that still is your assessment.

Secretary MAYORKAS. It is very——

Mr. BISHOP. Director Wray——

Secretary MAYORKAS. It is and it is very important—if I may.

Mr. BISHOP. Well, I don't—I know, there is just not enough time for a lot of explanation and you have got written testimony and so forth. I just wanted to understand that is your position still. I think it is a position that denies reality, respectfully. But I wanted to

give you the opportunity to say no, I think the situation has changed or something like that.

Director Wray, do you believe that the border is secure?

Mr. WRAY. Well, I can only speak to border security from our narrow lane, but I can speak to it from that lane. What I would say is that we see significant criminal threats coming from south of the border, whether it is guns, drugs, money, violence. We see transnational criminal organizations that are sending their drugs here and that are using street gangs here to distribute it, and that contributes to the violent crime crisis here. We have had takedowns just in the last few months that I could give you as an example.

You know, I will give you just one quick one. You know, in Phoenix we had a takedown working with CBP, who are phenomenal partners I should add, where we seized in one vehicle interdiction enough fentanyl to kill the equivalent of the entire State of Pennsylvania.

Mr. BISHOP. Yes, that is very troubling.

Mr. WRAY. Just one vehicle interdiction.

Mr. BISHOP. Thank you, Director Wray.

Director Abizaid, does the NCTC asses a significant threat from the historic level of uncontrolled crossing at the Southern Border?

Ms. ABIZAID. Thank you.

We don't actually. Border security is really important. If we look at the nature of the threat and how it has evolved here in the United States homeland, it has been striking how the evolution to lone actors actually reflects how much more difficult it is for terrorists to enter into the United States.

We look historically at the kind of attacks we have experienced here in the homeland. None of them have been connected to major illegal crossings or otherwise from the Southwest Border.

Mr. BISHOP. Right.

Director Wray——

Ms. ABIZAID. That said, it remains a top intelligence priority.

Mr. BISHOP. Director Wray spoke to that earlier about what has historically been true. It makes me mindful of the 9/11 report, that chapter that said the system was blinking red. It was a failure of the U.S. Government agencies to anticipate a threat that should have been obvious to everyone.

So it troubles me that the official response is we don't think that is much of a threat. We have an unprecedented number of people coming across the border, a lot of them are being interdicted, but released into the United States without enough scrutiny. A whole lot more apparently coming in without being interdicted at all. The official answer is, hmm, we don't think there is a terrorism problem there. Just hasn't happened in the past.

I think unfortunately we are going to find out if it happens in the future.

Mr. BISHOP. Reporting from the *Intercept* focused on the Department of Homeland Security—and I guess CISA has been the focal point for it—interactions with social media companies.

One thing it related was that DHS sent an email to Twitter about a Twitter account that could imperil election system integ-

rity. The user had 56 followers and a bio that indicated—had references to weed shops.

Secretary Mayorkas, does that kind of—and the level of interaction with social media platforms and that one specifically, that anecdote, not suggest that DHS is engaged with egregious overreach that threatens the First Amendment?

Secretary MAYORKAS. Congressman, I would note that the *Intercept* article focuses attention on the disinformation activities that preceded our administration. Let me assure you that our work to address disinformation, which is a tool that our nation-state adversaries seek to employ to sow discord in this country, is something that is very, very respectful of the civil rights and civil liberties of individuals, as well as their privacy rights.

Mr. BISHOP. You maintain that always, but let me just ask, when you say it is respectful, are you attempting to conduct censorship by proxy as a means of evading the First Amendment?

Secretary MAYORKAS. We absolutely do not.

Mr. BISHOP. My time is expired.

Chairman THOMPSON. The gentleman's time has expired.

The Chair recognizes the gentleman from Texas, Mr. Green, for 4 minutes.

Mr. GREEN. Thank you, Mr. Chairman. I thank the Ranking Member as well and appreciate greatly the commentary that you both gave earlier with reference to collegiality and an effort to get the optimum from this committee based upon the things that we can agree upon. I thank you both.

Mr. Chairman and Members, I am on a mission of mercy today. I am on a mission of mercy because of immigration laws and a need for comprehensive immigration reform. Please allow me to call to your attention, Mr. Secretary, the case of one Mr. Jaime Abavos Rosales. I would like to have additional conversations with you about this because there is no way for me to give you the intelligence necessary at this time, the entirety of it.

In 1996 Mr. Avalos came to this country at the age of 1 year. In 2013 he received DACA. He graduated from a high school in Houston, Texas, Bellarie High, 2014. No criminal record, Mr. Secretary. Married his wife, Yarianna, and they now have a child who is approximately 1 year of age.

Mr. Secretary, pursuant to the laws, he went back to Mexico, to Juárez, to the consulate in an effort to submit himself for re-entry into the country in a lawful fashion. The law permits this. It was discovered that he was brought back to Mexico at about the age of 7. Came at the age of 1, taken back at the age of 7. Because he was taken back to Mexico at the age of 7, a child, he is now barred from this country for 10 years. He had an appointment with the consulate, went there in good faith. Came here as a child, went back as a child, and because he went back as a child he is now barred for 10 years.

Won't be with his baby, won't have Christmas with the child. A very sad circumstance that if it doesn't impact one's heart, I am just sorry for the lack of sympathy and empathy that some people may have.

So I am appealing for some help. He is not a criminal. He didn't bring himself here, he didn't come on his own volition, he came as

a child. I am trying my best to bring him home. I am going to Mexico to visit with him. I will be taking his wife and his baby. She is an American citizen, the baby was born in this country. They will be going with me. I would like to bring him home and I would like to ask as much help as I could get from you and from our Government.

Let me say this before you give a brief response. I appreciate President Biden. He inherited a tough, tough job, a tough position. But he knew what he was inheriting and he has taken up the challenge admirably—admirably. I compliment you on doing the best that you can under the circumstances that exist and the laws that exist. The border is about as secure as it can be given the laws that we have. It is lawful for people to ask for asylum. That is lawful. It is lawful for us to consider the request. About as secure as it can be given the laws that we have. You can't change the laws, but we can. That is why we, many of us, keep in insisting on comprehensive immigration reform, so that we can deal with the situations that include Mr. Jaime Avalos Rosales. This needs to be dealt with. Shouldn't be banned because his mother took him home to register his birth as a child of 7 years. There is a law that requires persons who leave the country, once you are here, to go back to your consulate and then apply and be given consideration. But if you leave and come back to the country prior to your making that application, you are banned.

So I am hoping that we can do something to help him. I would like to know if I can visit with you, talk more with you about this, and many other cases of course. But I would like to visit with you.

I yield to you, sir, Mr. Secretary.

Secretary MAYORKAS. Congressman, I am of course not familiar with the case that you have described. I can say that U.S. Citizenship and Immigration Services, the agency that deals with administration of our legal immigration system, receives on almost a weekly basis cases that present tremendous heartbreak and sadness because of how broken indeed our system is. Those pleas for mercy, come from both sides of the aisle.

Chairman THOMPSON. The gentleman's time has expired.

The Chair recognizes the gentleman from New Jersey for 5 minutes, Mr. Van Drew.

Mr. VAN DREW. Thank you, Mr. Chairman, thank you Ranking Member.

Just very briefly, I respect Mr. Green very much and I feel for his passion. I would like to say though that there are a lot of people right now in the United States of America that are going through their own personal hells for many reasons, whether it is drug addiction, whether it is homelessness, whether it is problems that our Americans who live here and work here and try to function to here have, and I think our immigration system, respectfully, we are not doing as good as we could do. I believe that we could do much, much better. Quite frankly, we were doing much, much better.

Secretary Mayorkas, when you testified before this committee in September of last year, you stated that DHS continues enforcing our immigration laws and to my surprise you said that we were responsibly managing our border. In the last fiscal year, there were

over 2.3 million recorded migrant encounters at the Southwest Border, which included 98 non-U.S. citizens who were on the terrorist screening dataset. As you know, these figures do not represent those who avoided detection, which was estimated to be around 600,000. To attempt to combat the crisis on the border, you have deployed highly-trained and highly-skilled Federal air marshals to the border to perform non-law enforcement duties, such as hospital watch, transportation, and welfare checks. There have even been reports that marshals are performing janitorial duties.

I have the largest air marshal training center in the United States of America in my district and I have seen first-hand how talented and capable they are. DHS is removing hundreds of air marshals from the skies during one of the busiest travel seasons of the year, even though have stated that America's aviation infrastructure is a very high threat and is a target.

Furthermore, DHS is even classifying how many high-risk flights are not being covered due to your decision to deploy air marshals to the border. How do you justify this deployment? Don't you think it would make more sense to hire more Border Patrol agents who are trained for this and finish the wall—yes, finish the wall—rather than to continue to mishandle the crisis? But now, we are mishandling it at the expense of aviation security. So where we had one problem, which is a terrible problem—and I disagree with you thoroughly that there isn't a problem. That we can turn the TV on now on just about any news station and you can see what is going on. This is not rocket science, it is not complicated. The American public can see it, everybody can see it. It affects the whole country. But instead of having just one problem, now we have two problems because what we are doing to the air marshals. Enough is enough. Why can't we just do the right thing, the simple thing, and the functional thing? Why can't we go back to where we were where we had so much less of a problem?

Secretary MAYORKAS. Congressman, a few thoughts.

First of all, thank you for accurately describing the expertise, the professionalism, and the bravery of our Federal Air Marshals. Of course it is false that they are deployed to the border to conduct janitorial services. We have contract personnel to do that.

You make a very, very important point. You asked the question why can we not hire more Border Patrol agents out in the field. I think that is a very appropriate question and there is a very compelling answer for that. You know, for the first time since 2011 we have presented to Congress a budget that seeks to plus-up our Border Patrol agent personnel. We requested a budget to re-fund 300 more Border Patrol agents. Every single year since 2006 I believe it is, the Department of Homeland Security has relied on the Department of Defense to augment its resources to address the challenges at the border. So this is not something new.

I look forward to working with you to see what we can do to pass a budget that calls for additional resources for the Department of Homeland Security to address the challenges not only at the Southern Border, but all of the challenges we are describing.

Mr. VAN DREW. Secretary, I appreciate that and I don't mean to interrupt you, but I have like 5 seconds here.

The problem with the budget is there is so many unpalatable unacceptable other parts to it that. As you know, it is the old game that is always played in politics, jam a budget or jam a bill, or whatever it is with all kinds of other issues and initiatives that a lot of people don't want to see. If we had a stand-alone appropriation to do this, to fund this, you would see it go through in a second.

So if you want to fight for that, I will fight by your side to get more Border Patrol agents, I will talk to the President, as I know that you would, and let us see what happens. But it shouldn't be jammed with all kinds of other initiatives that we don't want.

Chairman THOMPSON. The gentleman's time has expired.

The Chair recognizes the gentlelady from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. I thank the Chair and the Ranking Member for this very important hearing and oversight assessment. Let me add my appreciation to Ranking Member Katko for the years of service we have had to work together in a mutual commitment to securing the homeland. Thank you for your service to the Nation. As well continue to thank you for your previous service. I thank the Chairman again for bringing us together around this important issue.

To our witnesses, let me acknowledge the 20th year of Homeland Security and the men and women who worked under that umbrella to thank them for that service.

Director Wray, let me also affirm the admiration and respect of the FBI, and I would frankly say law enforcement around the Nation and express my concern for the violent incident that happened in Cincinnati and appreciate the fact that—safety of those men and women.

Let me build on the tragedy that fell upon the second-in-line to the Presidency, the Speaker of the House, and ask the question about the depth and intenseness of political violence. Again, our time is brief, but I would like to yield to the Secretary first, Director Wray, and to Director Abizaid if we might. I do have other questions, so let me just quickly yield. Just the depth of political violence, which means speech driving people to violence.

Secretary MAYORKAS. Congresswoman, we of course are engaged to when in fact there is a connectivity between an ideological view, a political view, and violence. That is when we get involved and we all—the Director and I in our opening statements and in response to preliminary questions spoke of the gravity of the threat that the lone actors and small cells pose when they are driven to violence because of a political ideology, ideologies of hate, anti-Government sentiments, personal grievances, and other narratives propagated on on-line platforms. This is one of the greatest terrorism-related threats we face in the homeland.

Ms. JACKSON LEE. Director Wray.

Mr. WRAY. Well, Congresswoman, as I mentioned earlier, we have seen a clear trend in this country over the last several years of people across the political spectrum choosing to express their anger or upset at someone or about something through violence. That is a very alarming trend. As Secretary Mayorkas referenced,

it is exacerbated on-line, but it is a clear phenomenon that we are having to contend with that started several years ago.

Ms. JACKSON LEE. It is going up?

Mr. WRAY. It is going up.

Ms. JACKSON LEE. Thank you.

Director.

Ms. ABIZAID. I would concur with my colleagues. You know, as we look at the numbers since 2010, we see that domestic violent extremism accounts for 47 attacks, over 152 deaths. That actually pales in comparison to the 45 attacks that we have seen since 9/11 by foreign terrorist organizations.

Ms. JACKSON LEE. Let me just—can I get a yes or no answer on this, because I have some other questions? Is a cyber threat coming from China and Russia intense, continuing, and on-going?

Ms. ABIZAID. Cyber threat, I will defer to my colleagues in the FBI and DHS.

Ms. JACKSON LEE. Director Wray.

Mr. WRAY. Yes.

Ms. JACKSON LEE. Thank you.

Director Mayorkas, let me try to—my understanding is that immigration, defense of the border, protection of the border, is a Federal responsibility. Is that not correct?

Secretary MAYORKAS. That is correct.

Ms. JACKSON LEE. Have you see any positive impact from the $4 billion that has been spent by Governor Abbott of the State of Texas who continues to malign the work of the Federal Government and, to some extent, interfere with it and cause the National Guard, some of whom have committed suicide, to—Texas National Guard to be strained? I am going to ask that question in the context of what Director Wray said in terms of an answer to the question about security at the border. I think it is important to distinguish between even though we want to stop that flow, to distinguish fleeing families with children from Venezuela, Cuba, Haiti, et cetera, from the work, the strain of cartels, of smuggling, of human smuggling, smuggling of fentanyl. Those criminal elements, we are all fighting I assume to bring that down.

Can you distinguish and tell me whether you have seen any impact from the $4 billion that one State happens to be using of State tax dollars taken away from the needs of the people of Texas that has impacted the work that you are doing as a Federal officer to protect the border?

Secretary MAYORKAS. Congresswoman, let me answer the question this way. We advance law enforcement mission when we work collectively, collaboratively, and in a coordinated way. When there is a deliberate effort to not coordinate, it can and indeed has been quite counterproductive.

Ms. JACKSON LEE. Thank you.

Chairman THOMPSON. The gentlelady's time——

Ms. JACKSON LEE. Thank you.

Chairman THOMPSON [continuing]. Has expired.

The Chair recognizes the gentlelady from Iowa, Mrs. Miller-Meeks, for 5 minutes.

Mrs. MILLER-MEEKS. Thank you, Mr. Chair, thank you, Ranking Member Katko.

First I would also like to thank all of our witnesses for coming before the committee today. I am glad we are finally having the ability to seriously discuss the threats we are facing, particular along our Southwest Border.

Let me also say that prior to January 20, 2021, we had lawful operational control of the Southern Border.

The number of unaccompanied alien children, UACs, encountered along the Southwest Border has nearly doubled since 2019 and continues to increase, surpassing a record high in fiscal year 2021, approaching nearly 153,000 this fiscal year. We have heard reports of children being sent alone—I have encountered them when I have made trips to the border—across dangerous terrain with nothing but a relative's name and address pinned on their shirt. Some of these children so young as to not know their own name or to whom they are supposed to be sent. We have seen Border Patrol agents bravely fight to save young kids and infants in medical distress and in crossing the river.

When we have encountered these families—and I distinctly remember an occasion with Representative Carlos Gimenez and Representative Maria Salazar, who spoke their language, asking them specifically whether or not the Biden administration's policies, often cited directly by these migrants crossing the border, encouraged foreign nationals to send their children to seek entry into the United States despite dire conditions at the border.

Secretary Mayorkas, are the Biden administration's policies encouraging and increasing the pull factor for unaccompanied minors, UACs, to come into this country?

Secretary MAYORKAS. Congresswoman, a few thoughts, if I may.

First of all, thank you very much for capturing the vulnerability of unaccompanied children that migrate from their countries of origin and seek safety, not only in the United States, but elsewhere in the hemisphere, as I said at the very outset. I don't know——

Mrs. MILLER-MEEKS. Sir, I want to be respectful. I have limited time, so.

Secretary MAYORKAS. Yes. This is a challenge that we are experiencing throughout the hemisphere.

I also want to thank you for recognizing the bravery of the Border Patrol.

Mrs. MILLER-MEEKS. Thank you very much. I am going to relate back to my instances of appearing at the border and hearing directly from people crossing the border that the administration's policies in fact are a pull factor.

Given that, what actions are being taken at the Department to keep these kids safe and stem the flow of UACs crossing illegally into the United States across dangerous terrain?

Secretary MAYORKAS. So a few things. Of course I disagree with the premise of the pull factor.

As I was saying, this is a hemispheric challenge. We are seeing a tremendous amount of upheaval throughout the Western Hemisphere, authoritarian regimes, poverty, violence, corruption, and the like. We are doing a number of things, and let me give you two examples.

No. 1 is we are taking it to the smugglers in an unprecedented way. Throughout the Department of Homeland Security, through-

out the interagency, and with our partner countries to the south of our border. We have in the last year conducted more than 6,000 arrests in an unprecedented disruption effort to attack the smuggling organizations that seek to exploit the vulnerable.

Mrs. MILLER-MEEKS. Thank you.

Secretary MAYORKAS. But, No. 2——

Mrs. MILLER-MEEKS. I can say that when I have been——

Secretary MAYORKAS. No. 2——

Mrs. MILLER-MEEKS [continuing]. To the border and talked with the agents, the cartels seem to have tremendous control over what happens.

Secretary MAYORKAS. Yes, if I may, Congressman, just—I——

Mrs. MILLER-MEEKS. Sir, I only have 1 minutes 16——

Secretary MAYORKAS. Congresswoman——

Mrs. MILLER-MEEKS [continuing]. Seconds left. After being apprehended by the DHS, unaccompanied alien children are transferred to the Office of Refugee Resettlement within the Department of Health and Human Services. While this is supposed to occur within 72 hours of arrival, decrease in the amount of time children reside in CBP facilities, many unaccompanied children have remained in CBP facilities longer than the time allotted under Federal law. Is the large scale of UACs crossing the border contributing to these overstays in CBP facilities? How is this being addressed, No. 1? No. 2, how is the DHS managing the threat of sexual predators at the border, during CBP facilities detentions, as well as during the transfer of children to different locations?

If you don't have time to answer, you can respond to us in——

Secretary MAYORKAS. Congresswoman, we are also building lawful pathways, such as the Central American Minors Program. So children do not place, and their parents do not place, their lives in the hands of exploitative smugglers.

The information that you have with respect to the length of stay in the Border Patrol facility is I think quite dated. That was certainly a challenge that we faced in March 2021, but we have taken considerable measures to meet the 72-hour time frame. I look forward to providing you with further information.

Mrs. MILLER-MEEKS. Thank you so much.

Mr. Chair, I yield my time.

Chairman THOMPSON. The gentlelady yields back.

Pursuant to the order of the committee of today, the committee stands in recess for approximately 5 minutes.

[Recess.]

Chairman THOMPSON. The committee will be in order.

The Chair recognizes the gentlelady from New York, for 5 minutes, Ms. Clarke.

Ms. CLARKE. Thank you, Mr. Chairman. Like so many of my colleagues, I would like to thank Mr. Katko for his service. My colleague from New York. His commitment to bipartisanship and his commitment to the work of this committee has been uplifting. To all of our public servants seated here today, thank you for your service and commitment to the American people.

My question is really around cybersecurity. That is something that I really had a keen, keen interest in. We have recently this year passed legislation that I authored requiring the reporting of

major cyber incidents to CISA. Although CISA has 3½ years to issue a final rule, Mr. Secretary, none of us want to wait that long. My hope is that swift implementation will yield important security benefits, eliminate duplicative reporting frameworks, and encourage harmonization across the interagency.

Toward that end, I have two questions for you. What is DHS doing to support—and more specifically—expedite this rule making so we don't have to wait years to see results? How is DHS working with the SEC and other regulators to harmonize new requirements through, for example, the Cyber Incident Reporting Council established in CIRCIA?

Secretary MAYORKAS. Congresswoman, thank you so much for championing this critical security effort, cybersecurity effort.

We are already engaging with the private sector in preparation for the promulgation of the regulations that will implement the new legislation. It is vitally important, as you and other Members of this committee know who have championed this imperative, public-private partnership is the bedrock, the foundation of the cybersecurity ecosystem. So we already have begun to engage with the private sector in anticipation of the regulations that we will issue. No. 1.

No. 2, we have a council that we are chairing that is working across the interagency to ensure to the best of our abilities, harmonization of the reporting requirements. I should say that we have also taken that critical harmonization need and expanded it in the international domain, speaking with our international partners and seeing what we can do—given the multinational footprint of so many of our companies—to see what we can do to harmonize the landscape internationally as well as domestically.

Ms. CLARKE. Well, I am happy to hear that, you know, we are sort-of prepping, but do you have a sense of whether we can expedite the rule making so that it doesn't take us the 3½ estimated years to get to the final rule?

Secretary MAYORKAS. So I believe that there are set time frames in the statutory regime with respect to the promulgation of regulation. I think we have, if I am not mistaken—and I will correct myself subsequently if I am—that we have 18 months. We have what I would respectfully submit is the preeminent regulatory team to ensure the swift promulgation of the necessary implementing regulations.

Ms. CLARKE. In addition to the cyber incident reporting, I see the Cyber Safety Review Board, the CSRB, is another innovative way this administration has tried to better understand cyber threats. Does the administration intend to seek authorization for the CSRB? If so, what should those authorities entail and what does the CSRB plan to study next?

Secretary MAYORKAS. So that is—Congresswoman, thank you so much for recognizing the tremendous value of the Cyber Safety Review Board. It is very important to emphasize that that is a board that is not focused on accountability, but is focused on the diagnosis of the challenge and remediation of any potential harm that the challenge presents. Its first project was the Log4j Vulnerability. It is now preparing to issue a report. One of the things that we are considering is the authorization of the CSRB and what further sup-

port we can receive from Congress. We are very appreciate of the support we have received to date.

Ms. CLARKE. Mr. Secretary, in response to Congresswoman Slotkin's question, you raised the issue of cyber hygiene and the work that is being done from the administration's standpoint, certainly from the Congressional standpoint. I would like to include the private sector.

One of the things that I have been concerned about is that we can't amplify enough the need for there to be a National movement around cyber hygiene. Every weak link presents a vector for our adversaries to take us down. So I want to put on your radar as you speak with the private sector, perhaps looking at some public service announcements so that there is an educational campaign that is consistently out there in the public and that we grow up with the habit, like putting on our seatbelts, of regularly addressing our cyber hygiene.

With that, Mr. Chairman, I yield back.

Chairman THOMPSON. The gentlelady yields back.

The Chair recognizes the gentlelady from Tennessee, Mrs. Harshbarger, for 5 minutes.

Mrs. HARSHBARGER. Thank you, Mr. Chairman. I thank the witnesses for being here today.

I am going to read a statement. This is for all the witnesses. Late last month *Forbes* and other press reported that TikTok's parent company ByteDance planned to use TikTok to monitor the physical location of specific Americans for the purposes of surveilling individual U.S. citizens. As you know TikTok is close to signing a CFIUS contract and the Treasury Department has been assessing the National security risk of foreign ownership of TikTok, including its CCP ties of whether the platform enables the Chinese government to access U.S. person's data.

The first question is a yes or no. It is: Do you assess that TikTok is a significant National security threat given the accusations that the company specifically targets U.S. persons and given the ByteDance and TikTok ties to the CCP?

The second part of that question is yes or no. Is the CCP leveraging the application as a tool to collect information about U.S. citizens for the purposes other than targeted ads and content?

Anyone on the panel.

Mr. WRAY. Congresswoman, taking the first question, I would say we do have National security concerns, at least from the FBI's end, about TikTok. They include the possibility that the Chinese government could use it to control data collection on millions of users or control the recommendation algorithm, which could be used for influence operations if they so chose or to control software on millions of devices, which give it opportunity to potentially compromise personal devices. So there are a number of concerns there.

As to what is actually happening and actually being done, that is probably something that would be better addressed in a closed Classified setting. I could see what information we might be able to share that way. But there is probably not much more that I could add to that, other than to say it is certainly something that is on our radar and we share your concerns.

Mrs. HARSHBARGER. Yes. Thank you for that. I would love to have that close briefing.

Has ByteDance responded to allegations that their internal auditing system specifically targeted any members of the U.S. Government, activists, public figures, or generalists? Yes or no.

Mr. WRAY. I will have to see if we can get back to you on that. I am not sure that I can give the answer right here at this moment.

Mrs. HARSHBARGER. OK. Are you informing the Treasury's view through the CFIUS process of the National security threat it poses?

Mr. WRAY. I'm sorry, ma'am, I didn't——

Mrs. HARSHBARGER. Sir?

Mr. WRAY. Repeat the question. I just couldn't hear you very well.

Mrs. HARSHBARGER. Are you informing Treasury's view through the CFIUS process of the National security threat it poses to the United States?

Mr. WRAY. Yes. The FBI's foreign investment unit working through the Department of Justice is part of the CFIUS process and would be relevant. Our input would be taken into account in any agreements that might be made to address the issue.

Mrs. HARSHBARGER. OK. Last part of that question is what is currently being done to investigate the CCP's involvement in TikTok ownership, direction, and/or access? The reason I ask that is there was a current *60 Minutes* segment highlighting the stark differences between the Chinese-owned TikTok company that allows kids in China to view a totally different app, a clean app, and what is shown in the United States—they call it an "opium version"—that is designed to hook American children on an unsafe version of the video-based platform, you know, offering a healthier version and a limited viewing of 40 minutes for those children in China, which is unacceptable and parents need to know this. But what is currently being done to investigate the CCP's involvement in TikTok?

Mr. WRAY. Well, as to any specific investigative work, I could see whether some of that could be incorporated into the Classified briefing I referred to. There are obviously limits on what I can share in terms of discussing a specific on-going investigation.

But what I would say is that you have highlighted two very, very important threats. One, of course, something we are all concerned about, which is the threat to our youth on-line. But the second——

Mrs. HARSHBARGER. Yes.

Mr. WRAY [continuing]. Is the threat specifically from the Chinese government and the Chinese Communist Party and the ways in which their laws are used as an aggressive weapon against both U.S. companies and Chinese companies. Under Chinese law, Chinese companies are required to essentially—and I am going to shorthand here—basically do whatever the Chinese government wants them to in terms of sharing information or serving as a tool of the Chinese government.

So that is plenty of reason by itself to be extremely concerned.

Mrs. HARSHBARGER. Absolutely. Well, I look forward to the Classified briefing and I appreciate your time.

With that, Chairman, I yield back.

Ms. DEMINGS [presiding]. The gentlewoman yields back.

The Chair now recognizes the gentleman from California, Mr. Swalwell, for 5 minutes.

Mr. SWALWELL. Thank you. To the witnesses and the people in law enforcement that you represent, you are owed our thanks to your service to our country. You are not owed the bitter, divisive, cruel, violent rhetoric we heard from our colleague from Louisiana. That is a rhetoric that the voters rejected, an extreme rhetoric that voters rejected last Tuesday. Our Chairman of the committee, Mr. Thompson, was also not owed that display.

Director Wray, antisemitism is on the rise across America. The White House has recently proposed $360 million for nonprofit security grants that can assist community centers—and also Secretary Mayorkas. We funded that to the tune of $250 million in this committee and it was also a partnership between Chairman Thompson and Ranking Member Katko. But if we provided additional funding, what would that mean for combatting antisemitism in America?

Secretary MAYORKAS. Thank you very much, Congressman Swalwell.

You know, the Nonprofit Security Grant Program when I first addressed it was funded at $180 million and we are grateful for the support of this committee in funding it at the level of $250 million. What we would do if that funding increased to $360 million, which we certainly advocate that it does, is enable us to also fund target-rich resource or institutions that are vulnerable to attacks. That includes places of worship that guard against antisemitism. It is true of churches, synagogues, mosques, all sorts of nonprofit organizations, including historically Black colleges and universities that have seen a tremendous uptick in bomb threats, as Director Wray referenced earlier. That is much-needed funding because there are target-rich but resource-poor institutions, schools, places of worship that need to enhance their security against an ever-increasing threat.

Mr. SWALWELL. Great. Thank you, Secretary.

Director Wray, many of my Republican colleagues have run on a defund the FBI platform. They have made t-shirts, hats to fund their campaigns. If the FBI was defunded, would that hurt or help terrorism investigations?

Mr. WRAY. It would hurt. Just in the last several years, the FBI has thwarted terrorist attacks in places like Las Vegas, Tampa, New York, Cleveland, Kansas City, Pittsburgh—and those are just the ones I can think of off the top of my head. So we need more funding for those efforts, not less.

Mr. SWALWELL. If the FBI was defunded, would that hurt or help child exploitation investigations?

Mr. WRAY. It would hurt. We have a very, very active violent crimes against children program. We are literally arresting thousands of child predators and rescuing hundreds and hundreds of kids. So, again, we need more funding for that, not less.

Mr. SWALWELL. If the FBI was defunded, would that hurt or help COVID fraud investigations for money that went into the communities during the time of COVID?

Mr. WRAY. Well, again, it would hurt. We have a very active COVID fraud investigative program working with other agencies as partners, the Department of Justice Inspector General, et cetera. Given the remarkable amount of monies that were involved, courtesy of this Congress, it is important that we ensure the integrity of that spend so that it not be wasted on—I have been briefed by agents on cases involving, you know, violent gangs that have tapped into some of the COVID fraud money.

Mr. SWALWELL. Thank you.

Secretary Mayorkas, do you support the GOP plan for the border?

Secretary MAYORKAS. Congressman, I very much look forward to working in a bipartisan way to address the need to enhance our border security.

Mr. SWALWELL. I guess do you know what the GOP plan is for the border?

Secretary MAYORKAS. I do not. I want to work in a bipartisan way to address what is a unanimously understood to be a broken immigration system.

Mr. SWALWELL. I agree, Secretary.

Secretary MAYORKAS. I want to work——

Mr. SWALWELL. My point is I have not heard a plan, I have just heard grievances.

Finally, Director Wray, last week the "parliament in Iran" voted to execute 15,000 protestors, many of them teenagers and women. One of those members of parliament is actually in the United States right now at the United Nations, presumptively under diplomatic cover. Do we need more resources or should we reconsider who we allow to come to the United States? You know, after you have voted for such an atrocity, it just really concerns me that people could be enjoying themselves in New York after signing, you know, a death warrant for 15,000 innocent Iranians who just want freedom.

Ms. DEMINGS. The gentleman's time has expired.

Director, you answer the question.

Mr. WRAY. Well, what I would say is that the Iranian regime across multiple vectors has become more aggressive, more brazen, and more dangerous. I would just point everything just in—again, just in maybe the last 18 months, a cyber attack on a children's hospital, an attempt to assassinate the former U.S. National security advisor in the United States, and an attempt to kidnap a journalist from right smack in the middle of New York City. So if that is not enough to convince us that the regime is a threat, I don't know what is.

Mr. SWALWELL. Thank you, Director.

Ms. DEMINGS. The Chair now recognizes the gentleman from Florida, Mr. Gimenez, for 5 minutes.

Mr. GIMENEZ. Thank you, Madam Chairwoman. I want to echo the thoughts of some of my colleagues that Mr. Katko—I know he is gone—but certainly a great Ranking Member and the way that this committee has conducted its business in a bipartisan manner, that is to be commended.

Mr. Wray, I read in your testimony that you consider domestic violent extremists to be the greatest threat to our, you know,

health and well-being here in the United States. Do you stand by that?

Mr. WRAY. Well, let me just make a slightly finer point on it, because precision is important here.

The greatest threat to us in the homeland is the lone actors and small cells, typically radicalized on-line, using easily accessible weapons against soft targets. That group included two categories, both domestic violent extremists and home-grown violent extremists, which are foreign terrorist-inspired. So they are very similar, but it is two big buckets.

Mr. GIMENEZ. Do you know how many fatalities we had in 2020 from DVEs?

Mr. WRAY. I don't have the number of deaths off the top of my head, but I know that in 2020 the most lethal attacks—or the lethal attacks that we had came from what we categorize as anti-Government, anti-authority violent extremism, which includes both anarchist violent extremism, as well as militia violent extremism.

Mr. GIMENEZ. Yes, I think I read there was something like four. Four is too many, you know, that is—you know, for the four people that died.

Do you know how many people died per day from fentanyl overdose?

Mr. WRAY. I don't have that figure.

Mr. GIMENEZ. Would it shock you to say over 200 die daily from fentanyl overdoses?

Mr. WRAY. I know the numbers are eye-popping.

Mr. GIMENEZ. Eye-popping. Who controls that trade? Who is pouring in this deadly drug into the United States?

Mr. WRAY. Transnational criminal organizations, especially the cartels.

Mr. GIMENEZ. Which ones? From where?

Mr. WRAY. Typically from Mexico.

Mr. GIMENEZ. Would you consider that to be a terrorist act?

Mr. WRAY. Well, I certainly consider it to be a major, major law enforcement threat and a major, major security threat. Whether I would call it a National security threat gets into sort-of terminology. But certainly it is a major threat to the homeland of almost epidemic proportions.

Mr. GIMENEZ. So an organization that is killing over 200 Americans every single day, you have difficulty in saying that they are not terrorizing us?

Mr. WRAY. Well, again, in my world terrorism has a very specific legal definition. It is certainly a National security threat.

Mr. GIMENEZ. So what are we doing about it? So we know we have an organization across the border—they are not some far away land, they are right across the border, they are killing tens of thousands of Americans every year. What exactly are we doing about that?

Mr. WRAY. Well, as to true border security, obviously I would, you know, defer to Secretary Mayorkas. But on our end, to deal with the transnational criminal organizations, there are a number of things we are doing.

First, we have transnational organized crime task forces with not just agents, but lots and lots of State and local law enforcement of-

ficers who work with us to go after the cartels. Second, we have safe streets task forces, which deal with a related part, which is the violent gangs that work with those cartels and going after those. Third, we have border liaison officers in all of the field offices that we have that are on the border. I have visited all of them myself and walked around not just with our people, but with the CBP officers. Those folks ensure cross-border assistance. We have legats, which is legal attaché offices in Mexico. In fact last year we were able to apprehend two of the FBI's top ten most wanted fugitives, which is progress.

So those are some of the things we are doing, but it is a major, major concern for sure.

Mr. GIMENEZ. Have we done anything with the government of Mexico, warned them, et cetera, that they need to step up their war against these cartels? Because, again, these cartels are killing tens of thousands of Americans.

You know, a foreign group in 2000 killed about 3,000 Americans and we responded by waging war for about 20 years halfway around the world. There are foreign groups right now across the border that are killing tens of thousands of Americans every single year and we don't seem to be doing much about it. Frankly, I am upset about that. We seem to be focused on domestic violent extremists, which we should, OK, but we are—which kill four people in 2020, and we seem to be turning a blind eye to organizations that are killing tens of thousands of Americans. We also seem to be doing not much about stopping the flow of this drug coming into the United States through our Southern Border.

Thank you.

My time is up and I yield back.

Ms. DEMINGS. The gentleman yields back.

Let me just correct the record, 2019 most lethal year for DVE attacks. DVEs were responsible for 32 deaths in 2019.

The Chair now recognizes the gentlewoman from Nevada, Ms. Titus, for 5 minutes.

Ms. TITUS. Thank you very much.

At first let me thank the Department and Secretary for extending the TPS protections to Haiti, El Salvador, Nicaragua, Honduras, Sudan, and Nepal. I have a very diverse district, many people from Central America, who will be benefiting from this and I just want to thank you. I appreciate that effort.

My first question though will go to the Secretary, and it is pretty specific about my district. I apologize if it is too parochial. But Las Vegas is very excited to be getting a Formula One event for next November. They are going to be racing for 3 days up and down the strip, they are going to be close to all these major hotels, a lot of people are going to be there watching this race. I want to make sure that the event receives the appropriate—SEAR I think is the acronym—Special Event Assessment Rating. I just heard the director mention that Las Vegas is a place where they are always looking for terrorists, or we have seen terrorist threats.

So could you talk about how the criteria for these SEAR designations work, how it has been updated, how today differs from what is in the past that would accommodate the event in Las Vegas?

Secretary MAYORKAS. Congresswoman, we are evaluating right now the Formula One race that is scheduled to occur in Las Vegas to identify the appropriate SEAR rating that it deserves.

Please forgive me, but I must—I must respond to the Congressman's statement that preceded your question. It is candidly outrageous to say that we are not doing anything to address the transnational criminal organizations. We have incredibly brave law enforcement officers every day risking their lives to battle the criminality of those TCOs. I look forward to sharing with the Congress everything that we are doing in that regard.

Congresswoman, I would be pleased to share with you what we are doing to refine the SEAR rating process, that is a rating process that we use to identify the security level of particular events in the United States. We actually just met as a group and discussed this yesterday. So I look forward to sharing with you some details. That review is under way.

Ms. TITUS. Well, thank you very much. We want it to be a fun environment, but we also want it to be a very safe environment for all the people who come to enjoy this kind of race.

Related to this, Mr. Secretary, tourism is coming back, international tourism. We want to encourage that because such a big part of our economy—foreign tourists stay longer, they spend more, they visit regional areas, not just downtown Las Vegas. I wonder what is going on as you all try to accommodate this increase in tourism again. Whether it is with TSA or with Customs or COVID, all of those kind of considerations.

Secretary MAYORKAS. Congresswoman, we are incredibly excited about the fact that travel to the United States has resumed in full force. In fact, I think the latest figures exceed the patterns of 2019 before the COVID–19 pandemic gripped this country and the world in full force.

The TSA personnel have emphasized the PreCheck process, which of course really assists us and supports us in approaching travel security in a risk-based manner. We are seeing more than 15,000 enrollments per day in the TSA PreCheck process. Our Border Patrol personnel are also working on new technologies and innovations to facilitate the travel process, as is TSA. There was quite a robust article just a couple of weeks ago in the *Washington Post* that described some of the technological innovations that TSA specifically has displayed. We have a partnership with Apple, for example, that we are of course open to other vendors accessing and using for a mobile driver's license identification process. We are looking at innovation and technology and the capabilities to further facilitate the travel experience and to enhance security at the very same time.

Ms. TITUS. Is staffing improving in terms of needing additional personnel?

Secretary MAYORKAS. One of the things that we hope Congress passes is our request to provide pay parity for our TSA personnel. The disparity that our TSA personnel suffer in pay makes recruiting and retention very difficult. So we hope that Congress passes the much-needed legislation to provide pay fairness for our TSA personnel.

Ms. TITUS. Thank you.

I know my time is up, but I would certainly support that and I know the Chairman of this committee has been working hard on that issue.

Thank you and I yield back.

Ms. DEMINGS. The gentlewoman's time has expired.

The Chair now recognizes the gentlewoman from Florida, Mrs. Cammack, for 5 minutes.

Mrs. CAMMACK. Thank you, Madam Chairwoman, and good afternoon. Thank you all for being here with us this afternoon.

With so many threats to deal with, as has been pointed out today, it is really a shame that we have a major one that we have to contend with. It is completely unnecessary and manufactured. So we will just jump right in on that one.

Secretary Mayorkas, you have stated that you believe that the Southwest Border is secure. Giving me just the number and nothing else, no additional commentary, tell me how many gotaways there were for fiscal year 2022. Just the number please.

Secretary Mayorkas, I have a litany of questions, just the number please.

Secretary MAYORKAS. Six hundred thousand.

Mrs. CAMMACK. Thank you. You are correct, it is 600,000. Now, can you answer definitely with data backing up your answer that none of the 600,000 individuals who are now in the United States amongst our communities that got away are gang members or criminals?

Secretary MAYORKAS. Your question highlights precisely why we have sought to prioritize national security and public safety threats——

Mrs. CAMMACK. I am so glad to hear you say that.

Secretary MAYORKAS [continuing]. In our Immigration and Customs Enforcement apprehension and removal efforts.

Mrs. CAMMACK. I am really glad to hear you say that.

I am going to have to reclaim my time, because I have got a lot to get through.

So as you know, probably then, in fiscal year 2022 CBP arrested nearly 30,000 illegals attempting to enter the country who were previously convicted of a crime. Now, of those arrested—and just the number, no additional commentary—how many have claimed asylum?

Secretary MAYORKAS. Congresswoman, I will have to get back to you with——

Mrs. CAMMACK. OK.

Secretary MAYORKAS [continuing]. Specific numbers.

Mrs. CAMMACK. Thank you.

Now, officially there have been 2.4 million illegals that have been encountered at the Southwest Border in fiscal year 2022. That doesn't include the 600,000 gotaways. So giving me just the number, and again, no additional commentary, can you tell me how many illegals have been released into the United States that were encountered at the Southwest Border?

Secretary MAYORKAS. Putting aside your terminology, may I correct you? Because you have actually cited inaccurate facts in your question.

Mrs. CAMMACK. Well, this is actually from your webiste.

Secretary MAYORKAS. No, it isn't.

Mrs. CAMMACK. It is. I would be happy to provide it to you.

Secretary MAYORKAS. Congressman, 2.4 million or between 2.3 and 2.4 million encounters is different than 2.3, 2.4——

Mrs. CAMMACK. But I think you are missing the point of the question. How many——

Secretary MAYORKAS. If I may, Congresswoman——

Mrs. CAMMACK [continuing]. Have been released into the United States?

Secretary MAYORKAS. Congresswoman, if I may, because you are mistaken, factually mistaken.

Mrs. CAMMACK. So your data is incorrect?

Secretary MAYORKAS. No. No, you are misunderstanding our data.

Mrs. CAMMACK. No.

Secretary MAYORKAS. If I——

Mrs. CAMMACK. OK. I am going to reclaim my time because based on the information from your website—from your website, from your Department, officially there have been of all those encounters 1.4 million—and that is a conservative number—that your Department states have been released into the United States.

So I know you guys have done this really fun renaming, rebranding thing, calling it enforcement removal proceedings, but today in fiscal year 2022, you have now released over 1.4 million illegals into the United States. My question to you now is can you guarantee that none of those people have criminal records?

Secretary MAYORKAS. This enforcement work is not fun, Congresswoman. This is a noble profession in which people risk their lives to conduct it. You know that very well.

Mrs. CAMMACK. All the righteous indignation. Here we go.

So I want to make sure that you understand that per your own data and statistics, they have pointed out that in fact you hold the record as Secretary of Homeland Security for the most encounters and subsequent releases into the United States in history. Your own former boss, Secretary Jeh Johnson, said that 1,000 a day is considered a crisis. Today we are encountering 7,000 a day. The facts and figures make the point for me.

So is the border secure based on your feelings or facts?

Secretary MAYORKAS. Congresswoman, let me have the opportunity to correct a misstatement.

Two-point-three to 2.4 million encounters includes the fact that under Title 42, the Public Health Authority, individuals can actually be repeat offenders. They can try again. So there are actually approximately 1.7 million unique individuals whom we have encountered at the border. So when you say 2.4——

Mrs. CAMMACK. But based on your reporting——

Secretary MAYORKAS. I am actually—if I may——

Mrs. CAMMACK. Based on your reporting, these folks are here in the United States and there has been no proper vetting of these people. Then we don't even have the agreements in place to deport the folks that you are claiming under Title 42. Nicaragua is a great example of that.

Secretary MAYORKAS. Congressman, I hope you realize that we have removed or expelled more individuals from the United States than ever before.

Mrs. CAMMACK. Just to clarify, as a final question, with all of this data that has been presented, based on your own Department's releases, you still believe that the border is secure?

Ms. DEMINGS. The gentlewoman's time has expired. You may answer the question, Mr. Secretary.

Secretary MAYORKAS. Congresswoman, we remain committed to enhancing the security of our border every single day.

Mrs. CAMMACK. That is not an answer.

Ms. DEMINGS. The Chair now recognizes the gentlewoman from New Jersey, Mrs. Watson Coleman, for 5 minutes.

Mrs. WATSON COLEMAN. Thank you, Madam Chairwoman, and thank you to the witnesses for appearing before us today.

Secretary Mayorkas, I wanted to ask you a question about Coast Guard operations. Our country faces many pressing threats across the domestic and international landscape, several which we have discussed here today, obviously. However, we must not lose track of the threats we face over the long term, such as increased aggression by China and Russia within international waters. China is aggressively pursuing increased influence across the Indo-Pacific and a Coast Guard cutter recently found Chinese and Russian ships carrying out joint maneuvers in the Arctic less than 100 miles off of Alaska.

Mr. Secretary, how important to the U.S. interests are the Coast Guard's efforts to counter Chinese aggression in the Indo-Pacific and maintain a rule-based maritime order? Likewise, how critical are the Coast Guard's plans to build in and acquire new icebreakers to enable increased maritime presence in the Arctic?

Secretary MAYORKAS. Congresswoman, thank you very much.

It is vitally important that our United States Coast Guard be fully resourced to address what we all today have described, and accurately so, as an only increasing threat from China and other adverse nation-states. I was actually in Singapore and Japan several weeks ago to speak about the need to enhance our security partnerships. One of the main lines of effort in my bilateral discussions was in fact increased cooperation with our United States Coast Guard to address the increasing threat in the Indo-Pacific Region.

Of course, the United States Coast Guard also has an Arctic strategy that it is executing and that Arctic strategy includes increasing its aging fleet and replacing some of its most aged vessels. So we look forward to Congress' support for that necessary funding.

Mrs. WATSON COLEMAN. Are there any other resources that we should be considering to support you in that endeavor?

Secretary MAYORKAS. Congresswoman, we of course have presented our fiscal year 2023 budget, which includes much-needed resourcing of the United States Coast Guard. We do hope that our budget is implemented very quickly. Every day that passes fails to advance our security mission. We are of course working on our budget plans for the years beyond.

Mrs. WATSON COLEMAN. Thank you.

I want to just mention that I am totally in support of the questions raised by Congressman Swalwell as it related to antisemitism. I mean New Jersey has had a very unique experience just a week ago where someone was threatening synagogues in the State of New Jersey. We have a large Jewish population and we want all of our population to be safe. So to you and to Director Wray, we very much look forward to your diligence, your intelligence, and your proaction as well as reaction.

Finally, I have exactly a minute and 34 seconds left. I am wondering, Mr. Mayorkas, if you had any follow-up response to a former question or questions that you have been asked that you would like to share here?

Secretary MAYORKAS. Congresswoman, thank you so much.

You know, we maintain data with respect to the challenge at the border. That data informs our operational actions and it is vitally important that that data be cited with precision and accuracy. We demand that of ourselves so that the operational decisions that we make are best tailored to address the challenges that we confront.

I look forward to working in a bipartisan way with this committee to address the myriad of threats that we as a country face and to really enhance the security of the American people in every regard.

Mrs. WATSON COLEMAN. Thank you.

Madam Chair, I yield back.

Ms. DEMINGS. The gentlewoman yields back.

The Chair now recognizes the gentleman from Kansas, Mr. LaTurner, for 5 minutes.

Mr. LATURNER. Thank you, Madam Chairwoman.

Thank you Mr. Secretary, for being here today.

Secretary Mayorkas, you said "our message has been clear that the border is in fact not open". According to public data from the U.S. Customs and Border Protection, which you yourself oversee, we had 227,000 migrant encounters at the Southwest Border in September of this year alone, bringing the yearly total to almost 2.4 million, which is the highest number ever recorded. Do you believe that indicates a border that is not open?

Secretary MAYORKAS. Congressman, thanks for your question.

Please, it is very important that the American people understand that the individuals whom we encounter who are not expelled under the Public Health Authority of Title 42 are placed in immigration enforcement proceedings and are subject to removal if they do not qualify for the relief that they laws of this country provide them.

Mr. LATURNER. Respectfully——

Secretary MAYORKAS. I do not think——

Mr. LATURNER. Mr. Secretary——

Secretary MAYORKAS. If I may——

Mr. LATURNER. No, hang on. I have a limited amount of time and several questions. If you just give me a quick answer, I would really appreciate it.

Secretary MAYORKAS. Sure.

Mr. LATURNER. Among those nearly 2.4 million encounters, we had 98 non-U.S. citizens listed on the terrorist watch list who were caught trying to enter the homeland between ports of entry. This

is approximately five times the number of terrorist encounters from the last 5 years combined. Do you believe this indicates a border that is not open?

Secretary MAYORKAS. What this indicated, Congressman, is the fact that we have extraordinary personnel in the United States Border Patrol risking their lives every day to apprehend individuals at the border. We work——

Mr. LATURNER. Mr. Secretary, you are not going to answer the question. In fiscal year 2022 we had an estimated 600,000 gotaways. Do you believe this indicated a border that is not open?

Secretary MAYORKAS. Congressman, I would respectfully posit that I don't think that the 1.4 million people who were either removed or expelled——

Mr. LATURNER. Mr. Secretary——

Secretary MAYORKAS [continuing]. From the country would consider——

Mr. LATURNER [continuing]. Please——

Secretary MAYORKAS [continuing]. Would consider the border open.

Mr. LATURNER. I am going to take back my time.

In May Kansas City law enforcement seized more than 15,000 counterfeit fentanyl pills. This fiscal year alone CBP has seized enough fentanyl to kill almost 2.9 billion people, over 8 times the entire population of the United States. Do you believe this indicates a border that is not open?

Secretary MAYORKAS. Congressman, do you realize that the majority of the fentanyl that is sought to be smuggled into the United States comes through the ports of entry? Our interdiction efforts have been more successful than ever before. I should note that——

Mr. LATURNER. Mr. Secretary, in my home State——

Secretary MAYORKAS [continuing]. Year over year since 2018——

Mr. LATURNER. Excuse me. Mr. Secretary, you have done this all day. When you don't like a question, you filibuster.

In my home State of Kansas, the State Health Department saw a 54 percent increase in drug overdoses in the first half of 2021, nearly half of which were caused by fentanyl, primarily supplied by the cartels. Nation-wide, the CDC reported that over 107,000 Americans died of drug overdoses in 2021, with 66 percent of those related to synthetic opioids like fentanyl—300 Americans a day are dying from fentanyl. It is the equivalent of an airliner going down every day. Do you think this indicates a border that is not open?

Secretary MAYORKAS. Congressman, the fight against the scourge of fentanyl and the devastation that it is wreaking, is a years-long fight that we in the U.S. Government, with our State and local partners have been fighting. Do you realize that the number of overdose deaths from fentanyl has been increasing year over year since at least 2018? Certainly this is not a new phenomenon. It is——

Mr. LATURNER. Mr. Secretary, you clearly——

Secretary MAYORKAS. It is not a new tragedy.

Mr. LATURNER. Mr. Secretary, you clearly don't understand the problem.

Secretary MAYORKAS. I clearly do.

Mr. LATURNER. This has—excuse me—this has nothing to do with politics. This is about kids across the country dying every single day from fentanyl overdoses because people in Washington can't get their act together. This is about an overwhelmed Border Patrol. This is about migrants being victimized by the drug cartels. My concern and the concern of my constituents back home is how can you begin to solve the problem if you don't even acknowledge the depth and breadth of it?

Here is a question for you.

Secretary MAYORKAS. Congressman, I would respectfully——

Mr. LATURNER. Have you had discussions——

Secretary MAYORKAS [continuing]. Disagree with you.

Mr. LATURNER. Excuse me, Mr. Secretary. Have you had discussions with the President or anyone in the Biden administration about stepping down from your current role?

Secretary MAYORKAS. I have not.

Secretary MAYORKAS. Not a conversation with anyone in the administration?

Secretary MAYORKAS. Congressman, let me be very clear.

Mr. LATURNER. Yes or no.

Secretary MAYORKAS. May I answer your question?

Mr. LATURNER. No, you—yes or no. Have you had——

Secretary MAYORKAS. Congressman——

Mr. LATURNER [continuing]. That conversation with anyone in the administration?

Secretary MAYORKAS. I am very proud of what we have accomplished. I am very committed to——

Mr. LATURNER. Sir——

Secretary MAYORKAS [continuing]. Accomplishing more.

Mr. LATURNER [continuing]. Answer the question. Have you had a conversation with anyone in the administration about stepping down from your current role?

Secretary MAYORKAS. I have not.

Mr. LATURNER. I hope for the sake of the safety of the American people that that conversation happens very soon.

I yield back my time.

Secretary MAYORKAS. Madam——

Ms. DEMINGS. The gentleman yields back.

Mr. Secretary, you may respond.

Secretary MAYORKAS. Madam Acting Chair, thank you very much for the opportunity.

Congressman, I look forward to sharing information with you so that you understand the threat that fentanyl poses and how it is smuggled into the country. Everything that we are doing to fight the transnational criminal organizations across the Federal enterprise, with our partners to the south, and to disabuse you of misunderstandings that you have with respect to the fentanyl crisis, because they are grave. I look forward to not only sharing information with you, but hopefully sharing information with the American public.

Thank you.

Ms. DEMINGS. I recognize myself for 5 minutes.

In the Ranking Member's absence, I do want to thank him for his leadership and his civility.

I am hoping that this committee moving forward understands the importance of both of those things. I have heard a lot today and seen a lot, but there is one thing that I just cannot ignore, and I don't have to, of the performance of the gentleman from Louisiana earlier was an embarrassment. I am hoping that it was not reflective of the caliber of this committee and the very important work that you all have to do between the Members and staff moving forward.

See, I just happen to believe that we can in the interest of the country be our better selves. I just happen to believe that we can on this committee be examples of America's exceptionalism. That example for our children and our grandchildren. I just happen to believe that we can work to keep our homeland safe, all at the same time.

Director Wray, in June 2019, or somewhere around there, you talked about that you had—FBI had elevated the racially and ethically motivated violent extremism to your highest level—or highest threat priority, on the same level of ISIS and home-grown violent extremists. Is that still the case today? Why or why not?

Mr. WRAY. Yes, Congresswoman, it is still a National threat priority and that is reflective of the lethality that we saw over the years leading up to that designation and that have to some extent continued since then.

Ms. DEMINGS. How does the caseload for cases falling into that category look today?

Mr. WRAY. I don't have exact numbers here, but I can tell you that the number of both domestic violent extremism cases in general has been growing over the last 4 or 5 years.

Ms. DEMINGS. Would you say it has doubled?

Mr. WRAY. Depends on when you—what your starting point is.

Ms. DEMINGS. Last 5 years.

Mr. WRAY. Before the end of calendar year 2020 it had gone up by say 50 percent. Since then it has gone up yet again quite substantially. That is domestic violent extremism overall, of which racially and ethnically violent extremism is one part.

But I should say that along with racially and ethnically motivated violent extremism, we also saw starting in 2020 and continuing to the present, a lot of anti-Government, anti-authority violent extremism, which includes everything from militia violent extremism to anarchist violent extremism. While that hasn't resulted in as many lethal attacks, the sheer volume of it caused us to elevate that as well more recently to a National priority.

Ms. DEMINGS. Would you say that that is the result of a lone domestic violent extremist? You talked about the threat of—I used to say the lone wolf. I guess we don't say that anymore, but would you say that the increase that you just talked about is a result of these individual people out there who are influenced by an array of different things?

Mr. WRAY. We are certainly seeing a trend that is magnified online of people using a mix, a hodgepodge of different personal beliefs and ideologies and grievances as justification for violence. That is an alarming trend that has continued, again, for the last let us say 4 or 5 years. It something we have to be concerned about. Certainly the social media dimension is one of the ways in

which gasoline is poured on the fire, if you will. But there are a lot of other things that contribute to it.

Ms. DEMINGS. You have also said that China and Russia have basically piggybacked on the unrest that is here, the division within our country. What did you mean by that? In what ways?

Mr. WRAY. Well, a number of our foreign adversaries, a number of nation-states, Russia initially, but since then not just Russia but China and Iran as well have capitalized on the same toxic politically-charged violence that occurs in this country these days to try to pit us against each other, to sow divisiveness, to amplify tensions that are already there and make it worse. We saw that——

Ms. DEMINGS. Yes. They must be——

Mr. WRAY [continuing]. Not just with Russia——

Ms. DEMINGS. They must be smiling right now.

Let me just end with this. I want to thank all of you for the commitment that you have to protecting our Nation. You have tough jobs. Some day I wonder why you have answered the call, but on behalf of this committee, we are sure glad that you did.

At this time the Chair recognizes the gentleman from Michigan, Mr. Meijer, for 5 minutes.

Mr. MEIJER. Thank you, Madam Chair, and thank you to our witnesses who are here today. I know we all prize truth and accuracy.

One thing for Director Abizaid, before we begin, Mr. Swalwell had mentioned the Iranian parliament voting I think he said the death penalty for 15,000 protestors. Is that strictly speaking an accurate statement that he made?

Ms. ABIZAID. I don't have details on exactly what the Iranian parliament actually did. We can certainly get back to you on that. I mean I will say in the spirit of this question and in the spirit of Director Wray's response, the Iranian government is a state sponsor of terrorism. We have seen them assume multiple different inroads into the United States and elsewhere. It is a regime that raises significant concerns from a security perspective.

Mr. MEIJER. Thank you. The public reporting that I had seen said that the Iranian parliament had voted in a super majority to enact tougher, swifter punishments up to and including the death penalty. But I think it is important when we are talking about adversaries to be clear. Then, again, I know you are well aware of this from your own work. But I just want to make sure that those statements and exaggerations don't go unanswered.

I guess on the realm of that notion of exaggeration and jumping to false conclusions, you know, Secretary Mayorkas the September 19, 2021 incident in Del Rio, Texas, with the three mounted CBP officers, can—I know you had initial statements defending them last year. There were then, you know, a little bit of a walking back and President Biden making some very sweeping assumptions, accusing those officers of using their reins to whip or otherwise physically assault migrants who were coming across the border illegally. Then over the summer there was an investigation that essentially I believe clarified that it was cord split reins that were being used to control the horses. They never came into contact with migrants or the migrants didn't come into contact with those agents in that sense.

Do you have anything else to add, you know, in terms of your current assessment of that situation now that we are a year and change onwards from it.

Secretary MAYORKAS. Congressman, thanks so much.

From the very outset, I was actually in Del Rio the day that those photographs were first published. From that very afternoon in Del Rio at a press conference and ever since, I have spoken of the fact that the facts would be adduced in an objective, fair, and thorough investigation conducted by the Office of Professional Responsibility. The career personnel of the Office of Professional Responsibility did indeed conduct such an investigation and their thorough and extensive report speaks for itself.

Mr. MEIJER. I believe there are still three CBP members and a supervisor that are currently in an investigatory process. So they haven't—is that an accurate understanding? Just using media reports because there hasn't been too much forthcoming.

Secretary MAYORKAS. Congressman, to be precise——

Mr. MEIJER. Yes, please.

Secretary MAYORKAS [continuing]. To your point, I believe the investigation is concluded. The report has been submitted, and now the disciplinary process——

Mr. MEIJER. Correct.

Secretary MAYORKAS [continuing]. Is under way. That can take some time because of course the agents are afforded due process rights.

Mr. MEIJER. I appreciate hearing that, because so often the narrative gets far ahead of the facts. By the time, you know, the erroneous tweet gets a million likes and then the correction follow-up gets 15. Making sure that we are applying that same standard at 24-hour rapid news cycles, important as the narrative gets baked in and people have a misunderstanding and misapprehension.

I guess very quickly, because I am running a little bit out of time, the four Secret Service agents in April of this year who were found to have been taking gifts, free apartment rentals, a number of kind-of high-value items that were being given to them by individuals that they believed were DHS agents, Department of Homeland Security agents, but were instead just cosplay artists. I mean characters who were ingratiating themselves. All credit to the United States Postal Investigation Service that uncovered it. Is that essentially a personnel matter? Because that is the response that the Department has been giving to our committee when we are inquiring how such a glaring security lapse could occur.

Secretary MAYORKAS. So, Congressman, I can't speak to the facts because they are under review, there is a process there. But I can say this with tremendous conviction, that I am intensely proud of the men and women of the United States Secret Service and the manner in which they execute their message. I am a beneficiary of their willingness to risk their lives for the safety and security of others.

Ms. DEMINGS. The gentleman's time has expired.

The Chair now recognizes the gentleman from New York, Mr. Torres, for 5 minutes.

Mr. TORRES. So my question is directed toward the director. I am the future Congressman for Riverdale and the Bronx. Riverdale

happens to be home to the Russian Diplomatic Compound, which stands as one of the highest buildings at one of the highest points in the Bronx. It is both literally and metaphorically a structure of surveillance, towering over the Bronx. The compound is so shrouded in secrecy that not even the fire department could gain access when a fire broke out more than a decade ago. According to a retired FBI special agent, Robert Dreeke it is an open secret that there are Russian spies disguised as diplomats residing at the Russian Diplomatic Compound.

In 2015 the U.S. Attorney for the Southern District arrested and charged Evgeny Buryakov with conspiring to act as an agent of the Russian Federation on American soil. Mr. Buryakov lived in Riverdale in close proximity to the Russian Diplomatic Compound.

So in the FBI's view, does the Russian Diplomatic Compound pose a homeland security threat?

Mr. WRAY. Well, Congressman, I think we may have provided a Classified briefing to you on this topic. But if we can supplement that, I would be happy to do that. I will say that the Russian intelligence services are perhaps the most active and aggressive on U.S. soil and in no place more so than in the city of New York.

Mr. TORRES. Would you consider that a homeland security threat?

Mr. WRAY. I consider the Russian intelligence services activity here in the United States to be a homeland security threat.

Mr. TORRES. Under the Foreign Mission Act, the FBI has the authority to reject on homeland security grounds the citing of a new embassy or consulate. Section 4305(d)(2) reads as follows: "After December 22, 1987 real property in the United States may not be acquired by or on behalf of the foreign mission of a foreign country if in the judgment of the FBI director the acquisition of that property of that country might substantially improve the capability of that country to engage in intelligence activities directed against the United States." Do you think the Russian Diplomatic Compound, in the words of the Foreign Mission Act, substantially improves the capability of Russia to engage in intelligence activities directed against the United States Government?

Mr. WRAY. Well, I would be more comfortable taking this up in a Classified session. I am not an expert on the legality parts of the interaction here, but what I will tell you is that I know that the FBI's concerns from a counterintelligence perspective with respect to the Russian intelligence services are something that we discuss with the State Department, which has an important role here, quite frequently. I am very proud of the work, for example, that we were able to do together to ensure the closing, for example, of the San Francisco consulate for many of the same kinds of reasons that you are alluding to.

Mr. TORRES. I just want to be clear, I am not asking for confidential numbers or information, I am simply asking, you know, does the public have a right to know the FBI's view on whether a compound in their backyard poses a threat to the security of the homeland?

That could be answered without divulging highly sensitive information.

Mr. WRAY. Well, I can answer in a general sense, which is that we are concerned about the Russian intelligence service's activity in the United States, including in New York, and their ability to exploit their diplomatic presence to accomplish that. More than that, I think I would have to wait and have us brief you on that, as I think we have to some extent already in closed session. It is not because I don't absolutely—as somebody whose parents still live in New York—care deeply about the issue that you are concerned about.

But I just want to be careful about how I answer the question.

Mr. TORRES. Suppose the Russian Diplomatic Compound had never been built in Riverdale in the 1970's, if the Russian government were proposing to build the Russian Diplomatic Compound today, would the FBI reject it under the Foreign Mission Act?

Mr. WRAY. Well, I am reluctant to engage in hypotheticals, other than to say, as I have said, that we have seen a long history of the Russian intelligence services abusing and exploiting their diplomatic presence in the United States, including in New York, for purposes that are not in the interests of the United States. We will continue to express our views fairly forcefully in the interagency in that regard.

Mr. TORRES. I suspect the answer is no, that we would never allow this structure of surveillance to be built in 2022 in Riverdale. The fact that, you know, espionage in the Russian Diplomatic Compound has essentially been grandfathered in, is as indefensible to me as it is inexplicable.

I will leave it at that.

Thank you.

Ms. DEMINGS. The gentleman's time has expired.

The Chair now recognizes the gentleman from Texas, Mr. Pfluger, for 5 minutes.

Mr. PFLUGER. Thank you, Madam Chair.

So we have the FBI, the National Counterterrorism Center, and the Homeland Security Departments here, the three agencies that have largely been entrusted with the safety and security of—every American has entrusted your agencies with their safety and security. This is your legacy. This is the legacy that you are going to leave behind. It has already been mentioned today that this year we have 98 people—and that doesn't include the 9, Secretary Mayorkas, that were reported by your Department yesterday, in October. So over 100 people have matched the terror watch list—100 people. That is a 500 percent increase from the encounters of the previous year. Regardless of your testimony today under oath, that our border is secure, Americans can look at the numbers. We can look at the numbers right here and see from 2017 to 2021 and all the way into 2022, fiscal year 2022, over 100 people matched the terror watch list. All of you have testified today that you are worried about terrorism. Really?

You see here the gotaways. Secretary Mayorkas, you have told me several times under oath that we have operational control of the Southern Border. I assume that you maintain that because you testified earlier today. How many of these people match the terror watch list? How many of the 600,000 known gotaways match the terror watch list?

Secretary MAYORKAS. Congressman, your question points to the very reason why we prioritize National security and public safety in our immigration enforcement efforts. Why on September 30 of 2021——

Mr. PFLUGER. Mr. Secretary, can I reclaim just a minute—I am going to reclaim my time.

I think that is false. I have been to the Southern Border and I have talked to your Border Patrol agents. You know what they tell me? That on any given shift 70 percent of them are relegated to administrative duties. They are not in the field doing the National security mission.

How many of these 600,000 people—can you assure the American people that not a single one of these 600,000 people are a threat to our safety? That they don't match the terror watch list, that they are not part of a criminal or transnational organization?

That is what your agents have told me personally. So I am just taking their word for it.

Secretary MAYORKAS. I have the benefit of a vantage point of what the entire border represents, as well as what we are doing about it.

One of the things that we have done about the fact that Border Patrol agents were too often behind computers——

Mr. PFLUGER. Secretary, answer the question.

Secretary MAYORKAS [continuing]. Processing cases——

Mr. PFLUGER. How many of the 600,000 people—no, we have 2 minutes left.

Secretary MAYORKAS. I know, but I feel compelled to——

Mr. PFLUGER. You don't have the time to do that. I want to know how many of the 600,000 people match the terror watch list?

Secretary MAYORKAS. Well, Congressman, by definition they are gotaways.

Mr. PFLUGER. OK. So you don't know. So how can you say that the border is secure? The American people aren't buying it. We are not buying it because the deaths that are happening in our communities—I have invited you to come with me. I was in Del Rio the day before you got there when the 15,000 Haitians were there. I have been to El Paso, I have been to the Rio Grande Valley. You are going to hear more on that later.

Let us put up another slide because you are not going to answer that question, but I don't—while we are putting up the next slide, do you maintain that we have operational control of the Southern Border?

Secretary MAYORKAS. Congressman, let me just say one thing very briefly and then I will answer your question.

It is very difficult to answer your question when I am not given the opportunity to do so, No. 1.

Mr. PFLUGER. As my colleagues have said——

Secretary MAYORKAS. No. 2, I do feel compelled to correct inaccuracies that are contained in your question for the benefit of the American people.

Mr. PFLUGER. The accuracies are—the facts that I have stated are reported by you and your Department.

Secretary MAYORKAS. Congressman, so we are dedicated to resourcing the United States Border Patrol with additional personnel——

Mr. PFLUGER. OK.

Secretary MAYORKAS [continuing]. With additional technology, using barriers advisedly where they are most beneficial——

Mr. PFLUGER. OK. That is not my question.

Secretary MAYORKAS [continuing]. To deliver enhanced security at our border.

Mr. PFLUGER. Mr. Secretary, thank you for that.

I have heard you say, and President Biden—and this is your legacy, OK—the American people can count. We can count. There is a humanitarian crisis at our Southern Border. I have been down there. You and President Biden have continued to ignore this problem. Fiscal year 2022 was the deadliest year on record. More than 800 migrants died. Do you remember the 53 that died in a tractor trailer in the heat of July south of San Antonio, Texas? This is the legacy.

The American people are demanding that you secure the border.

You have testified under oath today that it is secure. It is not.

Ms. DEMINGS. The gentleman's time has expired.

The Chair now recognizes the gentleman from New Jersey, Mr. Gottheimer, for 5 minutes.

Let me just remind the Members that we do have a vote on the floor, 5 minutes is 5 minutes. You are all entitled to it, but just know that there is a vote on the floor.

Mr. Gottheimer.

Mr. GOTTHEIMER. Thank you, Madam Chairwoman.

I have called for a National carjacking car theft task force as a result of a rising number of car thefts impacting my district, the State of New Jersey overall, and of course the Nation. However, these threats reach our ports a well, according to CBP's own reporting thousands of vehicles have been illegaly exported through tri-State area ports, including the Port of Newark, bound for overseas destinations including West Africa and the Dominican Republic.

Last year in New Jersey there were more 14,000 vehicles reported stolen, a shocking 22 percent increase compared to 2020, and 2020 numbers were already up from the year before. Year after year these crimes continue to grow, there has been a 19 percent increase in New Jersey through the first 8 months of 2022, including in the county in my district, Bergen County, as seen a 54 percent increase in car thefts this year.

I have called this committee to hold a hearing on the issue of auto theft and port security, as well as for Secretary Mayorkas to appear to answer questions about DHS's failing to take what I believe are adequate steps to address this issue. I believe DHS must do more to crack down.

However, I am concerned this issue is not being addressed in an urgent manner from the Department.

Mr. Secretary, despite repeated efforts, officials from DHS refused to answer my questions or publicly speak out on what measures are being taken in response to these alarming numbers of stolen vehicles being taken to our ports. I reached out to your office

multiple times over multiple months to invite you or a senior official from DHS to come to Jersey to address this issue and you refused. Which, as you might imagine, is very frustrating for the people that I represent.

Clearly this is a serious issue.

Can I ask you, Mr. Secretary, do you think this is a serious issue? Why aren't you communicating more to the public, why aren't you taking more serious steps, and what is your plan there?

Secretary MAYORKAS. Congressman, forgive me, I am unfamiliar with your request to speak with me directly about what is clearly a homeland security issue. I would be pleased to speak with you subsequent to this hearing. I will proactively reach out to your office.

I was actually in one of our ports on the East Coat working with our homeland security investigations and our customs office personnel addressing stolen vehicles and the implications for our security, the effort to smuggle narcotics through our ports of entry in stolen vehicles and other methods. I can share some insights in that regard and also learn from you with respect to the methodologies that you think we should employ to address this criminal threat.

Mr. GOTTHEIMER. Well, I appreciate that.

Yes, just so you know, I personally left messages for you. We reached—spoke to your—the departments at Homeland. They refused to come, despite repeated requests, which is very frustrating because it was over many months. This has been a huge challenge and I think this should be front and center as an issue that you consider. I hope that somebody, obviously in addition to our conversation, from DHS will come to the port to actually investigate, to look, to see what other steps can be taken working with local and State law enforcement to address this issue.

So I hope that will happen. I hope that I have your word that that will happen please. Sir?

Secretary MAYORKAS. We look forward to working with you.

Mr. GOTTHEIMER. Thank you.

If I can turn to Director Wray. In October, Director, I helped host a full committee field hearing on countering violent extremism and terrorism and antisemitic threats in New Jersey. The ADL's—antisemitic incidents reported a record 2,717 acts of assault, vandals, and harassment, averaging more than 7 incidents a day of antisemitic incidents in Jersey, up 25 percent in the last year. We have a huge issue. Just recently the FBI alerted the State and warned of the threats—a broad threat to synagogues for which an extremist individual was ultimately arrested. It is a clear reminder to the Jewish community and place of worship are vulnerable.

Director, what is the FBI doing to counter antisemitic threats and violence in New Jersey and around the country? If you mind just addressing that please.

Mr. WRAY. Absolutely. I am obviously pleased that we were able to make an arrest in the case in New Jersey that you mentioned. I was actually speaking to all of ADL on this topic just last week more broadly.

Mr. GOTTHEIMER. Great.

Mr. WRAY. Certainly antisemitism and violence that comes out of it is a persistent and present fact. Numbers that we have seen, about 63 percent of religious hate crimes overall are motivated by antisemitism, and that is targeting a group that just makes up about 2.4 percent of the American population. So it is a community that deserves and desperately needs our support because they are getting hit from all sides.

We are trying to address it through a combination of things. No. 1, on the terrorism side, the domestic terrorism side, through our joint terrorism task forces. No. 2, on the hate crime side, through our civil rights program. We have elevated that to a National threat priority. We have created, third, a domestic terrorism hate crime fusion cell, which brings together those two programs that I just mentioned, domestic terrorism and hate crimes, to try to be more proactive. In fact, that fusion cell has already had results. We were able to bring a proactive hate charge to prevent an intended attack on a synagogue in Colorado as a result of it.

But then on top of that we are engaged in a very aggressive outreach campaign that is designed to kind-of raise awareness, help people know how to report, what to be on the lookout for. Because we need to tap into the eyes and ears that are in the community. That has included, for example, not far from you in New York, translating some of the materials into Yiddish, for example, and Hebrew to make it more accessible to certain parts of the Jewish community.

Ms. DEMINGS. The gentleman's time has expired.

Mr. GOTTHEIMER. Thank you.

Ms. DEMINGS. The Chair now recognizes the gentleman from New York, Mr. Garbarino, for 5 minutes.

Mr. GARBARINO. Thank you, Madam Chair.

Thank you, Mr. Secretary and the director, director for coming today.

I want to start off first with Secretary Mayorkas. Fiscal year 2021 National Defense Authorization Act, which was enacted January 1, directed the administration to develop a continuing of the economy plan. As we came upon the 1 year—and they are supposed to finish it by the end of this year—as we came upon the 1-year mark last year I sent a letter to you as well as Director Easterly, expressing, you know, my immense concern about the lack of progress. I never received a response.

Then 15 months after the Authorization was done, the President finally handed over the authority to CISA, pretty much setting up the agency for a failure. We are now over a little bit of a month before the deadline and we have yet to receive any information on where CISA or the Department is on the development of the continuation of the economy plan.

Again, we sent that letter and we still have received no response. You talked about cybersecurity in your opening remarks. The development of the continuation of the economy plan is a National security imperative for the safety, security, and prosperity of the U.S. economy. So can we please have an update where we are on the development of this plan, which is due in less than 2 months?

Secretary MAYORKAS. Congressman Garbarino, I will look forward to following up on that for you and responding swiftly. I will have to look in that.

Mr. GARBARINO. Well, I mean——

Secretary MAYORKAS. Where the report that is due to you is.

Mr. GARBARINO. OK. Well, the report is due in 2 months, but we—I have sent two letters, both to you and Director Easterly, and I have received no response at all. When can I expect a response?

Secretary MAYORKAS. Let me follow up with you very quickly on that, Congressman.

Mr. GARBARINO. OK. I appreciate that.

I have another question for you, Mr. Secretary, because you also talked about it a little bit in your opening statement. Earlier this summer Canada became the last member of Five Eyes intelligence pooling alliance to bar or restrict the use of Huawei equipment within its 5G telecom network. In addition, Canada's ban also includes equipment made by ZTE, which is one of China's biggest tech companies and one that is state-owned. The United States and Canada work in partnership at and beyond our borders to enhance security, sharing critical infrastructure.

So it is critically important that the United States can trust Canada's or any of our allies' 5G equipment and software will not threaten our National security, economic security and privacy, or intellectual property. As the world becomes increasingly connected via the rise of 5G networks, how can vulnerabilities brought on by other nation's 5G networks, such as those with Huawei equipment, how can we make sure they don't pose a National security risk?

Secretary MAYORKAS. Congressman, your question is so very important. Let me share with you. No. 1, Canada is a very, very close security partner with us. We have a robust information-sharing architecture with them. They are one of the participants in our regular dialogs in the area that you have identified and in so many other homeland and National security areas.

I was just in Singapore about 3 weeks ago speaking about the very issue that you have identified and really communicating a very clear and stark call to countries in the Indo-Pacific Region about the vulnerabilities that are created when we allow China, the People's Republic of China to control some of the architecture infrastructure——

Mr. GARBARINO. Can I ask you what their response——

Secretary MAYORKAS [continuing]. Such as 5G.

Mr. GARBARINO. What was their response when you brought—because we are already doing it, but our allies, you know, there are some of them that aren't doing it and some of them that will not have updated—you know, the put these plans in place and they haven't updated current infrastructure with Huawei technology.

Secretary MAYORKAS. Congressman, it is our responsibility to communicate information, to communicate accurate information with respect to the perils of having infrastructure, communications infrastructure in the hands of nation-states that don't protect freedoms and rights as do we.

Mr. GARBARINO. OK. Well, I think though if some of our allies are not willing to, you know, protect their vulnerabilities like we are, especially with Huawei, we should maybe be a little more care-

ful in the future deciding what we are going to share with them, just because, you know, we don't need the enemy knowing what we know.

I have a final question for Director Wray. According to an August 2019 U.N. report, North Korea has generated an estimated $2 billion for its weapons of mass destruction program using cyber attacks. Again, we had—just in April North Korea hackers stole $620 million in cryptocurrency from video game Axie. You know, they have been doing this for a very long time and they are getting a little aggressive. What are we doing to stop these hackers? You know, what actions have been taken?

Ms. DEMINGS. The gentleman's time has expired.

The witness may answer the question.

Mr. WRAY. Well, you are right that I think North Korea sometimes gets—and I think dangerously so—overlooked as a significant cyber threat, because we spend so much time, very rightly, talking about China, Russia, and Iran. But North Korea has a growing espionage in addition to the theft and attack capability. In some ways sort-of similar to Iran in recent years in particular. Especially targeting, as you say, financial institutions, cryptocurrency exchanges, and so forth because they need it to fund their regime because of the effectiveness of the sanctions that otherwise exist.

So we are actively investigating any number of North Korean threat actor groups when we are able to catch somebody who is working with them in a country that we can extradite from. That is a very important part, both in terms of insuring accountability, but also in terms of disrupting their efforts and in terms of learning valuable intelligence about their techniques, tactics, and procedures.

In addition to that, it helps us figure out how to further tighten the sanctions regime to make it harder for them to find loopholes, which they are always looking for.

Ms. DEMINGS. The Chair now recognizes the gentlewoman from Texas, Ms. Flores, for 5 minutes.

Ms. FLORES. Thank you, Madam. Thank you to Chair Thompson and Ranking Member Katko for holding this hearing today. To all the witnesses, thank you for taking the time to speak to us today. We really appreciate it.

Our country is currently facing never-before-seen levels of illegal immigration, drug smuggling, and child sex trafficking. To Secretary Mayorkas, as someone who lives the reality of our Southern Border every day, saying that the border is secure, you are lying to the American people. According to the CBP our country has experienced 2.7 million migrant encounters to our border during the fiscal year of 2022. This does not include the 900,000 gotaways. Further, there has been 98 people apprehended crossing the border who appear on the terrorist screening data set.

This administration's horrendous border policies will continue to threaten our National security because a secure border is National security.

This week has been a very difficult week for us in South Texas. Our Border Patrol agents, the ones who dedicate their lives to protect us, are not receiving the support that they need from this administration. One of the top things I have heard from our Border

Patrol agents across the Southern Border is the lack of action from the DHS leadership in addressing Border Patrol morale. Our Border Patrol agents are understaffed, not provided with the resources that they need to succeed, and are spending time processing asylum claims instead of doing the job that they signed up to do.

Tragically, in the last week in the RGV sector, two Border Patrol agents took their own lives, leaving behind families and creating a hole in our communities.

Question No. 1. Secretary Mayorkas, the historic level of illegal alien apprehension and crossings at the border, combined with the limited resources and personnel to handle the large influx of migrants has caused a steep decline in morale among the Border Patrol work force. In no other department is a mental health crisis more visible than Customs and Border Protection, Border Patrol Division, our agents and our officers. One life is too many. And in 1 week.

What are your plans to support the mental health for your work force and address the troubling increase of suicide among the frontline personnel?

Secretary MAYORKAS. Congresswoman, may I have a minute to answer your question? Because you have touched on very, very important matters. I first, at the outset, should thank you for your service, because I know you have a Border Patrol agent in your family and I know very well that it is the family that serves.

Ms. FLORES. Mm-hmm.

Secretary MAYORKAS. Our prayers and thoughts are with the families of the agents who took their lives.

Our Border Patrol agents, our heroic Border Patrol agents——

Ms. FLORES. Mm-hmm.

Secretary MAYORKAS [continuing]. Are indeed under intense pressure and indeed under intense challenge. We are very dedicated to providing them with the resources and support that they need to fulfill their responsibilities and to ensure their wellness. That is a commitment that we have and it is an unwavering one and our highest priority.

We have surged resources to the border to get more Border Patrol agents out in the field. We are taking it to the smuggling organizations and the transnational criminal organizations in an unprecedented way. We are working with our partners to the south, the countries that need to enforce their borders and enforce their laws of humanitarian relief. This is a challenge that is not specific to the United States, that is not specific to our Southern Border, that is something that has gripped the Western Hemisphere.

Let me take the example of Venezuela alone. There are approximately 25–28 million people in the country of Venezuela. Approximately 8 million Venezuelans have left their country. Colombia is hosting 2.4 million Venezuelans, Chile is reported to host over 1 million Venezuelans. It is not Venezuela alone. Costa Rica is hosting hundreds of thousands of Nicaraguans. We are seeing a migration in the Western Hemisphere and in fact across the world that is unprecedented. There are more displaced along our border.

But with respect to our border, please rest assured, Congresswoman, and please have your family rest assured that we are dedicated to enhancing the security of our Southern Border and taking

care of our extraordinary and brave personnel who secure it every day.

Ms. DEMINGS. The gentlewoman's time has expired.

I want to thank the witnesses for your testimony and the Members for your questions. The Members of the committee may have additional questions for the witnesses and we ask that you respond expeditiously in writing to those questions.

The record will remain open for 10 business days. Also that there is a vote on the floor.

Without objection, the committee stands adjourned.

[Whereupon, at 1:05 p.m., the committee was adjourned.]

APPENDIX

QUESTIONS FROM SECRETARY SHEILA JACKSON LEE FOR HONORABLE ALEJANDRO MAYORKAS

Question 1a. The midterm elections resulted in a highly secure election in which Americans can be confident.

What is your assessment of the threat of cybersecurity breaches and intrusions during the 2022 midterm elections and the response to them?

Question 1b. What DHS efforts do you believe were most effective in securing this year's elections?

Answer. Response was not received at the time of publication.

Question 2a. We have seen a sustained rise in the use of influence operations to sway U.S. policy, manipulate elections, weaken the United States' geopolitical standing, and attempt to contravene our democratic process.

What changes have you seen in the frequency, magnitude, and impact of misinformation and disinformation operations since last year?

Question 2b. In what ways, and to what extent, do DHS and the FBI work together through such means as coordinating strategies, personnel, and other resources to combat the threat of influence operations?

Answer. Response was not received at the time of publication.

Question 3. Human trafficking and child exploitation are often spoken about as if they are separate crimes committed by separate parties.

In what ways, and to what extent, are human trafficking and child exploitation interrelated? Are the same perpetrators undertaking both crimes?

Answer. Response was not received at the time of publication.

Question 4a. Secretary Mayorkas' testimony that was provided prior to the hearing referenced a Climate Change Action Group that DHS began recently. My district has been impacted by extreme climate events that have greatly affected my constituents, including large-scale flooding from Hurricane Harvey and wide-spread infrastructure damage from Winter Storm Uri.

What specific climate change threats to homeland security has your Climate Change Action Group identified? What proactive and remedial measures has the group identified and recommended?

Question 4b. How is DHS investing in Community Resilience?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE JAMES R. LANGEVIN FOR HONORABLE ALEJANDRO MAYORKAS

Question 1a. Secretary Mayorkas, it has been 1 year since the Department of Homeland Security submitted its report evaluating PPD–21, as required by section 9002 of the 2021 NDAA. In a letter last week concurring with that review, President Biden acknowledged the United States "lacks a comprehensive way to establish mandatory minimum cybersecurity requirements across our critical infrastructure, and current approaches differ by sector." He also committed to "working with Congress to fill gaps in statutory authorities."

What gaps should we be looking to fill related to improving the cybersecurity of critical infrastructure?

Question 1b. The letter mentions a focused effort to help Sector Risk Management Agencies identify Systemically Important entities in their sector. How is DHS approaching this task?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE NANETTE BARRAGÁN FOR HONORABLE ALEJANDRO MAYORKAS

Question 1. I was happy to hear that the President's Interagency Task Force on the Reunification of Families that you chair has successfully reunified more than 500 children who were cruelly separated from their parents or family during the Trump administration. What strategies is DHS taking to reunite the remaining families and to remedy the harms of the past administration on these children and families?

Answer. Response was not received at the time of publication.

Question 2a. When I visited Puerto Rico as part of a Congressional delegation in September, residents and local officials highlighted how microgrids and solar power that helped keep power on after Hurricane Fiona hit. As we rebuild in Puerto Rico, does FEMA have the authority to approve clean energy projects with the Federal disaster recovery funding authorized by Congress after Hurricane Maria?

Question 2b. If yes, will FEMA prioritize clean energy projects to build a more decentralized power system?

Answer. Response was not received at the time of publication.

Question 3. We are not only falling short of our goal to scan 100 percent of U.S.-bound cargo containers, but it is also my understanding that multi-energy portal scanners leave a sizable blind spot with the containers we do scan, because they have a very limited ability to penetrate dense cargo. This is a major security concern for the Port of Los Angeles in my district, and for many of our Nation's seaports. Are there alternative scanners that may produce better results? And, if so, does DHS plan on utilizing these alternatives at our seaports?

Answer. Response was not received at the time of publication.

Question 4. As of July 2022, the Port of Los Angeles has been hit with almost 40 million cyber attacks per month, with most attacks coming from Europe and Russia. What precautions have DHS and the FBI taken to combat against these potential cyber threats, particularly those that could harm or disrupt the flow of cargo at our Nation's busiest seaport?

Answer. Response was not received at the time of publication.

QUESTIONS FROM RANKING MEMBER JOHN KATKO FOR HONORABLE ALEJANDRO MAYORKAS

Question 1a. Due to botched screening and vetting efforts during the U.S. withdrawal from Afghanistan, Customs and Border Protection (CBP) admitted or paroled dozens of evacuees with derogatory information into the country, including one individual who had been liberated by the Taliban from an Afghanistan prison and another who was determined to be a National security threat by the FBI 3 months after being granted entry to the United States.

Provide the total number of individuals with derogatory information who were transported into the United States as a result of Operation Allies Refuge and Operation Allies Welcome.

Question 1b. What is the current status of these individuals? Have all of these individuals been apprehended? What is being done with them once apprehended?

Answer. Response was not received at the time of publication.

Question 2. What are the overall impacts of the Afghanistan relocation effort as viewed by your agency? What continuing impacts should we anticipate both in the homeland, as evacuees assimilate to the United States, and abroad, as Foreign Terrorist Organizations (FTOs) continue to flourish in the post-withdrawal climate?

Answer. Response was not received at the time of publication.

Question 3. The People's Republic of China (PRC), the Democratic People's Republic of North Korea (DPRK), Russia, and Iran have all been involved in malicious cyber attacks against the United States, harming our critical infrastructure sectors, attempting to influence our democratic processes, and compromising Government projects.

Explain your agency's work to mitigate these threats, especially in conjunction with the cyber nexus of other threat vectors, including Transnational Criminal Organizations (TCOs) and FTOs?

Answer. Response was not received at the time of publication.

Question 4a. More than a year has passed since the conclusion of Operation Allies Refuge and the height of Operation Allies Welcome, allowing us time to analyze and reflect on the challenges each operation faced.

In September 2022, the DHS OIG released a report highlighting DHS's screening and vetting failures. This included issues from falsely recording dates of birth for evacuees to failure to collect biometric information such as fingerprints. What is DHS doing to remedy these failures?

Question 4b. The committee was notified by a source from the Department of State that DHS, along with partner agencies assisting in the evacuation, would issue identification cards/papers to evacuees who did not present identifying paperwork, basing information on the cards/papers (which included name and date of birth) solely on the word of the evacuee. How many of these cards/papers were issued during the operations?

Answer. Response was not received at the time of publication.

Question 5. On August 24, 2022, following the recommendation of the Homeland Security Council, you terminated the DHS Disinformation Governance Board. However, according to reports published at the end of October, DHS and the FBI have continued policing speech, even pressuring private companies to do so on your behalf. Has DHS requested that tech and social media companies remove or label posts as misinformation, disinformation, or malinformation in the lead up to the 2020 election?

Answer. Response was not received at the time of publication.

Question 6a. Please discuss in detail what the Department plans to do to help alleviate the devastating migration crisis we face.

Ninety-eight non-U.S. citizens listed on the terrorist watch list were caught attempting to enter the homeland between ports of entry. Please discuss the challenges our brave Border Patrol agents face in apprehending these individuals as well as the threats those who evade detection present to homeland security.

Question 6b. Given your record over the last 2 years, how can the American people expect you to prioritize the security of the Southwest Border throughout fiscal year 2023?

Answer. Response was not received at the time of publication.

Question 7a. On October 12, 2022, the Department announced a new legal entry path specifically targeting Venezuelan migrants. This path would be a fully on-line process for up to 24,000 qualifying Venezuelans. Under this new policy, Venezuelan migrants who cross into the United States illegally will be returned to Mexico.

Please explain the reason why this new policy targets Venezuelans and no other nationality? Does the Biden administration intend to expand this program beyond Venezuelans?

Question 7b. The National Border Patrol Council has stated there will be a daily cap on the number of Venezuelans that Mexico will receive as part of this initiative. What is that daily total cap? What will happen to Venezuelan nationals once that cap is exceeded?

Question 7c. It is already evident the Department's new policy may increase the potential number of Venezuelan gotaways. How does the Department intend to address this potential increase?

Answer. Response was not received at the time of publication.

Question 8. At the beginning of November, the U.S. Border Patrol reported a more than 500 percent increase in encounters with Cuban migrants in South Florida since the same time last fiscal year. South Florida has seen more than 800 migrants arrive since October 1, 2022 in more than 50 landings. At the same time, the number of U.S. Coast Guard personnel recruitments has plummeted, with the USCG offering unheard-of $50,000 signing bonuses to encourage enlistments.

Do you believe our maritime security readiness is in jeopardy in the face of these recruitment issues and increased maritime-based migration? Please describe how you plan on addressing this critical shortage of personnel and what you are doing, other than the signing bonus, to bolster Coast Guard recruitment.

Answer. Response was not received at the time of publication.

Question 9a. As of the end of September 2022, Immigration Court judges dismissed a total of 63,587 cases because Border Patrol agents are not filing the "Notice to Appear" (NTA) with the Immigration Court. Without a filed NTA, a case cannot proceed, meaning that 1 out of every 6 Court cases were thrown out for this reason in the past fiscal year, and the migrant tied to that case is unaccounted for.

What is the Department doing to ensure that all NTAs are filed with Immigration Court to ensure that thousands of migrants are not left in limbo and are not lost in the interior of our homeland?

Question 9b. Are you aware of the reasons why Border Patrol agents are not filing NTAs with the Immigration Court System?

Answer. Response was not received at the time of publication.

Question 10a. Under the Biden administration's policies, ICE removals have plummeted to a fraction of the normal levels.

Provide a monthly breakdown of interior enforcement actions—arrests, detentions, and removals—which ICE has effectuated since January 2019.

Question 10b. As the number of migrants attempting to enter the United States continues to surpass historic records, growing in tandem with an increasing flow of

illegal narcotics, human trafficking, and transnational crime in the U.S. homeland, has the Department considered any alternative policy options regarding deportation?

Question 10c. How do you reconcile President Biden's weakened enforcement priorities with the fact that because of these policies, fewer serious criminals are being removed?

Answer. Response was not received at the time of publication.

Question 11. Over the past several years, supply chain attacks have greatly increased and have the potential to impact thousands of victims simultaneously. What steps has the Department taken to ensure a robust commercial cyber incident response capacity that could be called upon in times of need?

Answer. Response was not received at the time of publication.

Question 12a. While many illicit drugs are seized at a port of entry, we also know that drugs like fentanyl are coming across the border between ports of entry:

Provide an estimate of the quantity (in pounds) of fentanyl that has been transported into the United States through the southwest land border, northern land border, and otherwise entered the interior broken down by each of these respective locations, as well as by month, from Jan. 2021 to present.

Question 12b. What are your plans to provide CBP personnel with the technology and resources to intercept a larger percentage of illicit drugs flowing across our border?

Question 12c. Due to the influx of migrants, CBP officers and agents are being pulled away from their primary mission to assist with processing individuals into the United States. With the lack of front-line officers and agents patrolling the border, how is this hampering CBP's ability to intercept these deadly drugs?

Answer. Response was not received at the time of publication.

Question 13a. Following the Russian invasion of Ukraine earlier this year, CISA developed the Shields Up campaign to bolster cyber defenses across public and private sectors and throughout all sectors of our economy.

What more is CISA and the Department doing to prepare critical infrastructure owners and operators to mitigate Russian cyber threats stemming from the conflict?

Question 13b. As we brace for the potential of escalatory actions by the PRC in Taiwan, what is CISA and the Department doing to mitigate cyber risk based on the intelligence community's assessment of the PRC's specific tactics, techniques, and procedures (TTPs)?

Answer. Response was not received at the time of publication.

Question 14. To attempt to combat the crisis on the Southwest Border, you have deployed highly-trained and highly-skilled Federal Air Marshals (FAMs) to perform non-law enforcement duties such as hospital watch, transportation, and welfare checks. DHS is removing hundreds of FAMs from the skies during one of the busiest travel seasons of the year to send them to the border, even though you have stated that America's aviation infrastructure is a very high threat and a target. How many high-risk flights are not being covered due to your decision to deploy FAMs to the border? How many FAMs have already been sent to the border, or are scheduled to be sent, who have not volunteered for the deployment?

Answer. Response was not received at the time of publication.

Question 15. In the case *Texas* v. *Biden* (Case 2:21–cv–00067 N.D. Tx), DHS was filing monthly status reports with the court reporting on six distinct topics. Those updates ended in August (covering the July reporting period). Provide the monthly data, in the form it was provided to the Court, to be current through November 2022.

Answer. Response was not received at the time of publication.

Question 16. Provide an estimated number of gotaways who have crossed the southwest land border, northern land border, and otherwise entered the interior broken down by each of these respective locations, as well as by month, from Jan. 2021 to present.

Answer. Response was not received at the time of publication.

Question 17. Provide the monthly total, from January 2019 to present, of all Southwest Border encounters—both at and between Ports of Entry—delineated by citizenship/nation of origin. Provide the citizenship/nation of origin, from January 2019 to present, of all Southwest Border encounters subsequently determined to be present within the Terrorist Screening Dataset.

Answer. Response was not received at the time of publication.

Question 18. How does DHS anticipate the granting full legal status to 11 million unlawful migrant aliens present in the United States will affect the total number of future apprehensions, arrests, detentions, and removals at the Southwest Border? How did DHS formulate this prediction? How does DHS anticipate the granting full legal status to 11 million unlawful migrant aliens present in the United States will

affect the time line and backlog of adjudicating new cases at the Southwest Border? How did the Department formulate this prediction?

Answer. Response was not received at the time of publication.

Question 19. Provide the Department's working definition of the below terms. What is the basis for each of these respective definitions? What is the authority for each of these respective definitions? What is DHS's statutory authority to determine each of these respective definitions? Explain how a DHS employee, or an employee of any DHS component, determines if information qualifies as each of these respective definitions. What training does DHS provide employees to make this determination? Are there written guidance documents? If so, please provide them.

- Misinformation
- Disinformation
- Malinformation

Answer. Response was not received at the time of publication.

Question 20. What entities, companies, executives, and other contacts are DHS's largest private-sector partners in its Misinformation, Disinformation, and Malinformation efforts? What entities, agencies, officials, and other contacts are DHS's largest Government partners in its Misinformation, Disinformation, and Malinformation efforts?

Answer. Response was not received at the time of publication.

Question 21. What non-governmental organizations, contacts, and sources of information do DHS employees and contractors rely on to help determine whether something is Misinformation, Disinformation, and/or Malinformation? In which countries are those non-governmental organizations, contacts, and/or sources of information based? From what sources—including but not limited to the U.S. Government and/or non-U.S.-based entities, organizations, or governments—do those organizations receive funding?

Answer. Response was not received at the time of publication.

Question 22. Rank the 5 greatest threats posed by the PRC, in order, as you see them.

Answer. Response was not received at the time of publication.

Question 23. How is DHS ensuring that foreign students from the PRC who pose counterintelligence risks are not admitted into the United States? How is DHS preventing Chinese nationals from gaining access to sensitive research at universities or other publicly-funded institutions? How does DHS discourage State and local governments from continuing to procure Chinese tech that is banned from Federal procurement, including from companies like Huawei, ZTE, Hikvision, Dahua, and Hytera?

Answer. Response was not received at the time of publication.

Question 24. How will DHS support the National Biodefense Strategy's objective to update and upgrade National and SLTT capabilities for contact tracing, including digital technologies to facilitate contact tracing, to enable the containment of infectious pathogens during future biological incidents? How will DHS support the National Biodefense Strategy's objective to detect, report, and respond to diseases brought across the Nation's open borders? How will DHS support the National Biodefense Strategy's goal to "Promote Evidence-Based Health Communication to the Public," including the increasing vaccine uptake rates and its objectives to coordinate information?

Answer. Response was not received at the time of publication.

Question 25. With the surge of migrants along the Southwest Border, what specific efforts is DHS taking to ensure the vetting and screening of each individual who is encountered at a port of entry and between ports of entry? Where are DHS resources and capabilities lacking in terms of vetting and screening? What is being done to handle these inefficiencies?

Answer. Response was not received at the time of publication.

Question 26. With no confirmation on the credibility of migrant biographical data provided by other countries, how does DHS ensure the accuracy of their screening systems? How is DHS verifying that the data used for these processes is accurate, up-to-date, and objective?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE SHEILA JACKSON LEE FOR CHRISTOPHER A. WRAY

Question 1a. We have seen a sustained rise in the use of influence operations to sway U.S. policy, manipulate elections, weaken the United States' geopolitical standing, and attempt to contravene our democratic process.

What changes have you seen in the frequency, magnitude, and impact of misinformation and disinformation operations since last year?

Question 1b. In what ways, and to what extent, do DHS and the FBI work together through such means as coordinating strategies, personnel, and other resources to combat the threat of influence operations?

Answer. Response was not received at the time of publication.

Question 2. The 2021 Annual Threat Assessment by the Office of the Director of National Intelligence found that ISIS and al-Qaeda remain the greatest Sunni terrorist threats to U.S. interests overseas but that "U.S.-based Lone Actors and Small Cells with a broad range of ideological motivations pose a greater immediate domestic threat."

How can the U.S. Government use policy and law to address the rise in groups seeking to organize themselves as militias that use intimidation and force to influence the political process?

Answer. Response was not received at the time of publication.

Question 3. Human trafficking and child exploitation are often spoken about as if they are separate crimes committed by separate parties.

In what ways, and to what extent, are human trafficking and child exploitation interrelated? Are the same perpetrators undertaking both crimes?

Answer. Response was not received at the time of publication.

QUESTIONS FROM RANKING MEMBER JOHN KATKO FOR CHRISTOPHER A. WRAY

Question 1a. Due to botched screening and vetting efforts during the U.S. withdrawal from Afghanistan, Customs and Border Protection (CBP) admitted or paroled dozens of evacuees with derogatory information into the country, including one individual who had been liberated by the Taliban from an Afghanistan prison and another who was determined to be a National security threat by the FBI 3 months after being granted entry to the United States.

Provide the total number of individuals with derogatory information who were been transported into the United States as a result of Operation Allies Refuge and Operation Allies Welcome.

Question 1b. What is the current status of these individuals? Have all of these individuals been apprehended? What is being done with them once apprehended?

Answer. Response was not received at the time of publication.

Question 2. What are the overall impacts of the Afghanistan relocation effort as viewed by your agency? What continuing impacts should we anticipate both in the homeland, as evacuees assimilate to the United States, and abroad, as Foreign Terrorist Organizations (FTOs) continue to flourish in the post-withdrawal climate?

Answer. Response was not received at the time of publication.

Question 3. The People's Republic of China (PRC), the Democratic People's Republic of North Korea (DPRK), Russia, and Iran have all been involved in malicious cyber attacks against the United States, harming our critical infrastructure sectors, attempting to influence our democratic processes, and compromising Government projects.

Explain your agency's work to mitigate these threats, especially in conjunction with the cyber nexus of other threat vectors, including Transnational Criminal Organizations (TCOs) and FTOs?

Answer. Response was not received at the time of publication.

Question 4. The Chinese Communist Party's (CCP) strategy of "Military Civil Fusion" aims to establish the People's Liberation Army (PLA) as a globally dominant military force by 2049. To achieve this goal, the CCP has worked to obtain cutting-edge technology, often through theft. This theft has come in many forms, including through the infiltration of American research and aggressive talent recruitment programs. Could you please explain to the committee the various ways the CCP pursues its goals through theft and espionage and how the FBI has worked to mitigate this threat?

Answer. Response was not received at the time of publication.

Question 5. You have expressed concern over potential terrorist attack on U.S. soil emanating from Afghanistan given the growing intelligence gaps since the U.S. withdrawal last August. Could you please elaborate on this concern given our new understanding of the vetting challenges cited in the DHS OIG report on Operation Allies Welcome?

Answer. Response was not received at the time of publication.

Question 6. The United States' global competition with the PRC presents one of the greatest challenges the United States will face this century. You yourself have said "the greatest long-term threat to our Nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China." Could you please elaborate on this statement?

Answer. Response was not received at the time of publication.

Question 7a. The 2022 Annual Threat Assessment states, "Transnational cyber criminals are increasing the number, scale, and sophistication of ransomware attacks, fueling a virtual ecosystem that threatens to cause greater disruptions of critical services world-wide."

As the threat of ransomware cascades across all sectors of our Nation's economy, and threatens to disrupt global services, what practical steps do you recommend critical infrastructure owners and operators as well as small business owners implement to mitigate this risk?

Question 7b. Who is the first person a small business owner should contact if they experience a ransomware attack?

Question 7c. How does the FBI work with other interagency partners to create situational awareness of reported ransomware attacks across the Federal Civilian Executive branch?

Answer. Response was not received at the time of publication.

Question 8a. The DHS Office of Intelligence and Analysis (I&A) is charged with the mission to equip the Homeland Security Enterprise with the timely intelligence and information it needs to keep the homeland safe. I&A's customers and partners include DHS leadership, DHS components, State, local, Tribal, territorial, and private-sector partners, and the IC. Could you please describe the nature of your organization's relationship with I&A?

Question 8b. How often does your organization collaborate with I&A on an issue area or arising threat?

Question 8c. How often does your organization receive an I&A product that is used to bolster your organization's mission?

Question 8d. What challenges have you experienced in your collaboration with I&A?

Question 8e. Are there any aspects of I&A's collection or analysis processes that you think could be improved? If so, how?

Answer. Response was not received at the time of publication.

Question 9a. At the World Wide Threats hearing in 2020 you stated "DVEs pose a steady and evolving threat of violence and economic harm to the United States. Trends may shift, but the underlying drivers for domestic violent extremism—such as perceptions of government or law enforcement overreach, sociopolitical conditions, racism, antisemitism, Islamophobia, misogyny, and reactions to legislative actions—remain constant." How has this threat evolved since your testimony in 2020? Please provide annual statistics from 2016 through present for the following.

How many DVE threats were identified arising from sociopolitical conditions? How does the FBI define "sociopolitical conditions" in the above context? How many DVE threats were identified arising from racism? How does the FBI define "racism" in the above context? How many DVE threats were identified arising from antisemitism? How does the FBI define "antisemitism" in the above context? How many DVE threats were identified arising from islamophobia? How does the FBI define "islamophobia" in the above context? How many DVE threats were identified arising from misogyny? How does the FBI define "misogyny" in the above context? How many DVE threats were identified arising from reactions to legislative actions? How does the FBI define "reactions to legislative actions" in the above context?

Question 9b. How many white RMVEs committed ideologically-motivated incidents and violence against Black individuals? How many white RMVEs committed ideologically-motivated incidents and violence against Asian individuals? How many Black RMVEs committed ideologically-motivated incidents and violence against white individuals? How many Black RMVEs committed ideologically-motivated incidents and violence against Asian individuals? How many Asian RMVEs committed ideologically-motivated incidents and violence against white individuals? How many Asian RMVEs committed ideologically-motivated incidents and violence against Black individuals?

Answer. Response was not received at the time of publication.

Question 10. In September 2021, the Attorney General circulated a memo labeling parents at school board meetings "domestic terrorists" and directing the FBI to collaborate with U.S. Attorneys and other local officials to address this alleged issue. Explain all actions the FBI has taken in the implementation of this memo. Explain, for each field office, all actions they've taken to implement the Attorney General's memo.

Answer. Response was not received at the time of publication.

Question 11. The FBI has recently conducted a series of investigations and arrests related to FACE Act violations at abortion providers. At the same time, it appears that a spate of attacks at pro-life pregnancy resource centers have led to no arrests and limited investigation. Provide the number of reported FACE Act violations stemming from actions at abortion providers. Provide the number of reported FACE

Act violations stemming from actions at pregnancy centers which do not provide abortion services. Provide the number of open investigations into alleged FACE Act violations stemming from actions at abortion providers. Provide the number of open investigations into alleged FACE Act violations stemming from actions at pregnancy centers which do not provide abortion services. Provide the number of FACE Act arrests stemming from actions at abortion providers. Provide the number of FACE Act arrests stemming from actions at pregnancy centers which do not provide abortion services.

Answer. Response was not received at the time of publication.

Question 12. Rank the 5 greatest threats posed by the PRC, in order, as you see them.

Answer. Response was not received at the time of publication.

Question 13. How is the FBI ensuring that foreign students from the PRC who pose counterintelligence risks are not admitted into the United States? How is the FBI preventing Chinese nationals from gaining access to sensitive research at universities or other publicly-funded institutions? How does the FBI discourage State and local governments from continuing to procure Chinese tech that is banned from Federal procurement, including from companies like Huawei, ZTE, Hikvision, Dahua, and Hytera?

Answer. Response was not received at the time of publication.

Question 14. Did the FBI have any Confidential Informants present at any polling place or voting location during the midterm election?

Answer. Response was not received at the time of publication.

Question 15. What internal FBI procedures exist to ensure that retaliation against whistleblowers does not occur? What steps has the FBI taken to protect whistleblowers from retaliation?

Answer. Response was not received at the time of publication.

Question 16. How has the FBI ensured compliance with the Attorney General's policy prohibiting Justice Department political appointees from participating in campaign-related activities in any capacity? How many violations occurred?

Answer. Response was not received at the time of publication.

Question 17. What steps have you taken to ensure that politically-driven individuals such as Timothy Thibault are not tasked with investigating cases of corruption or other politically-related matters? What initial and continuous vetting for political bias is done by the FBI regarding these agents and investigators?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE SHEILA JACKSON LEE FOR CHRISTINE ABIZAID

Question 1a. The 2021 Annual Threat Assessment by the Office of the Director of National Intelligence found that ISIS and al-Qaeda remain the greatest Sunni terrorist threats to U.S. interests overseas but that "U.S.-based Lone Actors and Small Cells with a broad range of ideological motivations pose a greater immediate domestic threat."

What is the National Counterterrorism Center's assessment of the scope and severity of the current threat of domestic violent extremism?

Question 1b. In what ways does NCTC distinguish between and assess domestic violent extremist groups that characterize themselves as militias and who, in some cases, stockpile weapons?

Answer. Response was not received at the time of publication.

QUESTIONS FROM RANKING MEMBER JOHN KATKO FOR CHRISTINE ABIZAID

Question 1a. Due to botched screening and vetting efforts during the U.S. withdrawal from Afghanistan, Customs and Border Protection (CBP) admitted or paroled dozens of evacuees with derogatory information into the country, including one individual who had been liberated by the Taliban from an Afghanistan prison and another who was determined to be a National security threat by the FBI 3 months after being granted entry to the United States.

Provide the total number of individuals with derogatory information who were transported into the United States as a result of Operation Allies Refuge and Operation Allies Welcome.

Question 1b. What is the current status of these individuals? Have all of these individuals been apprehended? What is being done with them once apprehended?

Answer. Response was not received at the time of publication.

Question 2. What are the overall impacts of the Afghanistan relocation effort as viewed by your agency? What continuing impacts should we anticipate both in the homeland, as evacuees assimilate to the United States, and abroad, as Foreign Terrorist Organizations (FTOs) continue to flourish in the post-withdrawal climate?

Answer. Response was not received at the time of publication.

Question 3. The People's Republic of China (PRC), the Democratic People's Republic of North Korea (DPRK), Russia, and Iran have all been involved in malicious cyber attacks against the United States, harming our critical infrastructure sectors, attempting to influence our democratic processes, and compromising Government projects.

Explain your agency's work to mitigate these threats, especially in conjunction with the cyber nexus of other threat vectors, including Transnational Criminal Organizations (TCOs) and FTOs?

Answer. Response was not received at the time of publication.

Question 4a. The DoD OIG discovered that Afghan evacuees were not vetted by the NCTC using all available data prior to entering the United States because CBP enrollments were compared against DHS data, which did not initially include all biometric data held by the DoD.

What steps have been taken to mitigate this issue?

Question 4b. Could you please discuss the efforts, if any, the NCTC has made in partnership with DHS to ensure proper data sharing is in place to prevent such an issue going forward?

Answer. Response was not received at the time of publication.

Question 5a. Foreign terrorism remains a persistent threat to the United States, both in the homeland and abroad. Following the U.S. withdrawal from Afghanistan, the country quickly returned to its status as a safe haven for terrorism. Are you concerned about this?

Question 5b. How concerned are you with the lack of visibility we have into the Taliban-run country?

Question 5c. Is the NCTC aware of any terrorist training camps currently existing in Afghanistan?

Question 5d. How do you perceive the withdrawal from Afghanistan will impact the threat landscape over the next decade?

Answer. Response was not received at the time of publication.

Question 6. Iran remains committed to its terrorist activities against the United States, both directly and via proxy attacks. In August 2022, the DOJ disclosed one such attack in which an Iranian national attempted to arrange the murder of former National Security Advisor John Bolton in retaliation for the death of Islamic Revolutionary Guard Corps-Quds Force (IRGC–QF) Commander Qasem Soleimani. Please describe to the committee the on-going threats presented from Iran.

Answer. Response was not received at the time of publication.

Question 7. The U.S. Border Patrol reported 98 encounters with people on the U.S. Government's terrorist watch list along the Southwest Border in fiscal year 2022. What are your concerns for this enormous increase in such encounters, especially with the context that there was an estimated 600,000 gotaways in fiscal year 2022?

Answer. Response was not received at the time of publication.

Question 8a. The DHS Office of Intelligence and Analysis (I&A) is charged with the mission to equip the Homeland Security Enterprise with the timely intelligence and information it needs to keep the homeland safe. I&A's customers and partners include DHS leadership, DHS components, State, local, Tribal, territorial, and private-sector partners, and the IC. Could you please describe the nature of your organization's relationship with I&A?

Question 8b. How often does your organization collaborate with I&A on an issue area or arising threat?

Question 8c. How often does your organization receive an I&A product that is used to bolster your organization's mission?

Question 8d. What challenges have you experienced in your collaboration with I&A?

Question 8e. Are there any aspects of I&A's collection or analysis processes that you think could be improved? If so, how?

Answer. Response was not received at the time of publication.

○