S. Hrg. 117–682

THREATS TO THE HOMELAND

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

NOVEMBER 17, 2022

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

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

U.S. GOVERNMENT PUBLISHING OFFICE
51–543 PDF WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
SARAH C. PIERCE, *Senior Counsel*
STERLIN A. WATERS, *Research Assistant*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
CLYDE E. HICKS JR., *Minority Director of Homeland Security*
JEREMY H. HAYES, *Minority Senior Professional Staff Member*
MARGARET E. FRANKEL, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
ASHLEY A. GONZALEZ, *Hearing Clerk*

CONTENTS

WITNESSES

THURSDAY, NOVEMBER 17, 2022

ALPHABETICAL LIST OF WITNESSES

APPENDIX

THREATS TO THE HOMELAND

THURSDAY, NOVEMBER 17, 2022

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

The Committee met, pursuant to notice, at 10:15 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Gary Peters, Chairman of the Committee, presiding.

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

OPENING STATEMENT OF CHAIRMAN PETERS[1]

Chairman PETERS. The Committee will come to order.

First of all, I would like to thank our witnesses for joining us and for your continued service to the American people. This hearing is an important opportunity for this Committee to hear from our nation's top national security and law enforcement officials about the threats facing our nations, and how Congress can ensure the Federal Government is prepared to protect our communities from them.

More than 20 years ago, the September 11th (9/11) terrorist attacks changed our nation forever. In response, Congress created the Department of Homeland Security (DHS) and our entire national security apparatus focused on keeping Americans safe from international terrorism.

However, in the more than two decades following those attacks the threats to our communities have evolved and have become increasingly complex.

While we must continue to monitor international terror threats, there is no question that we must be better prepared to defend against what top national security officials, including those before us today have called the most lethal terrorist threat to Americans: domestic terrorism fueled by white nationalist and anti-government ideologies.

Yesterday, I released a report detailing the results of my investigation. Alarmingly, my investigation found that DHS and the Federal Bureau of Investigation (FBI) are not adequately addressed the evolving domestic terrorism threat. Despite a requirement in law, written by myself and Senator Johnson, DHS and FBI have failed to effectively measure and share comprehensive data on

[1] The prepared statement of Senator Peters appears in the Appendix on page 55.

the threat posed by violent domestic extremists (DVE), and specifically white supremacist and anti-government violence.

Without this comprehensive data it is impossible for Congress, and for this Committee, to determine whether our nation's counterterrorism (CT) resources are effectively aligned to tackle the domestic terrorism threat. We need a data-driven approach to preventing deadly incidents like the January 6th Capitol breach, the tragic shooting in Buffalo, and countless other domestic terrorist attacks that have been fueled by hateful extremist ideologies. I look forward to hearing from our witnesses today about what resources and tools their agencies need to effectively collect data on domestic terrorism and to prevent these crimes.

Today we will also have the opportunity to discuss the significant threat that cyberattacks pose to our national and our economic security. I am proud of the bipartisan work Senator Portman and I have led this Congress to enact some of the most significant reforms to our nation's cybersecurity policy in history. Our reforms will ensure that DHS has the tools, resources, and authorities needed to protect critical infrastructure, State and local governments, and other targets from cyberattacks. However, there is more that must be done to continue securing our vulnerabilities from criminal hackers and foreign adversaries, and I look forward to discussing these topics today.

One of the most serious threats, and one of the toughest to tackle, is the threat posed by increasingly severe natural disasters and climate change. This is an existential threat to our planet, and unless it is addressed it will have a significant impact on our homeland security. Today we will hear more about how our national security agencies are tracking these challenges and how they are planning to address the security threats they present now and in the future.

We also have a challenging situation at our Southern Border, and today we will discuss the Administration's work to secure both our Northern and Southern Borders, and prevent illegal trafficking and stop the flow of deadly illicit drugs like fentanyl into our communities. Those are difficult missions that must be accomplished, ensuring that lawful international trade and travel can continue to flow smoothly at our ports of entry (POEs), and keep States like my home State of Michigan a hub for international commerce.

As our national security agencies continue to tackle these longstanding threats, they must also be prepared to counter emerging ones. Over the last few years the threat posed by unmanned aerial systems (UAS), or drones, has become increasingly perilous. Small drones, which can be purchased off the shelf at any electronic store, can be weaponized by malicious actors to damage our nation's critical infrastructure or inflict mass casualties.

Today's drones could be used to launch remote attacks on everything from government buildings to crowds at public events, including large sports stadiums. We cannot let the current authorities that help address this grave threat expire in December, and I will continue working to ensure those important authorities are extended and that they are updated.

Similarly, weaponized biological, chemical, nuclear and radioactive materials also remain a significant threat to our homeland

security. I have introduced bipartisan legislation with Senator Portman to reauthorize and strengthen the office in DHS charged with overseeing these threats, and I will continue working with my colleagues to pass it as soon as possible.

The scope and volume of these and many other national security threats requires Congress and this Administration to work together to ensure we are doing everything we can to keep Americans safe.

Today I am pleased to welcome back each of our witnesses to hear more about how their agencies are working to effectively carry out this daunting and essential mission, and I look forward to a productive discussion.

Before I turn things over I want to take a moment to recognize my colleague, Senator Portman, who is retiring this year.

Rob, it has been a real pleasure to work with you for the past two years on this Committee. I am grateful for all of your hard work and your diligence to help us pass so much meaningful, bipartisan legislation through this Committee, from providing important financial relief to the U.S. Postal Service (USPS), to strengthening our ability to detect and deter cyberattacks, and working to make our nation more secure and more effective for taxpayers. It has certainly been a real pleasure and I wish you Godspeed in all your future endeavors, but all the work you did here will certainly never ever be forgotten.

Senator CARPER. Mr. Chairman, will you yield to me for just a minute. I just want to say I am Tom Carper, and I approve that message. [Laughter.]

Chairman PETERS. I would also like to thank your Staff Director Pam Thiessen. You have been exceptional, and you have put together an incredible team. We have worked together, accomplished a lot together. Always have been open, maybe not agreeing fully, but always finding a way to try to find common ground. We wish you Godspeed as well in your future as well, Pam. Thank you. Thank you so much for that.

With that, Ranking Member Portman, you are recognized your opening remarks.

OPENING STATEMENT OF SENATOR PORTMAN[1]

Senator PORTMAN. Thank you, Chairman Peters, and just to respond to those comments, we appreciate the relationship we have had and the work we have gotten done. This Committee has done a lot on a bipartisan basis, and some of it does not get any notice because it is noncontroversial by the time we finish our process, but in the process I want to thank you and all the Members of the Committee for working with us to pass dozens of bills that are making an important difference to our constituents.

And to you and David Weinberg of your staff, we want to thank you for your willingness to work with us. Again, we have not agreed on everything, but we have been able to find common ground where possible and move the country forward. Thank you very much for that.

Today is my last hearing as Ranking Member, and it is appropriate that it be this hearing because it is so important to the over-

[1] The prepared statement of Senator Portman appears in the Appendix on page 58.

sight responsibilities of this Committee and more importantly, important to our country right now. We have, unfortunately, a proliferation of threats facing the homeland, and I appreciate the fact that the right people are here today before us to be able to address those concerns and particularly to talk about what the Administration is doing to counter those threats. Welcome to Secretary Mayorkas, Director Wray, and Director Abizaid. We look forward to hearing from you.

As the respective leaders of your agencies, you are responsible for overseeing thousands of career employees, men and women who wake up every day at DHS, the FBI, and the National Counterterrorism Center (NCTC), with a mission to safeguard our Nation, and on behalf of the entire Committee I want to thank those employees who are patriots and are doing their best to further that mission.

Every fall since the terrorist attacks on September 11, 2001, we have had this hearing. We are a little late this year because of scheduling issues, but I think it is really important that we hold it because it is a time to stand back a little bit and reflect on where we are and how we can work together to address these potential threats, and active threats. I can think of no greater priority for this Committee.

I am going to start with the crisis at the Southern Border because sadly, I am leaving at a time when we really have not made the progress we should have made on a bipartisan basis. But again, we have to raise these issues and attempt to solve some of these very significant problems.

The failed border policies from this Administration has ensured that not only do our nation's borders remain unsecure, but foreign adversaries, transnational criminal organizations (TCOs), and other nefarious actors can too easily enter our country now, and therefore threaten the safety and the security of our public.

This issue has not gotten better. It has gotten worse. In the past year, Border Patrol apprehended more than 2 million total unlawful migrants. This is up 143 percent since 2019. This chart[1] behind me shows, in color, kind of the blue, green, and red of where we have been. Fiscal year (FY) 2021 and fiscal year 2022 figure are on the right. We just got the final figures for fiscal year 2022, and unfortunately it tells a very dramatic story of us failing to secure that Southern Border.

This does not include the number of "got-aways," or individuals who are not detected. What we hear from the Border Patrol is that the number of got-aways has increased significantly as well.

These are criminals, often, who engage in human trafficking, criminals who involve themselves in the drug trade. This is about people but it is also about the fact that we have a record number of fentanyl shipments coming through the border, both through ports of entry and between the ports of entry now. We know this from anecdotal evidence but also because there is a record number of seizures of these deadly fentanyl shipments into our communities.

[1] The chart referenced by Senator Portman appears in the Appendix on page 113.

Fentanyl, of course, is what is causing the most number of overdose deaths at time when we have a record number, sadly, of overdose deaths in our country. In Ohio, we think it is between two-thirds and three-quarters of the deaths related to this one drug, deadly fentanyl, which is primarily coming across the Mexican border now.

This has been a tough couple of years, the worst two years of unlawful migration and the worst two years of drug seizures in our nation's history. I look forward to talking about that. We have to figure out how to move forward. Again, on a bipartisan basis, we have to figure out how to fix what is clearly a broken system.

Another issue I want to address today is the chaotic withdrawal from Afghanistan, what that means in terms of the United States. Afghans who stood with us and our allies were left behind to suffer under Taliban rule, and meanwhile more than 36,000 Afghans with no record of ever having partnered with us, some of whom may have ties to terrorist groups, were paroled into our country without proper screening and vetting.

I appreciate the fact that, Director Wray, you are here to talk about that in addition to Secretary Mayorkas, because, this is one, again, where if we made mistakes, and we can correct those mistakes. We can go back, and I know you are starting to do that, from testimony we have had both publicly and privately.

But, we had this unfortunate, chaotic, and precipitous withdrawal that caused a lot of issues, but one was paroling people into our country who were not properly screened. There have been three reports now from two inspectors general (IGs) documenting the failures of DHS vetting and then paroling known or suspected terrorist into our communities, and yet we just do not have an acknowledgment of that problem from DHS.

President Biden requested and received an additional $15 million for the FBI to conduct counterterror investigations of known or suspected terrorists among the Afghan evacuees released into our country by DHS. In other words, he asked for $15 million to give to the FBI to do this additional vetting, and yet the Administration says it is not a problem. Those two are inconsistent, of course. Perhaps we can talk about those divergent views on this panel this morning.

We all recognize the grave threat posed by our adversaries, such as Russia, Iran, and China, who rely on disinformation tactics to weaken our democracy. I think there is a consensus about that. But at home, we have to be much more careful around issues of domestic speech. We must respond to imminent threats of violence, of course—I do not think anybody on this Committee disagrees with that—but censoring constitutionally protected speech is an entirely different matter. To be precise, that should be a redline.

I hope we can all agree that the United States government should not censor the speech of our own citizens. Americans' speech, differences of opinion, and political viewpoints are not a threat to democracy, but actually a bedrock of it.

We know now that DHS disbanded its disturbing Disinformation Governance Board after significant public outcry, but we also know that it has continued its efforts to curb speech under the guise of countering misinformation or disinformation. The entanglement of

the FBI and DHS with social media platforms for the purposes of controlling narratives is something we need to talk about today. I think it is a deep concern that all Americans have that we not cross that red line.

Recent reports allege that DHS is colluding with Big Tech to moderate content in a way that conforms with the Biden administration's political views, including on the Afghanistan withdrawal and things like the origin of Coronavirus Disease 2019 (COVID–19).

Our democracy is also under threat because Congress and the Administration have been unwilling to confront the systematic theft of U.S. intellectual property by China which is undermining our national security and our economic security. Secretary Wray has been outspoken on this. His quote is, "There is no country that presents a broader, more severe threat to our innovation, our ideas, and our economic security than China." I could not agree more.

But every day, China reinforces the findings of our various investigations of this Committee, showing the staggering extent of the Chinese government's efforts to conduct influence and espionage operations in our country, and to steal American technology, research, and information for their own military and economic benefit. Addressing what the Communist Party of China is doing is more urgent than ever, and yet the Safeguarding American Innovation Act, which was reported out of this Committee, has been blocked from becoming law because of the unwillingness of Congress to confront this issue.

Cyberattacks are another significant issue facing every sector of our country. We talked about this a moment ago with Senator Peters. We have made some progress here in this Committee. I appreciate that. But cyberattacks are growing and they are a force multiplier for our adversaries. We have to understand that this is an issue that they are going to continue to use. Our economic and security is depending on technology, and we have to be sure that we are not vulnerable here. Compounding that problem is the inherent difficulty of attributing cyberattacks to specific nation-states or criminal groups.

Terrorism and targeted violence also remain serious threats to our country. This year, an Islamist terrorist gained entry to the United States and attacked a synagogue in Colleyville, Texas. In a separate incident, an Ohio-based Islamic State operative plotted to assassinate former President Bush. We are not out of the woods in terms of the Islamic terrorist threat.

I remain convinced that we can deal with these issues on a bipartisan basis, as we have in the past, but I am concerned about the threat posed by foreign terrorist organizations (FTOs), especially in the wake of our withdrawal from Afghanistan. Al-Qaeda continues to pose a threat. The Islamic State continues to expand and mobilize. Iranian-sponsored Shi'a terrorist groups target key U.S. interests and government officials consistently. We must remain vigilant as these organizations regroup and evolve.

We must restore confidence in the American public that we are committed to protect our nation from terrorism, espionage, and other homeland security threats, and this should be a bipartisan effort. We all have the same goal, a safe, secure American homeland.

With that said, I look forward to the testimony this morning, Mr. Chairman, but most importantly, the responses to our questions regarding the record of the Administration addressing these threats, what we can do going forward together. I will note that only last week did we finally receive overdue answers to questions that we had from last year's hearing. It took over a year. I hope that in this case we will get more prompt responses to Committee questions that are posed.

Thank you, Mr. Chairman. I look forward to the testimony.

Chairman PETERS. Thank you, Ranking Member Portman.

Before I swear in the witnesses I want to make sure everyone knows how this will proceed, both our witnesses and Members. We are going to have two rounds of questions today. The first round, as we normally do, will be seven minutes for each person. Then second round we are going to have five minutes per person on the second round, due to time constraints with all of our witnesses.

I am going to enforce those time limits perhaps a little more aggressively than I have in the past for everyone—seven minutes first round, five minutes the second round.

It is the practice of the Homeland Security and Governmental Affairs Committee (HSGAC) to swear in witnesses, so if each of you will stand and raise your right hand.

Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Secretary MAYORKAS. I do.

Mr. WRAY. I do.

Ms. ABIZAID. I do.

Chairman PETERS. Thank you, you may be seated.

Secretary Alejandro Mayorkas is the seventh Secretary of the Department of Homeland Security. Over his distinguished 30-year career as a law enforcement official and nationally recognized lawyer he has served as the Department's Deputy Secretary, as Director of U.S. Citizenship and Immigration Services (USCIS), and at the Department of Justice (DOJ) as Assistant United States Attorney (ASUA) in the Central District of California.

Mr. Secretary, thank you again for being here before the Committee. You may proceed with your opening remarks.

TESTIMONY OF THE HONORABLE ALEJANDRO N. MAYORKAS,[1] SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Secretary MAYORKAS. Chairman Peters, Ranking Member Portman, distinguished Members of this Committee, thank you for inviting me to join you today. Ranking Member Portman, thank you for your unwavering support of our Department.

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 grave threat we faced as a nation from ter-

[1] The prepared statement of Secretary Mayorkas appears in the Appendix on page 62.

rorism brought to our shores by foreign actors and foreign terrorist organizations.

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 platform 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 or small cells, domestic violent extremists seeking to further some political or social goal or act on a grievance, and home-grown violent extremists (HVE) looking to advance the interest of a foreign terrorist organization. From cyberattacks 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 cyberspace, our adversaries, hostile nations, and non-nation state cybercriminals 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, and North Korea, and cybercriminals 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 cyberattack, impacting our critical infrastructure earlier this year. Nation-state aggression is creating a heightened risk of chemical, biological, radiological, and nuclear (CBRN) related threats to Americans as well.

While fast-emerging technologies like unmanned aerial systems, artificial intelligence (AI), 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 counter unmanned aerial systems (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 indi-

viduals and national 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 workforce 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.

Chairman PETERS. Thank you, Secretary Mayorkas.

Director Christopher Wray is the eighth Director of the Federal Bureau of Investigation. Director Wray began his law enforcement career over two decades ago, serving in the Department of Justice as the Assistant U.S. Attorney for the Northern District of Georgia.

He has also served on the President's corporate Fraud Tax Force and supervised the Enron Tax Force, in addition to playing a key role in the national security objectives for the Department.

Director Wray, thank you for appearing before the Committee once again. You may proceed with your opening remarks.

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

Mr. WRAY. Good morning, Chairman Peters, Ranking Member Portman, and 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 the current threat landscape, what makes our current situation unique, and I would add particularly serious, is the fact that we are seeing so many different threat areas all elevated at the same time. I am proud of the work the FBI's agents, analysts, and professional staff are doing all across the country and around the world every day to rise to that challenge and 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 you are talking about 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

[1] The prepared statement of Mr. Wray appears in the Appendix on page 85.

very quickly from radicalization to action and often use easily obtainable weapons—think a gun, a knife, a car, a crude improvised explosive device (IED)—against soft targets, which is really just intelligence community (IC)-speak for everyday people going about their everyday lives.

Overseas, Islamic State of Iraq and Syria (ISIS) and al-Qaeda still aim to inspire, plan, and launch attacks against the United States and our allies, both abroad and here at home. As the Zawahiri strike this summer in Kabul reinforces, the threat of foreign terrorist organizations like al-Qaeda attempting to reconstitute in Afghanistan following our withdrawal is very real, and our ability to gather valuable intelligence on the ground inside Afghanistan has been reduced. That is just a reality, and all of that places a premium on our continued collaboration with our partners, both within the U.S. Government and internationally. We have 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 all growing more aggressive, more brazen, more 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.

But we are confronting that threat head on. Three weeks ago, for example, we unsealed charges against 13 individuals, 10 of them Chinese intelligence officers and government officers, for a variety of criminal efforts to exert influence right here in the United States on behalf of Beijing, and we have scores of investigations into the China threat in all 56 FBI field offices.

On the cyber front, China's vast hacking program is the world's largest by a mile, and they have stolen more of Americans' personal and business data than every other nation combined.

But, of course, China is not our only challenge in cyberspace, 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, each with scores of victims, as well as a 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 cybercriminal 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 multiyear scheme to compromise the networks of hundreds of organizations, many of which offer critical services Americans rely on every day.

These sort 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 kids who depend on it.

Our opponents in this space are relentless, and we have 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 those adversaries, removing their malware, taking down their botnets, and hunting them down all over the world.

Now that is just a snapshot really of some of the many threats we are tackling and does not 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 day.

Or our continued focus on human trafficking, where this August, through our annual Operation Cross Country, for instance, the FBI and our partners located more than 200 victims of human trafficking, many of them little kids.

Or the work our transnational organized crime section is doing, in partnership with agencies 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 the FBI's dedicated men and women are tackling each and every day is staggering, and 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.

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

Chairman PETERS. Thank you, Director Wray.

Director Christine Abizaid is the eighth Senate-confirmed Director of the National Counterterrorism Center. Previously, she served on the National Security Council staff as both Director for Counterterrorism and Senior Policy Advisor to the Assistant to the President for Homeland Security and Counterterrorism.

She has also served as Deputy Assistant Secretary of Defense for Afghanistan, Pakistan, and Central Asia, and as a Senior Intelligence Analyst for the Defense Intelligence Agency (DIA).

Ms. Abizaid, thank you again for appearing before this Committee. It is good to have you back. You may proceed with your opening remarks.

TESTIMONY OF THE HONORABLE CHRISTINE ABIZAID,[1] DIRECTOR, NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Ms. ABIZAID. Thank you very much. Chairman Peters, Ranking Member Portman, and Members of the Committee, thank you very much for the opportunity to appear before you today to discuss the overall terrorism landscape.

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 at home and abroad. An array of actors, whether foreign ter-

[1] The prepared statement of Ms. Abizaid appears in the Appendix on page 103.

rorist organizations, state sponsors of terrorism, or lone actors, are shaping the nature of today's threat.

This changed environment exists amid an ongoing transition for the counterterrorism community where CT, while still critical, is one of many competing priorities 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, turn to the overseas threat environment, and then end with some comments on the importance of our continued CT effort.

Regarding the United States homeland, terrorist organizations such as ISIS and al-Qaeda remain committed to attacking inside 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 networked and hierarchically directed 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 directed 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 (RMVEs), militia violent extremists (MVEs), and anarchist violent extremists (AVEs).

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

Transitioning to the overseas environment, Sunni- and Shia-driven terrorist movements worldwide continue to dominate the threat to Americans. ISIS and al-Qaeda continue to aspire to attack United States and other Western interests overseas, but have been more effective at pursing operations against regional and local adversaries.

For its part, ISIS in Iraq and Syria remains an intact, centrally led organizations that will most likely continue to pose both a global and local threat, this despite the death of its emir, Haji Abdullah, in February.

While significantly weaker than 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 the organization, but it does not put an end to al-Qaeda.

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 attacks inside the U.S. 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 Jama'at Nusrat al-Is lam al-Muslimin (JNIM) and Somalia-based affiliate, al-Shabaab.

Of note, we continue to monitor for signs al-Qaeda has chosen a successor to Zawahiri, now three months since his death. In addition to al-Qaeda affiliate leaders, we are particularly focused on the role that Iran-based legacy leaders, such as Sayf al-'Adl, may play in the future of the organization.

Transitioning from Sunni terrorism to threats emanating from Iran, its partners, and its proxies, Iran continue 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 Lebanese Hizballah have sought to plot attacks against former U.S. officials to retaliate for the death of Islamic Revolutionary Guard Corps (IRGC) Qods Force commander, Qasem Soleimani, 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 international terrorism and extremism environment that I just outlined continues to demand a collaborate, agile, and sufficiently resourced counterterrorism 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 two 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 the strategic success. In fact, the role of NCTC today is perhaps more important than ever. Charged with integrating and analyzing all terrorism information across the United States government and sharing that information with partners, both foreign and domestic, organizations like NCTC can help ensure that CT remains a foundational element of national security, even as other organizations must shift to other pressing priorities.

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. It is with great gratitude and privilege that I appear before you today and have the opportunity to recognize 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.

With that, Mr. Chairman, I am subject to your questions.

Chairman PETERS. Thank you, Director Abizaid.

Yesterday I released a report following a multiyear investigation on the growing domestic terrorism threat. I believe we provided it to each of the witnesses yesterday. This is also available through the website, the Homeland Security Committee website, to read in its entirety.

In the report we found that despite being required by law, my investigation found that DHS and FBI have failed to systematically track and report data on domestic terrorism, they have not appropriately allocated resources to match the current threat, and have not aligned definitions of domestic terrorism to ensure consistency across the investigations of these crimes. Quite frankly, it is hard to address this rising threat if we cannot quantify and define the scope of the problem so that we can tailor an appropriate response to, and the agencies appear not to be doing that.

Director Wray, we have seen think tanks and nonprofits collect more comprehensive about domestic terrorism attacks than the U.S. Government has been able to do. Why has the FBI been unable to collect and report complete data about domestic terrorism despite a Federal law requiring you to do so?

Mr. WRAY. Mr. Chairman, I know all too well that there have been frustrations in the reports that have been generated under the law that you are referring to. I think we have made progress between the first report and the second report, and we are committed to continuing to make progress. Some of the issues have to do with, if you go further back in time, before 2015 for example, we were using paper as opposed to electronic and so the ability to go back and track earlier than 2015 I know has been a source of tension at times.

In addition, State and local law enforcement and tribal law enforcement are not required to report domestic terrorism to us. While we do get lots of reports of that through our Joint Terrorism Task Forces (JTTF), it is not as systematic as any of us would like it to be.

Then you mentioned the terminology change. We have changed terminology over time. There are good reasons for that. But there is some risk then at having sort of an apple-to-orange type effect in the comparisons.

But we are committed to continuing to work with the Committee on this topic, and our data-tracking limitations should in no way be confused with our commitment to prioritizing this issue. I elevated racially motivated violent extremism to a national threat priority all the way back in June, I think it was, or the summer of 2019, and we have surged resources to address that, and the pace of investigations and arrests over my first 3.5 years as director, doubled, or in the case of arrests even tripled in this space.

We have been working hard on it but we do need more resources in this space, and our fiscal 2022 budget specifically asks for more resources to help address the domestic terrorism threat.

Chairman PETERS. I appreciate your work on this, you were right. The second report was better than the first report, and I would hope that we could work closely together to make the third report even better, because that information is obviously critical for us to understanding the scope of the problem and then design appropriate responses to it. But I appreciate your active engagement in that, Director Wray.

I also remain extremely concerned about the threat posed to our nation from bad actors using unmanned aircraft systems, to disrupt our society, or worse, to potentially conduct a lethal attack on our Nation.

Earlier this year this Committee unanimously passed a bill, authored by Senator Johnson and I, to protect our nation's airports, critical infrastructure, and public spaces from these evolving threats.

Secretary Mayorkas, as you are well aware, these authorities are set to expire next month, on the 16th of December. Could you explain to this Committee the consequences of allowing these authorities to lapse?

Secretary MAYORKAS. Chairman Peters, I am deeply appreciative of your and Senator Johnson's bipartisan effort to propose legislation to not only continue our authority to counter unmanned aerial systems but also to expand it critically, and that need is very grave.

Just yesterday I was meeting with experts who were speaking of the increased efficiency, sophistication, and capability of drones in terms of their visibility, the speed with which they can move, the distance with which they can move, and also the loads that they can carry. This poses a real threat, and we see it very often, sometimes by innocent operators who mistakenly interfere with the airspace and cause aircraft to reroute their journeys, to bad actors, and we see it quite tragically in the war zone that Russia created with its unprovoked assault on Ukraine.

These are extraordinarily sophisticated tools that can carry drugs, that can launch weaponry, and we must be able to counter it. It is only an increasing threat, and we hope that Congress passes the legislation that you and Senator Johnson have proposed.

Chairman PETERS. Thank you, Secretary. We have limited time and I am going to keep strict to seven minutes for everybody.

Director Wray, the FBI is the lead on protecting mass gatherings like the Super Bowl and other areas. How concerned are you about these authorities lapsing?

Mr. WRAY. We are deeply concerned, and we appreciate this Committee's leadership on this topic. It is important for Americans to understand that if that authority is not reauthorized next month that public gatherings like the Super Bowl in Arizona, like New Year's Eve in Times Square, like Formula One in Las Vegas, and I could go on, none of those things will have protection from this threat. All the times that we have deployed with the authority that this Committee has led the passage of before, we have located hundreds of drones that have been acting in violation of Federal law each time.

As the threat continues to grow, we are investigating, even as we speak, several incidents within the United States, of attempts to weaponize drones with homemade IEDs. That is the future that is here now, and this authority desperately needs to be reauthorized.

Chairman PETERS. Thank you, Director Wray, with eight seconds left of my time.

Ranking Member Portman, you are recognized for your questions.

Senator PORTMAN. Thank you, Mr. Chairman. I wanted to thank you and Senator Johnson for working on a bipartisan basis to put together this legislation. I am a co-sponsor of it. I know the House has a different view in terms of how they would like to approach it, but we have to get this one done. I mean, we just heard about

the importance of it, so I thank both of you for working on this issue, and it is less than a month when it expires, so we have to move, and move quickly.

I spoke in my opening statement about the appreciation we have for the men and women who you represent. We just learned from media accounts that five Customs and Border Protection (CBP) agents were shot, one fatally, during a vessel interdiction against suspected drug smugglers off the coast of Puerto Rico. This just happened, and our thoughts and prayers, of course, are with the family of the agent who was fatally shot and also with those agents who were wounded.

But I think it is a sober reminder of the sacrifices that the individuals who you represent today here make every day, and we owe them our support. It is a dangerous time, and this is an unfortunate example of that.

With regard to the Southern Border, we have talked a lot about this over the months, and years even. How do you take a broken system and fix it? Because clearly, if you look at this chart[1] behind me, it is broken. We have had all kinds of charts in this Committee and all kinds of discussions about it.

There was an interesting back-and-forth recently between President Biden's Chief of Border Patrol, Raul Ortiz, who works for you, as you know, Mr. Secretary, and the State of Florida. The Attorney General (AG) in Florida has a lawsuit against the Department with regard to the Southern Border. I just thought I would go over that quickly.

This has been the worst year of apprehensions ever, the last fiscal year, but the second-worst year was last year. These numbers speak for themselves. More than two million people apprehended between the ports of entry in 2022.

This summer, when the Chief of Border Patrol was questioned by the State of Florida he gave his answers under oath, and I would ask unanimous consent (UC) to place the transcript of the Border Patrol Chief's testimony into the record, Mr. Chairman.

Chairman PETERS. Without objection.

Senator PORTMAN. Secretary, I am going to ask you the same questions that the Chief of Border Patrol was asked to see if you agree with him, and if you could, please just give me a yes or no answer, as he did.

The first question, is the Southern Border currently in crisis? Yes or no.

Secretary MAYORKAS. Ranking Member Portman, the entire hemisphere is suffering a migration crisis. We are seeing an unprecedented movement of people from country to country. It is not restricted to the Southern Border. We are seeing an unprecedented movement of people throughout the Western Hemisphere, and I think the case of Venezuela is the most compelling example. With a population of between 25 and 28 million people, approximately eight million of them have left that country. Colombia is hosting 2.4 million Venezuelans.

Senator PORTMAN. I would ask you for a yes-or-no answer to the Southern Border. I have been to Colombia twice in the last year.

[1] The chart referenced by Senator Portman appears in the Appendix on page 113.

I am very aware of what is going on with regard to the displaced people out of Venezuela, and for that matter Nicaragua and Cuba.

But the question is all the more pressing. What are we doing about? Should we not be changing our policies at the border to deal with it instead of having this result.

My question to you again, is the Southern Border current in crisis? Yes or no.

Secretary MAYORKAS. We are seeing a significant challenge at the Southern Border, as we are seeing it throughout the hemisphere.

Senator PORTMAN. Chief Ortiz stated yes, just so you know. He said the obvious, which is yes.

Second question. Would you agree that an unprecedented number of unlawful migrants are entering the United States right now? Yes or no.

Secretary MAYORKAS. Ranking Member Portman, I believe that the number of encounters that we have had the border, I think it is approximately 2.3 million this past year, is the highest on record.

Senator PORTMAN. OK. So the answer is yes by Chief Ortiz, and it sounds like you agree with him on that.

Mr. Secretary, since when President Biden took office is it true that the number of migrants trying to unlawfully enter the United States has increased substantially? Yes or no.

Secretary MAYORKAS. It has, and there are many different factors that contribute to that.

Senator PORTMAN. OK. But I ask you these questions obviously because the answer was yes. He was candid and gave short answers. We cannot fix the problem unless we acknowledge it. We cannot fix the problem unless we understand the facts.

Secretary MAYORKAS. Yes.

Senator PORTMAN. We cannot fix the problem unless we are willing to be honest Republicans, Democrats, everyone alike, saying we have a crisis. If we do not fix this crisis at the border we will continue to see these same rules.

Secretary MAYORKAS. Ranking Member Portman, if I may, there has been a problem with our immigration system, an acknowledge one, unanimously, for years and years.

Senator PORTMAN. For years and years, but again, look at this chart. This is the numbers, so it has gotten far worse. Look, we do not have time to go into the details as to how we fix it, but you and I have talked about this a lot, Mr. Secretary. If the asylum system is not fixed, this will not end. If we do not give the Border Patrol more resources, this is not going to end. If we do not figure out a way to provide for deportations when people are here illegally, particularly when they are committing other crimes, this will continue.

We are unfortunately looking at a situation where, you mentioned Colombia, if you go to the countries throughout the hemisphere they believe this is a pull factor, our policies. The leadership of these countries actually do not want their people moving into the United States. That might seem counterintuitive to some people, but some of their best and brightest are leaving because of our pull

factor, because we are not putting in place the right policies to go to control our own Southern Border.

I have so many other questions, and we will get a chance in the second round. I hope to talk about some of these. With regard to the cyberattacks we talked about earlier, the agencies that have been compromised in some of these attacks concern us greatly. Yesterday, Cybersecurity and Infrastructure Security Agency (CISA) and the FBI issued a joint advisory detailing suspected Iranian government-sponsored actors' compromise of the Federal agencies using this Log4j vulnerability. I would ask, Mr. Chairman, to include that advisory in the record[2] so we have it as part of this record.

We have discussed this vulnerability at length in this Committee, another example of the issues.

My time is expiring here in a second, but can you just tell us, Secretary Mayorkas, what agencies are agency was compromised with regard to this latest announcement you made regarding the Iranian government-sponsored attack?

Secretary MAYORKAS. Ranking Member Portman, that identity has not been disclosed, and I would need to speak with my colleagues to determine whether I would be compromising any security interest in doing so.

Senator PORTMAN. Are you confident that the actors have been expelled from our Federal networks?

Secretary MAYORKAS. I will once again need to confer with my colleagues to determine the status of the effort by the bad actors.

Senator PORTMAN. We are considering, as you know, this Federal Information Security Modernization Act (FISMA) reauthorization to trigger cyber incident reporting to Congress. Would this be considered a major incident?

Secretary MAYORKAS. I believe so, Ranking Member Portman.

Senator PORTMAN. Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Ranking Member Portman.

Senator Carper, you are recognized for your seven minutes of questions.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Seven. OK.

To each of our witnesses, welcome. It is great to see you all again. Some of you I have known for a while and pretty well, and I even know your families. I just want to say, to begin with, we do not do these jobs by ourselves, whether you are on that side of the table or this side of the table. Our families put up with a lot, and we just want to thank your families for sharing you with us, especially as Thanksgiving approaches.

The first Secretary of Homeland Security was a guy named Tom Ridge from Pennsylvania, from Erie, Pennsylvania. We are both Vietnam veterans. We were congressmen together in the same freshman class. We were Governors together for a number of years. He remains a very close friend.

I joined this Committee, I was elected in, oh Lord, I want to say 22 years ago, and Joe Lieberman said, when I tried to decide what

[2] The information referenced by Senator Portman appears in the Appendix on page 114.

Committees to be on, he said, "You should try to get on the Governmental Affairs Committee." I said, "Well, I am interested in that," and he said, "It is just the perfect fit for you, a former Governor, former State treasurer. You care about things working well." And he said, "You should join the Committee," and I did. Two years later, 9/11 came along, and we ended up the whole world changed. Our whole world changed.

The nature of the threats that we faced the day that Tom Ridge was sworn into office to be our Secretary, and what we face today is unbelievable. It is just incredible how the world has changed, in not so good ways. I just want to say a special thanks to each of you and the folks you work with that help us try to address and be ready for the threats that are coming our way, almost every day.

I will start with Secretary Mayorkas, and in the second round of questions, if I am lucky, I will ask questions of our other two witnesses. But Mr. Secretary, again, my first question is to you. I know your job is not an easy one. Between leading a workforce of almost a quarter of a million people, whose duties range anywhere from aviation to border security, enhancing our nation's cyber posture, responding to natural disasters, and protecting the homeland, I hope that everyone here today can respect that and that your dedication and service to our nation is commendable. That goes for all three of our witnesses here today, and I thank you again for your service.

As we continue to see a number of encounters at our Southern Border, the Department of Homeland Security has been leading a whole-of-government response to address these challenges and to help keep our borders more secure. Mr. Secretary, can you just talk about some of the changes in migration patterns that we have seen at our Southern Border in the last year and a half, and what policies the Department has put in place to address these challenges? Specifically, can you speak to the investments in border technology and legal migration pathways and your level of engagement with other countries in the region, given that the migration patterns have been a hemispheric challenge? Please.

Secretary MAYORKAS. Senator Carper, thank you for acknowledging the challenge that these positions present. Of course, a challenge is all relative. Ranking Member Portman mentioned the tragic loss of one of our frontline personnel. Several other were gravely wounded. I was briefed on the situation very early this morning. These are brave members of our Air and Marine Operations within U.S. Customs and Border Protection. The difficulty of this job cannot be compared to the difficulty that our frontline personnel face every day, and their bravery and selfless service should be recognized. I appreciate Ranking Member Portman acknowledging that.

The migration patterns in the hemisphere have changed dramatically. When I was the Deputy Secretary we were very concerned about migration from the Central American countries of El Salvador, Guatemala, and Honduras. We have encountered now the highest level of encounters by Venezuelans, Cubans, and Nicaraguans, and that demographic, that changed demographic makes the challenge even more acute because our diplomatic relations with these countries is obviously quite strained and we are unable to remove as easily individuals from these countries of origin.

Of course, we implemented thus far, at an early stage, a very successful response to the Venezuelan migration, in particular.

We have six lines of effort, Senator Carper. We have surged resources to the Southern Border—personnel, technology, facilities, transportation capabilities. We have increased our processing efficiency. We are increasingly digitizing our processes, modernizing them so that the intake process and the screening and vetting process is enhanced and more efficient.

We are delivering consequences for unlawful entry. We have increased the level of prosecution of illegal entry when individuals seek to evade law enforcement. We have sought to bolster the capacity of non-governmental organizations (NGOs) and State and local jurisdictions. We are conducting an unprecedented disruption campaign against the smuggling organizations and the transnational criminal organizations.

We are also working very closely with our partners to the south to deter irregular migration. The declaration that was signed in the Summit of the Americas in Los Angeles several months ago speaks powerfully of that. We need countries throughout the hemisphere to enforce their laws of humanitarian relief as well as their laws of enforcement.

This is a multipronged effort to address a multinational challenge throughout the hemisphere.

Senator CARPER. Thank you for that response.

Most of us are people of faith, and there is a verse of scripture in Matthew 25 that I think a lot of us are familiar with, "When I was hungry, you would feed me. When I was thirsty, you gave me drink. When I was naked, you clothed me. When I was sick and imprisoned, you visited. When I was a stranger in your land, did you welcome me?" When I was a stranger in your land, did you welcome me?

The last one is hard. In fact, they are pretty difficult. But the last one is especially hard.

In an effort to try to reduce the likelihood that people are going to risk life and limb to come to this country and relocate here, they leave, in some cases, hellacious conditions in which they lived. They have come many miles, hundreds of miles sometimes, to reach our borders, and some of us think, why do we not give them the opportunity if they want to come here, to actually go to our embassies or our consulates and let those intentions be known and to work from there?

Would you respond to that idea, please? Just briefly?

Secretary MAYORKAS. Senator Carper, our laws are laws of humanitarian relief and laws of accountability. We have an asylum system that is one of the sources of pride of our country and we enforce the law. When an individual qualifies for humanitarian relief they are, under the law, entitled to remain here, and if they do not qualify they are to be removed, and we are enforcing the laws in every respect.

Senator CARPER. Thanks so much. Thanks, Mr. Chairman.

Chairman PETERS. Thank you, Senator Carper.

Senator Johnson, you are recognized for your questions.

OPENING STATEMENT OF SENATOR JOHNSON

Senator JOHNSON. Thank you, Mr. Chairman. Director Wray, you made a comment here, in answer to the Chairman's questioning, that you were committed to working with this Committee. You will excuse me if I find those words ringing incredibly hollow. I had to subpoena you, as Chairman of this Committee. I really did not get anything. I have written repeated letters, either with no response whatsoever or a nonresponse response.

It is one of the reasons that I am very grateful to all the whistleblowers that are coming forward, to various committees, to various members, people of integrity within your organizations, blowing the whistle on the corruption at some of the highest levels of the FBI.

First question. Do you commit, publicly, that the FBI will not retaliate against those whistleblowers?

Mr. WRAY. Senator, we will not retaliate against whistleblowers. I take the protections that are in law and regulation of whistleblowers extremely seriously.

Senator JOHNSON. I will hold you to that.

Mr. WRAY. Just like I take compliance with all of our other rules very seriously.

Senator JOHNSON. Yes. Senator Grassley wrote you a letter on July 25, 2020, in which he said that whistleblowers to his office reported that FBI officials initiated a scheme to downplay derogatory information on Hunter Biden for the purpose of shutting down investigatory activity related to his potential criminal exposure by labeling it, "disinformation." Boy, that is a familiar term. That scheme was hatched in August 2020.

Also included, he said, in August 2020, FBI supervisory intelligence analyst, Brian Auten, opened an assessment which was used by FBI headquarters team to improperly discredit negative Hunter Biden information as disinformation and caused investigative activity to cease.

Have you responded to Senator Grassley's letter that he wrote over three months ago?

Mr. WRAY. Senator, I know there have been a whole slew of letters, and I believe we have responded to a number of them. But sitting here I cannot tell you which ones——

Senator JOHNSON. You have not.

Mr. WRAY [continuing]. Which ones we have responded to and which ones we have not.

Senator JOHNSON. Have you looked into those charges, that there was a scheme hatched in August 2020, to downplay the derogatory information on Hunter Biden? Have you looked into that personally?

Mr. WRAY. We have, as we speak, a number of personnel matters that are underway, and for reasons which I am sure you can appreciate we cannot discuss personnel matters.

Senator JOHNSON. I know that is always your excuse. No, I got it. I understand how you remain above the law by using that excuse repeatedly.

The reason I am a little sensitive on August 2020 is that on August 6th, both Senator Grassley and I received an unsolicited briefing by members of the FBI, which I knew immediately was a setup. No new information whatsoever. I knew it was a setup, and I was

correct because nine months later, on May 1st, it was leaked to The Washington Post to smear me.

I have written you publicly a number of times, asking who directed that briefing. Are you prepared to tell me, in public, who directed that briefing now?

Mr. WRAY. Senator, first off, I cannot discuss specific defensive briefings, more broadly, and that is a longstanding practice.

Senator JOHNSON. Tell me then why have you refused to meet with us to privately tell us who directed that briefing?

Mr. WRAY. If I may finish my answer to the question. It is a longstanding practice not to discuss specific defensive briefings. We have, as my understanding, responded in writing to a letter that you sent. I think responded back——

Senator JOHNSON. It is bureaucratic——

Mr. WRAY [continuing]. At the end of 2021.

Senator JOHNSON. It is bureaucratic gobbledygook, is what that is.

Mr. WRAY [continuing]. And——

Senator JOHNSON. That is not a response.

Mr. WRAY [continuing]. We offered in that letter to provide a senior executive of the FBI to walk through, in detail, our process.

Senator JOHNSON. What your process is but not specifically who directed a briefing that was used to smear me.

Have you looked into the leaking of that briefing The Washington Post? Have you investigated that?

Mr. WRAY. I am not going to discuss specific investigations. As to the briefing question, and who directs it, let me be very clear about this. When it comes to election-related defensive briefings there is not a single person who makes that decision. That is an interagency process that was set up by the prior administration, signed off on by the former President prepared by the Office of the Director of National Intelligence (ODNI)——

Senator JOHNSON [continuing]. There are persons in that interagency. Correct? There would be persons. We should know who those persons are. Why will you not tell us who directed that briefing, the persons then?

Mr. WRAY. I would refer you to the process that was put in place, and we can give you more information about the process if you would like.

Senator JOHNSON. Have you read Senator Grassley's and my report on Hunter Biden's corruption, issued in September 2020 and November 2020? Have you read those reports?

Mr. WRAY. I have had a chance to look at it.

Senator JOHNSON. Do you see any sign of Russian disinformation in those reports?

Mr. WRAY. That would be a hard question for me to answer.

Senator JOHNSON. No, it is very easy.

Mr. WRAY. What I would say——

Senator JOHNSON. It is a very easy answer. There is no Russian disinformation. That report is completely clean of any interference of foreign influence, although we have been falsely accused, including by the Chairman of this Committee, of spreading Russian disinformation.

Are you aware of the FBI having any involvement whatsoever in the October 19, 2020, public statement by 51 former intelligence officials?

Mr. WRAY. I am not aware of any involvement by the FBI in what you are describing.

Senator JOHNSON. The reason I ask is, if it is true that in August 2020, the FBI initiated a scheme to downplay derogatory information on Hunter Biden, it would seem like maybe part of that scheme would be to get intelligence officials to issue a letter that stated that the laptop had all the earmarks of a Russian information operation. That was totally false. We now know that the Hunter laptop is completely authentic.

The point I am trying to make here is the unsolicited briefing that was leaked in May 2021, was used to smear me and interfered into the U.S. Senate election of November 2022. One of the whistleblowers to my committee has stated that the FBI was no longer going to interfere in elections, something to that effect. I cannot find it right now and I am running out of time. Oh, here it is. The FBI is, "not going to change the outcome of the election again."

The FBI certainly tried to by leaking, or somebody leaked that FBI briefing. Are you going to investigate that? Because that is the election interference, and let us face it—this letter by 51 intelligence officials, this interfered in the 2020 election to a far greater extent than anything Russia or China ever could have hoped to accomplish. You have to acknowledge that. It has to be investigated. I have no faith that you will do so.

Chairman PETERS. Thank you, Senator Johnson.

Senator Hassan, you are recognized for your questions.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you, Chair Peters, and I want to thank you and Ranking Member Portman for holding this hearing today. Thank you to our witnesses for being here. I want to add my prayers and thoughts for the CBP officers, the officer who was fatally wounded and those who were gravely wounded, and to their families. I think it is fair to say that the people of New Hampshire and the United States are holding these brave men and women in our prayers.

Secretary MAYORKAS. Thank you.

Senator HASSAN. I also wanted to take the opportunity, although he has stepped out for a moment, just to thank Ranking Member Portman for his years of service and for his work on this Committee and for the bipartisan work that he has led.

Again, to all of the witnesses, but more importantly to the men and women you lead, thank you to you, to them, their families. The first priority of government is to ensure the safety and security of its citizens, and your work is really critical to that mission.

Director Abizaid, I want to start with a question to you and then a follow-up to the other two witnesses. When we held this hearing a year ago some assessments indicated that in the wake of the United States' withdrawal from Afghanistan al-Qaeda would have the ability to reconstitute itself and threaten the United States homeland within one to two years. Here we are, one year later.

To the extent that you can discuss it in an unclassified setting, what is the National Counterterrorism Center's assessment of al-Qaeda's capability to threaten the U.S. homeland?

Ms. ABIZAID. Thank you very much for the question. Al-Qaeda's capability to threaten the United States homeland from Afghanistan is quite limited, in part thanks to the operation that killed Ayman al-Zawahiri in Kabul here recently, but also because the al-Qaeda elements that are still present in Afghanistan are really not focused on external operations, as far as we can tell.

There are other terrorist elements in Afghanistan that we are concerned about, primarily ISIS's branch there, ISIS Khorasan. But the threat from al-Qaeda should be disaggregated from that, I think given the very unique circumstances around that group, its relationship with the Taliban, and some of the specifics in which it has evolved over the years.

Senator HASSAN. Thank you.

Director Wray and Secretary Mayorkas, do you agree with this assessment, and what are your agencies doing to mitigate the threat? I will start with you, Director Wray.

Mr. WRAY. I would add a couple of things to what Director Abizaid had to say. One is we are obviously very concerned about ISIS–K as one of the threats. Second, I think as time progresses I am concerned that we will have fewer and fewer good sources of information about what al-Qaeda is or is not doing in Afghanistan, so we always have to be mindful of, as Secretary Rumsfeld famously said, "the known unknown" that goes there. Third, we are very concerned about al-Qaeda and ISIS's ability to inspire attacks, even from over there. Those are a few points I would add.

Senator HASSAN. Thank you. Secretary?

Secretary MAYORKAS. Senator, I think the point that my colleagues have made underscores a broader point, which is that we have spoken about the evolving threats, but we should keep in mind that the threats of the past remain the threats of the present. Only new ones have been added. I defer to the experts to my left.

Senator HASSAN. Thank you. Now, Secretary Mayorkas, I want to move on to a different topic. Every week a new drug seizure along the border makes headlines, but the flow of drugs across the Southwest Border is unrelenting. The drugs that DHS seizes accounts for just a fraction of the total that criminal organizations attempt to smuggle into our country.

What specific steps is DHS taking to stem the flow of drugs crossing the border, and what additional resources are you using to address this problem? What additional resources do you need?

Secretary MAYORKAS. Senator, thank you so much. It is a fact that the smugglers seek to transport controlled substances, illegal drugs into the United States, primarily through the ports of entry, through trucks, vehicles, and the like. What we have done is we have surged technological resources that can most effectively defect the effort to smuggle those dangerous substances into our country, specifically, for example, non-intrusive inspection (NII) technology, which has remarkable x-ray capabilities that can be implemented very swiftly.

We have deployed forward operating labs so personnel, scientists, can detect the controlled substances and we can effect the seizure

immediately and refer to law enforcement the persons who have sought to smuggle them.

What we need is more resources like that, and we really hope that Congress passes our fiscal year 2023 budget. We are already six weeks into the new fiscal year without the resources that we need financially to invest in that technology and deploy additional personnel as well.

Senator HASSAN. Thank you. One additional question I think, given my time, to you, Secretary Mayorkas. Over the last few years, cyberattacks have plagued State and local governments and other public entities. Toward that end, as part of the Bipartisan Infrastructure Law, Senator Cornyn and I helped create a Federal grant program for State and local entities to improve their cybersecurity. The application period for the first year of the grant program concluded just this past Tuesday.

I understand that the Department of Homeland Security is still reviewing applications, but can you explain what the Department's goals are for this first year of grants and how you intend to achieve them?

Secretary MAYORKAS. We are so grateful for that grant program. It is a multi-billion-dollar grant program, over several years. This first year of its implementation we are dedicating $185 million in resources to State and local governments. This is all about building their capacity to enhance the security of the cyber ecosystem.

In cybersecurity, Senator, we say we are only as strong as our weakest link, and the fact of the matter is that there are target-rich and resource-poor localities that we need to strengthen, and that is what this grant program is going to enable us to do.

Senator HASSAN. So your goal right now, is making sure that the State and local governments that have applied get the resources they need and really focus on strengthening that level of cybersecurity. Is that fair to say is a priority there?

Secretary MAYORKAS. Yes it is, Senator.

Senator HASSAN. Thank you very much, and thank you, Mr. Chair.

Chairman PETERS. Thank you, Senator Hassan.

Senator Paul, you are recognized for your questions.

OPENING STATEMENT OF SENATOR PAUL

Senator PAUL. Director Wray, is Facebook or any other social media company supplying private messages or data on American users that is not compelled by the government or the FBI?

Mr. WRAY. Not compelled, in other words, not in response to the legal process?

Senator PAUL. No warrant. No subpoena. They are just supplying you information on their users.

Mr. WRAY. I do not believe so, but I cannot sit here and be sure of that, as I sit here.

Senator PAUL. Can you give us a yes or no by going back to your team and asking? Because it is a very specific question, because if they are, it is against the law. The law, the Stored Communications Act, the Electronic Communications Privacy Act of 1986, prohibits providers from sharing electronic communications with any person or entity unless it is compelled. This was done to protect the

privacy of people so we could feel like we can send an email or direct message to people without having that information given over.

It is a very specific question. Will you get with your team of lawyers and give us a specific answer? Because this is the law. If you are doing it, then we need to go to court to prevent you from receiving this information.

Mr. WRAY. I can tell you that I am quite confident we are following the law, but what I will also——

Senator PAUL. that is not the answer.

Mr. WRAY [continuing]. Follow up with you to make sure that we get you more detailed information.

Senator PAUL. Is the FBI obtaining anonymous social media data and then using technical methods to pierce the anonymous nature of the data?

Mr. WRAY. Anonymous social media data?

Senator PAUL. You purchase data. People purchase data all the time, and we sort of tolerate it, for advertisings and things, because it is anonymous data. Are you purchasing what is said to be anonymous data, through the marketplace, and then piercing the anonymous nature to attach individual names to that data?

Mr. WRAY. Right. When you asked about anonymous data I was thinking more in terms of——

Senator PAUL. No. I am talking about data that is out there, and are you purchasing data and then piercing the anonymous nature of that data?

Mr. WRAY. So the manner in which we usually use the term "commercial data"—is probably longer than I could explain here. But again, let me have one of our——

Senator PAUL. You will not answer the question of whether or not you are attaching names to anonymous data.

Mr. WRAY. I think it is a more complicated answer than I can give here.

Senator PAUL. So far we are 0 for 2 with getting you to answer this, but you are pledging you will actually answer the question, because you have to realize the frustration. We will write you a letter and your team of lawyers will write back a 15-page letter that says nothing, and you will not answer the question.

These are very specific. This is whether you are obeying the law, whether we can have confidence. I want to have confidence in the FBI.

Mr. WRAY. We are obeying the law.

Senator PAUL. You are saying that but you will not tell us the answer.

Mr. WRAY. That is not what I said.

Senator PAUL. No, you are not telling me the answer, and the answer is, are you collecting data not compelled by a warrant? That would not be in compliance with the law. But you will not answer that you are not collecting that data.

Mr. WRAY. I said two things. One, we are following the law, and second, that we would have somebody follow up with you with more detailed, specific information.

Senator PAUL. So those are two specific questions. Are you getting data from them that is not compelled, and then are you piercing the anonymous nature of that, technically.

Are you receiving private messages from social media companies through the use of confidential human sources. From Facebook, social media companies. Do you have people working over there who you are paying or who are volunteering to give you information, even though it would be against the law for Facebook to do this, but now you are saying, "We will get around the law by using confidential human sources?"

Mr. WRAY. Just to be clear I am following the question, you mean, in effect, recruiting a human source inside the company?

Senator PAUL. Exactly.

Mr. WRAY. No, I do not believe so. I think we have had situations where we have confidential human sources, not employees of those companies but who report to us on their own communication. If the two of us had a communication, and Secretary Mayorkas was a human source, he could report to us about what he is saying to me.

Senator PAUL. Once again, I would like the answer to be more specific from your team, not that "I do not believe so" but that you are or are not using human confidential resources within Facebook.

We get back to the idea of whether or not you are getting information for them outside the warrant process, because the next question is—which you probably will not answer either—are you taking information that you are getting not through the warrant process and then going around and coming back and using that as a predicate for getting a warrant to actually get the information you have already been given?

Mr. WRAY. I am not sure I am completely following.

Senator PAUL. Basically you get information that Facebook is volunteering. This has all been written up in The Post article. You are familiar with The Post article with the accusations. The question is, are you getting information they are giving to you. They say, "Oh, somebody says January 6th was great. Here is information on this guy." Then you are taking it and then using it as a predicate to say, "Well, now let us go to the court and get a real warrant and get the information we already actually got without a warrant."

Mr. WRAY. We get tips and leads from all over the place, from members of the public, from businesses, from community leaders, from other in-government partner, all the time, and we use the tips and leads that we get to often——

Senator PAUL. Are you getting tips and leads from Facebook and social media companies?

Mr. WRAY. We get tips and leads from companies. Absolutely.

Senator PAUL. That includes private information.

Mr. WRAY. I am not aware of us receiving any tips or leads in a way that——

Senator PAUL. See, here is the point. You may think it is just jolly well to get all this stuff without a warrant, that people volunteer to you, but many of us are alarmed that you are getting this information that are private communications between people, because it is against the law. It is against the law for Facebook or social media companies to give it to you, but it is also against the law for you to receive it.

You are going to have to very specifically go back with your team and search over whether you are doing it or not, and just say, "Oh, probably not. We obey the law. We are good people." Well, no, there

are doubts, because this has been reported. Even the FBI, when you responded to the New York Post article, said that companies are referring information to the FBI with investigative value relating to foreign malign influence.

Now there would probably be a great deal more tolerance about that if it is foreign malign influence, but the question is are you also receiving information on so-called domestic? What would that mean? Is someone questioning whether paper ballots are an accurate way of running election? Is that good enough for you to be getting our private information because we have a political beef with the way votes are counted or recorded in our country? Is that something that you are collecting information on? Are they giving you information on private things that you have told them, "People who question the election, we want to hear about these people," and so they are giving you this information. Are you receiving information like that?

Mr. WRAY. I will give you two classic examples that I think happened with some frequency. One, if we supply information to, say, Facebook or any number of other technology companies about foreign accounts, Russian Intelligence Service, for example, accounts, when they look in their system for those accounts they often find other accounts related to those and they provide tips and leads back to us about those. That is one example.

A second would be a situation where a technology company encounters a threat of violence on their platform, on their services, and they provide tips and leads to us, and we follow up on those.

Senator PAUL. There is really not a lot of disagreement about that. The question is, is when we start to talk about political speech, and that is the question. Are you receiving things that could be interpreted, and we would want to know, and if you are not going to admit to us, whether it is political speech, someone who questions the election, someone who is mad about something that is going on. They are not saying they are directly going to commit violence. They are mad about things.

What the New York Post article said is yes, you are getting this, and then when they are finally read in context—and this is from a whistleblower, which makes us suspect you are not being forthcoming or honest with us—is that whistleblowers are saying you are receiving this information from Facebook and others and that you are going around the Constitution and to come back and try to get warrants for it. But then once you read it there has been no actionable intelligence on this, but this is an active program that you have got.

You work for the government. You should admit to us whether or not you have a program going after our speech.

Chairman PETERS. Thank you, Senator Paul.

Mr. WRAY. We investigate violence, not speech.

Chairman PETERS. Thank you, Senator Paul.

Senator Lankford, you are recognized for your questions.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Mr. Chairman, thank you. Thank you to all three of you and the service that you give to the country on this.

We do have lots of questions, just about process and how things are going on this.

Secretary Mayorkas, you and I have talked about Title 42 for about 18 months, and I have asked you the question, what happens when Title 42 goes away? For 18 months you have said, "We are working on it."

Judge Sullivan just stepped in and unilaterally canceled out Title 42. We are at this very odd situation right now where DHS is in one court, asking to extend Title 42 a little longer, and then another court asking to cancel Title 42 altogether. But we are still waiting to try to figure out what happens now and how many people are about to cross the border.

What is the plan for dealing with this illegal immigration coming now, post Title 42?

Secretary MAYORKAS. Senator, what we requested of Judge Sullivan in the District Court of D.C. was an orderly wind-down period of 35 days, which was unopposed and which was granted by the court.

What we are doing is precisely what we announced we would do in April of this year, and we have indeed been executing on the plan. It is six different lines of effort, and I will review them very quickly, given the limited time.

Surging resources to the Southern Border, including personnel, technology, facilities, capabilities, and transportation, medical support.

Two, increasing our Customs and Border Protection processing efficiency to mitigate potential overcrowding. We have been digitizing, for example, our electronic A-files (Alien files), the immigration files, when individuals are placed in proceedings.

Three, we are enhancing the consequences for unlawful entry, especially with respect to individuals who seek to evade law enforcement, including removal, detention, and criminal prosecution when warranted.

Four, we are seeking to bolster the capacity of nonprofit organizations, State and local officials, and working very closely with them.

Fifth, we are targeting and disrupting the smuggling organizations and transnational criminal organizations. In fact, we have effected more than 5,000 arrests and more than 6,000 disruption events, and that means arrests of individuals, the breakdown of smuggling of stash houses, the seizure of the instrumentalities that these smuggling organizations use.

Sixth, we are working with our partners to the south to deter irregular migration. I spoke earlier in response to Ranking Member Portman's question about the fact that this is a tremendous hemispheric challenge. We are seeing the movement of people, and the demographics of the population that we are encountering at the border has changed dramatically.

Senator LANKFORD. It has, and there are a couple of big challenges in this. One is the numbers just came in for October. It is the third-highest number in recorded history. While those things were implemented, the numbers continue to accelerate. This goes back to the estimates when Title 42 goes away, there was an expectation from intel to be able to say these numbers will surge even

greater. You built a Venezuelan policy on trying to be able to deter Venezuelans, based on title 42. That just went away.

What we are trying to figure out is what is the plan, because the plan you just articulated has led to the third-highest number for any single month in history.

Secretary MAYORKAS. There are few points, if I may, Senator, and thank you. No. 1, the number of encounters is not equal to the number of unique individuals we encounter——

Senator LANKFORD. Correct. Yes, we know that.

Secretary MAYORKAS [continuing]. Because Title 42 creates a potential for the ease of recidivism.

No. 2, we are working with our partners to the south, with Mexico, with respect to the end of Title 42, and whether we will be able to continue our thus-far successful program with respect to Venezuelan nationals, and use our Title 8 authorities.

But we also have other opportunities ahead of us, because as we sought to do earlier, and we will resume this effort, is an enhanced use of expedited removal, which is a Title 8 authority. We are looking at our consequence regimes and how we can most effectively employ them.

Senator LANKFORD. There are a lot of people counting on these numbers coming down, and they are not. They are going up, and they continue to be able to rise. While we are examining these things and looking at it, the numbers continue to rise. With the end of Title 42 coming in 35 days, we expect it is going to accelerate even higher. There is an expectation that your Department is going to change this number dramatically.

Let me ask a point-blank question that is challenging on this. What percentage of the individuals that are encountered at our Southern Border do we know their criminal history from the country they are coming from? I am not talking about if they have an American criminal history or they are on our Terror Watch List, that we know their criminal history of the country they are coming from. Do we know that history?

Secretary MAYORKAS. I will have to get back to you on that, Senator, whether we have the capability of identifying the percentage, which is what you have inquired about.

Senator LANKFORD. It is my understanding that we do not know the criminal history of the vast majority. Can you give me an estimate on this? I am not asking for a 0.8 percent, but give me a guess.

Secretary MAYORKAS. I understand. I am quite hesitant to guess on information that is so important to our mission. But I will certainly get back to you with whatever information we can provide.

Senator LANKFORD. It is incredibly important because I think there is an assumption that the American people feel that the 2 million-plus individuals that were encountered just in the last 12 months have been vetted in some way at our Southern Border or they have been checked. We do not know if these individuals are fleeing poverty or fleeing from the law. We do not know.

Secretary MAYORKAS. Oh, if I may——

Senator LANKFORD. There is a check to see if they have an American criminal history record, but we do not know if they have a criminal history record of where they are coming from.

Secretary MAYORKAS. As my colleagues here will attest as well, Senator, we conduct screening and vetting of individuals whom we encounter. We have a robust screening and vetting process. It actually is recurrent vetting, and it is not just with respect to criminal history in the United States.

Senator LANKFORD. I would like to get in a good guess of how many people we know their criminal history when they come in then.

Secretary MAYORKAS. As I mentioned, Senator, I will get back to you and see if we have that data, and if so, I will certainly provide it to you.

Senator LANKFORD. That would be great. Thank you.

We have asked your team, and you and I have talked about it before, about the information for the Migrant Protection Protocols (MPP) and the decisionmaking process for the Remain in Mexico policy on this. We asked about that for a while. We just recently got a letter back saying that there are no responsive documents that have been withheld. Basically you have everything that we would have. But the implication then is the decisionmaking process of who qualifies for the MPP and who does not was left up to a case-by-case basis, and there are no guidance documents. I find that hard to believe that there were no guidance documents given to anyone on your team anywhere along the border, on how to be able to decide. Yet your team is so far telling me, "Hey, we do not have anything. We never printed anything." I find that exceptionally hard to believe, and I would like to be able to follow up and be able to get access to those documents.

Secretary MAYORKAS. I look forward to discussing that with you because I certainly have some very important points to make in response to your concern.

Senator LANKFORD. Thank you.

Chairman PETERS. Thank you, Senator Lankford.

Senator Scott, you are recognized for your questions.

OPENING STATEMENT OF SENATOR SCOTT

Senator SCOTT. First, Secretary Mayorkas, thanks for your calls around the hurricanes. I have a very positive experience with the Federal Emergency Management Agency (FEMA), so I think you have a great team there, and everybody there does a good job.

Secretary MAYORKAS. Thank you, Senator.

Senator SCOTT. I think the last time, Director Wray, you testified I had the opportunity afterwards to go to West Virginia, and I just want to compliment you on what you have done to revamp the call center operation. I am sure it is still hard to catch everything that goes on out there, but I want to thank you for that.

Secretary Mayorkas, you know that I have been disappointed in the border. It just seems like it is open, with all of this fentanyl coming across. We have people dying.

But here is my question, and I do not know if Secretary Mayorkas or Director Wray, if you want to answer it. It has been reported that the Chinese Communist Party (CCP) are operating police stations in the United States in an effort to surveil Chinese dissidents. It seems obvious the U.S. should not allow its most significant geopolitical rival, an oppressive communist regime, to es-

tablish police stations in the United States what authority or jurisdiction does the CCP have in the United States?

I do not know which one wants to testimony.

Mr. WRAY. Senator, like you I am very concerned about this. We are aware of the existence of these stations. I have to be careful about discussing our specific investigative work, but to me it is outrageous to think that the Chinese police would attempt to set up shop in New York, let us say, without proper coordination. It violates sovereignty and circumvents standards, judicial and law enforcement cooperation processes.

The reason this is so important is because we have seen a clear pattern of the Chinese government, the Chinese Communist Party exporting their repression right here into the United States. We have had now a number of indictments that you may have seen of the Chinese engaging in uncoordinated, quote/unquote, "law enforcement" action right here in the United States—harassing, stalking, surveilling, blackmailing people who they just do not like or who disagree with the Xi regime.

It is a real problem and it is something that we are talking with our foreign partners about as well, because we are not the only country where this has occurred.

Senator SCOTT. They do not have any right to be here?

Mr. WRAY. We are looking into the legal parameters of it. I want to be a little bit careful not to get out over my skis on that. But suffice it to say, I can tell you from an FBI director perspective, I am deeply concerned about this, and I am not just going to let it lie.

Senator SCOTT. Secretary, does it impact homeland security at all?

Secretary MAYORKAS. Of course. The threat of China is one of the most significant threats that we face in the homeland. It is not only a matter of national security, it is a matter of homeland security, in a number of arrays, in a number of areas of our mission.

Senator SCOTT. Do you think you have the ability to shut them down? Do you know if you have the right to shut them down?

Secretary MAYORKAS. I would have to defer to the Department of Justice with respect to that.

Senator SCOTT. It would go to Justice, not Homeland Security? OK. So it would be under FBI?

Mr. WRAY. Well, or to the extent that the remedies might be some part of the Justice Department, outside of the FBI, that could also be a possibility. Then there may be a State Department dimension to this that we are looking into.

Senator SCOTT. When you know they are here, do you know if they are surveilling U.S. citizens? Do you know that yet? Do you have enough information to know if they are?

Mr. WRAY. Again, I do not want to get too far into our ongoing investigative work, but as I said, we have seen plenty of situations, plenty of situations in the past, where the Chinese government, under the pretext of going after corruption, have essentially used that as vehicle to surveil. We have had situations where they have planted bugs inside Americans' cars, for example.

One of the things that we are seeing more and more is them hiring private investigators here in the United States to essentially be their agents, if you will, to conduct some of this work.

This is something we are trying to call out, and it is important the Chinese Americans and Chinese dissidents who are here know to call the FBI to report when they think they may have been targeted with this conduct.

Senator SCOTT. Because you probably cannot talk about it in here. I would like to get a classified briefing on what they are doing, at some point, whenever it works out for you.

Mr. WRAY. We would be happy to set that up.

Senator SCOTT. Director Wray, I am going to ask you and you can tell me if it is accurate or not. I am not suggesting all of this is accurate. But it appears that DOJ have become politicized with regard to pro-life things. There is a recent rise in high-profile FBI investigations of pro-life Americans, which raises the concern that the FBI is weaponizing Federal law enforcement as becoming a partisan tool, which I do not think, when we have talked, that has been your goal.

There appears to be investigations that arrest the pro-life community, and it is just the opposite of what has happened. We have had numerous firebombings, violent attacks, acts of vandalism against churches, pro-life organizations, and crisis pregnancy centers in the days and weeks following the Dobbs decision.

Is this right? Is that happening? Not happening?

Mr. WRAY. First let me say I firmly believe that the FBI is going about its work, doing the right thing in the right way. Now, I am glad you raised this topic because it gives me an opportunity to speak to it.

My view, plainly expressed to all of our people, including in the context of abortion-related violence, is that I do not care what side of the issue you are on, you do not get to engage in violence, and we are equal opportunity when it comes to that.

Now we have quite a number of investigations, as we speak, into attacks or threats against pregnancy resource centers, faith-based organizations, and other pro-life organizations. You might be interested to know that since the Dobbs Act decision probably in the neighborhood of 70 percent of our abortion-related violence cases or threats cases are cases of violence or threats against pro-life, so where the victims are pro-life organizations. We are going after that through our Joint Terrorism Task Forces, through our criminal authorities, and things like that. We have about 20 field offices involved in this.

We take it very seriously, and again, I do not care whether you are motivated by pro-life views or pro-choice views, you do not get to use violence to express it.

Senator SCOTT. We have talked about this before. It just seems to me that in DOJ, and FBI in particular, they might be doing the right thing, but you guys allow information to go out, not talking about what you are doing. Because if you read the press you would think that you guys are only going after pro-life groups and not going after groups that attack pro-life.

I have never understood this about the FBI and DOJ, in that you guys are not more proactive about what you are actually doing. Be-

cause I am pro law enforcement, as you know, but I cannot defend you with no information.

Mr. WRAY. Senator, we do not have the time for me to tell you how frustrated I sometimes get by some of the news reporting about our work and the misreporting about our work. The circumspection that we display with regard to discussing our investigations is based on rules and practices that are important to people having confidence in the integrity of our work, and go back decades, in multiple administrations. Sometimes it can be very frustrating to agents on the ground when they see things being misreported about their work.

But we have all been taught that we have to bite our lips and let the facts come out in the right way, through court proceedings, and sometimes that can be very frustrating, to us and it sounds like to you too.

Senator SCOTT. It makes it harder for me. It makes it hard for us, right, because people come to us and say, "Oh yes, they must have done that." So thank you.

Chairman PETERS. Thank you, Senator Scott.

We will have a second round.

Senator Hawley has deferred to Senator Romney. Senator Romney, you are recognized for your questions.

OPENING STATEMENT OF SENATOR ROMNEY

Senator ROMNEY. Thank you, Mr. Chairman. Thank you, Senator Hawley. I appreciate the chance to be able to ask a few questions.

Director Wray, I begin by saying how much I appreciate the work of your agents and how much I respect them, and I am convinced of their quality. One of my sons, years ago, interviewed to become a member of the FBI. He was turned down. He was able to go on and get a degree at Harvard Business School and has done quite well. He survived. But we learned from that experience that the qualifications for getting into the FBI are high, indeed, as they should be, and I have great respect for the men and women who work for the FBI.

There is a great deal of discussion about the political orientation of the FBI. My experience with your organization is that that is not the case, by and large. I am sure there are individuals among the 38,000 who work with you who have political points of view, may leak things, and may do things from time to time that are not appropriate, and I hope that you are able to evaluate them and evaluate where those come from and correct them.

Can you give us a sense of how the resources the FBI are directed, how much goes into looking at violent crimes of various kinds and human trafficking? How much goes into terrorist-related prevention? Are there categories of effort that are carried out? Because I think there is a public perception that the whole FBI, we ought to defund it because it is only doing political work. What is the FBI doing? Where are the resources devoted?

Mr. WRAY. If you were to look at our allocation of resources, and I cannot give you the numbers off the top of my head, but if you were to look at the allocation of our resources you would see that the single largest chunk is devoted to traditional criminal programs, and of which the violent crime is by far and away the big-

gest. We have Safe Streets Task Forces all over the country. We have Transnational Organized Crime Task Forces all over the country. We have Violent Crimes Against Children Task Forces. So those remain our bread and butter. Those remain our biggest programs.

We do have unique responsibility for national security threats as well. If you were to look at our strategy you might see the national security threats listed first because those are places where if we do not do it, no one will, whereas violent crimes, crimes against children, we work much more shoulder-to-shoulder with our State and local law enforcement partners. A lot of times those national security threats—terrorism, counterintelligence work, cybercrime—get most of the, to Senator Scott's point, the media attention. But day in, day out, the FBI that most Americans, and certainly most law enforcement professionals—and I talk to chiefs and sheriffs every week—the FBI they experience most is really more focused on the traditional criminal stuff.

Senator ROMNEY. Yes, thank you. You have spoken a great deal about the cyberattacks from State actors, from China, as well as non-state actors. Secretary Mayorkas has spoken about that as well. I do not know that it is possible, through a process of defending against attacks, to prevent all the potential attacks and all the theft that will come from our businesses and into our government.

It strikes me that the only effective way to stop the attacks that come, of a cyber nature, is to attack back, that the best defense is a good offense. I know your respective organizations are not responsible for the offensive of this, but to get China to stop attacking, they have all these private enterprises that are doing these attacks into our systems. Fighting against all these things will never stop it unless China recognizes that if they do not stop it that they are going to be hurt more than we are.

Do you believe we have a sufficient effort, an offensive effort, to push back against the cyberattacks that come from State and non-state actors, and should we expand on that, and where should that reside? I will ask both Director Wray as well as Secretary Mayorkas and Director Abizaid to respond.

Mr. WRAY. Certainly when it comes to offense, offense is a critical part of our overall effort to push back against cyber adversaries, in addition to some of the offensive cyber operations that we probably could not talk about in this kind of a setting.

There is actually a lot of progress being made in what I obliquely referred to earlier as joint sequenced operations, where we, with our intelligence community partners, law enforcement partners, foreign partners—go with the whole "2 plus 2 to make 5" kind of effect. We are going after the adversaries' infrastructure, we are going after their cryptocurrency, we are going after the individual actors. Some of them we can extradite. Some of them we can have charged there. We are engaging in other sort of more sensitive counterintelligence type work to amplify those effects.

But what we have found is that when we go after the actors, the infrastructure, and the money all simultaneously we can degrade and disrupt their effectiveness. That is, I think, ultimately the real goal is to degrade, disrupt, and defend in that way. In some ways the deterrence model is harder, much the same way, we are not

going to deter the Chinese or the Russians from spying but we can make it hellishly difficult for them to do it. That is what we are after now, is imposing risks and consequences on the adversaries, to hit them where it hurts, to make it harder and harder for them to really come after us with cyber means.

Secretary MAYORKAS. If I may, Senator, add a point. Of course, I do not need to speak of the criticality of a strong defense, and you are, of course, focused on offensive behavior.

A few weeks ago I was in Singapore to speak to our allies in the Indo-Pacific region about the importance, or I should say the peril of having China own or operate other nations' critical infrastructure and the perils it presents from a cybersecurity and other security perspectives. It was a very important dialog, not only with our Singaporean partners, our Japanese partners, but other countries in the region because China is very aggressive in seeking to own or operate the infrastructure in telecommunications and other technologies.

Senator ROMNEY. Thank you. Director.

Ms. ABIZAID. Senator, I would just say I will defer to my colleagues on the cyber-specific piece of your question, but what I would say from a counterterrorism community perspective, there is so much that we have learned as a collaborative community about both offense and defense at the same time. Those lessons learned applied to things like transnational organized crime or cyber threats I think really position us well as a government to take it to the threat actors.

Senator ROMNEY. Thank you. Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Romney.

Senator Hawley, you are recognized for your questions.

OPENING STATEMENT OF SENATOR HAWLEY

Senator HAWLEY. Thank you very much, Mr. Chairman. Thanks to the witnesses for being here.

Director Wray, let me start with you if I could. I think the last time that I got to visit with you was back in August. On August 4th of this year you were at the Senate Judiciary Committee. You remember that, I assume.

We had to cut that hearing short. We were supposed to do two rounds of questions. You said you had to be somewhere so we cut it short. Republicans were not able to ask a second round as we had been informed we would.

The press reported shortly thereafter that the reason that the hearing had to be cut short is because you were flying on a Gulfstream jet for a personal vacation in the Adirondacks. Please tell me that is not accurate.

Mr. WRAY. Senator, the hearing was not cut short from my experience. We had agreed beforehand on the time and length of it, and I was very surprised to find that anyone on the Committee was surprised as to how I fly. I am required, not only permitted but required to fly on an FBI plane wherever I go.

Senator HAWLEY. So you were going on vacation?

Mr. WRAY. I was, yes.

Senator HAWLEY. You left a statutorily required oversight hearing in order to go on a personal vacation in the Adirondacks.

Mr. WRAY. I took a flight to go visit my family, as had been previously arranged in conjunction——

Senator HAWLEY. No.

Mr. WRAY [continuing]. With the leadership of the Committee.

Senator HAWLEY. The Ranking Member, Chuck Grassley, asked you during the hearing. He said, "I assume you must have other business." You said, "Yes." He then said, "If you have a business trip, you have your own plan. Can't it wait a while." He then said, Chuck Grassley, "We only just heard half an hour ago that now you have to leave. We were going to have a seven minute round followed by a three minute round. I have seven people on my side of the aisle"—that included me—"who are waiting for this additional round. Is there any reason we cannot accommodate them for 21 minutes?" You said you had a plane to catch. You had somewhere to go. Now we find out it was for vacation?

Mr. WRAY. The reference to other business was not a reference to that day. It was a reference to the following week where Senator Grassley and I were going to see each other in Iowa, when I had other business in Iowa, and I did in fact see him then.

Senator HAWLEY. So wait. You had to leave the hearing early because you were going to see him later in Iowa, in a week?

Mr. WRAY. No. I had to leave when I said I was going to have to leave, as had been previously organized with the leadership of the Committee.

Senator HAWLEY. You left an oversight hearing before the Senate Judiciary Committee, required by statute, so you could vacation with your family. I find that absolutely unbelievable, and frankly, indefensible.

Now is it your practice to use government planes? You say you do this all the time. You flew in a Gulfstream 550, I think, that was originally purchased for counterterrorism purposes. You were using it to go to, what is it, Saranac Lake? Is that how I say it? I have never been there. Is that the right pronunciation, Saranac Lake? That was your destination?

Mr. WRAY. Yes.

Senator HAWLEY. Did you enjoy the flight? I mean, did you pay for it?

Mr. WRAY. Yes, I paid for it.

Senator HAWLEY. Will you turn over all receipts and reimbursement to this Committee?

Mr. WRAY. Senator, we will be happy to comply with oversight requests related to the use of the plane. As I said, it is important for people to understand——

Senator HAWLEY. Why do you not just give me a yes. Will you turn over the receipts——

Mr. WRAY. I will turn over the information——

Senator HAWLEY [continuing]. For this flight to the Committee?

Mr. WRAY [continuing]. Related to my use of the plane. The use of the plane, I am required, not just permitted, required, even for personal travel, to use the FBI plane.

Senator HAWLEY. How convenient for you.

Mr. WRAY. I pay every single time that I use the plane for personal reasons.

Senator HAWLEY. I am glad it is available for you to jet away from your statutorily required hearings and oversight before this Congress, where you denied the ability of Members of Congress to ask you questions because you had to go on a personal vacation using a government plane.

Let us just look at some of the things, while you have been vacationing, that your FBI has been doing. According to numerous whistleblowers who have come forward to members of this body, to members of the House, the FBI has been sending more than, in one instance, a dozen armed agents to a rural Pennsylvania home of a Catholic pro-life demonstrator to arrest him at gunpoint in front of his children in the early morning hours, despite the fact that he posed no risk of violence or threat and had previously offered to turn himself in.

Numerous whistleblowers, field agents, have alleged that D.C., your headquarters, has pulled them off working on child sex abuse cases, working on human trafficking cases, in order to work on January 6th matters for this reason, to give the appearance, they say, that there are hundreds of new domestic terrorism cases in the country when in fact there are not.

Whistleblowers, field agents, have also said that D.C. has ordered the use of special weapons and tactics (SWAT) teams on nonviolent suspects who may have attended a January 6th rally, and they have been ordered to conduct surveillance and knock on doors of people who were not even in D.C. on January 6th. Again, all of this, according to the whistleblowers—these are your agents—all of this in order to make it look as if there is a mass surge in domestic terrorism all across the country when, in fact, the stats are being padded by political directive in your office.

They also say, these whistleblowers, the D.C. leadership deliberately suppressed investigations into Hunter Biden, contrary to FBI procedure, and have also retaliated against FBI agents and whistleblowers who have contacted Congress, which, by the way, they are protected by statute to do so.

This is what is happening at your FBI while you are evading oversight hearings. Mr. Director, do you think you are still up to this job?

Mr. WRAY. I absolutely think I am still up to this job, and I think our workforce feels the same way.

Senator HAWLEY. I do not, and frankly, I think you should have been gone a long time ago. Given your behavior recently, I think it only makes it more clear.

Are there any travel plans today that we should be aware of that you have? We are supposed to have a second round. Will you be here for that?

Mr. WRAY. Yes.

Senator HAWLEY. Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Hawley.

Senator Rosen, you are recognized for your questions.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you all for being here today. I appreciate it.

I wanted to thank DHS, before I get started with my questions, for extending Temporary Protected Status (TPS) to several countries last week. It is going to provide critical relief to thousands of families in Nevada. Those families appreciate that very much.

We do know that Congress must take action to enact immigration reform that both secures our borders and provides a path to citizenship for TPS recipients, dreamers, and others, but as we work toward this goal I do appreciate, and the families in Nevada appreciate your consideration.

I am going to turn now to the topic of the hearing, threats to the homeland. Difficult subject, again, like all things here, but rising antisemitism. Every day, in every way we see more and more attacks, outbreaks of antisemitism here in the United States. The recorded incidents nationwide, I believe they are at an all-time high. Not a day goes by without another report of an antisemitic hate crime or prominent individuals inciting anti-Jewish conspiracy theories.

With Jewish communities around the world facing increasing discrimination as well as threats and acts of violence, a whole-of-government approach is needed to effectively address antisemitism.

Because many individual agencies play a critical role in combating antisemitism, we need closer interagency coordination to share best practices, share that ever-important data that keeps us safer when we share it, that intelligence, the same thing, identify gaps in our efforts between agencies, and streamline overlapping activities and roles so that we can best combat antisemitism where we see it, and I believe execute a unified national strategy.

Secretary Mayorkas, how is DHS coordinating with other Federal agencies in the fight against antisemitism? Would you support the development of a national strategy that uses a whole-of-government approach, cohesive, comprehensive approach to address this rising threat for all of us?

Secretary MAYORKAS. Senator Rosen, thank you. I think Director Wray spoke very powerfully, but a couple of weeks ago, I believe it was in New York City, about the rise in antisemitism. Of course, where we become involved in the Department of Homeland Security is the connectivity between an ideology of hate, regardless of the ideology in particular, and violence.

That is where we become involved. We are working very closely with the FBI and our Federal, State, local, tribal, territorial (SLTT) campus law enforcement partners to address violence, an increasing level of violence borne of ideologies of hate, and quite clearly antisemitism is one of the rising ones, and it was at a high level to begin with.

We are very grateful for your and this Committee's support of the Nonprofit Security Grant Program (NSGP). We are seeking, in the fiscal year 2023 budget, an increase from $250 to $360 million. That assists religious institutions, faith-based institutions, and other nonprofit organizations to really raise their level of security in response to increasing violence borne of hate.

The FBI and the Department of Homeland Security have published an unprecedented number of alerts and bulletins to our local State law enforcement personnel about an increasing threat level borne of ideologies of hate.

Senator ROSEN. So you would support a national strategy to combat antisemitism?

Secretary MAYORKAS. I would.

Senator ROSEN. Thank you.

Director Wray, I want to move over to you because I know that the FBI, as you have stated, found antisemitic hate crimes rose by six percent in 2020. It represents the highest total in 12 years. It constitutes 60 percent of all incidents based on religion. In your estimation, your research, data, what it is telling you, what is driving this alarming trend? How is the FBI working with communities, State and local law enforcement, again to be sure we are coordinating? Would you support a national strategy to combat antisemitism?

Mr. WRAY. Taking the last part first, certainly I would support a national strategy. Second, the percentage is even worse than you summarized it. I think it is 63 percent of all religiously motivated violent extremism incidents are motivated by antisemitism, and that is against a population that is only 2.4, I think, percent of the American public. So it is pretty stark.

From our perspective we see the Jewish community getting it from all sides, which may contribute to what is driving it. Because not only have they long been a target of foreign terrorist organizations, and we have disrupted attacks by foreign terrorist organizations and foreign-inspired violent extremists against synagogues, for example, but then in addition to that they are, of course, the target of domestic violent extremists. As you may remember, we disrupted an attempt to blow up a synagogue in the Las Vegas area just a couple of years ago, for example.

Senator ROSEN. Yes, thank you.

Mr. WRAY. We are trying to tackle it both through the domestic terrorism lens, through our Joint Terrorism Task Forces, and through the hate crime lens, through our civil rights program. We created a Domestic Terrorism Hate Crimes Fusion Cell which brings those two things together to ensure that we are pushing out information to our partners, whether it is at DHS or State and local law enforcement, or the community, and particularly the Jewish community, to be better able to anticipate what might be coming and prevent attacks.

Senator ROSEN. That is good, and it really goes to my next question because we do believe that hate crimes are vastly underreported because of fear sometimes, right? Since the enactment of the COVID–19 Hate Crimes Act last year, do you feel that there has been an improvement in local and State law enforcement reporting hate crimes to the FBI, and just reporting in general, or how has that been helping us?

Mr. WRAY. Two things. One, I think overall reporting of hate crimes has gone up, and frankly, the Jewish community has been ahead of other communities that are victims in reporting, historically. We have been trying to preach the importance of reporting, and we have seen reporting coming up.

The only caveat I would put on that is that we are in the midst of a multiyear transition to a different crime statistics reporting mechanism, that has been anticipated for about a decade, I think. This particular year the number may be somewhat flawed or

underreported in terms of the recordkeeping, just because of the transition that some police departments are making over from the old system to the new system.

But I would expect as we go forward next year and beyond it will get back to being more comprehensive, and I fully expect it to show exactly what you are saying, which is that hate crimes are on the rise.

Senator ROSEN. The analyst in me hopes that everyone who is converting to this is all using the same algorithm so we have good reports.

Thank you so much for being here.

Chairman PETERS. Thank you, Senator Rosen.

Senator Sinema, you are recognized for your questions.

OPENING STATEMENT OF SENATOR SINEMA

Senator SINEMA. Thank you, Mr. Chair. Before I begin I want to express my sorrow with the news from Puerto Rico today. Air and Marine Operations (AMO) agents perform a very dangerous job with honor and integrity, and my thoughts are with our injured agents and their families, the family of the deceased agent, and all of Air and Marine Operations. News like this today underscores why our work and our oversight is so important, and we owe it to our agents and our officers to do our part to secure the border and keep our communities safe.

Thank you, Mr. Chairman, for holding this hearing, and thank you to our witnesses for being here today.

Fiscal year 2022 saw a record number of encounters at our Southwest Border, over 2.3 million individuals. While just under half of these migrants were removed under Title 42 authorities, the current system had multiple points of failure throughout the summer. In Arizona, local governments were forced to step in to provide emergency support to avoid street release and have reassigned staff from other important roles to help manage the release of migrants from CBP custody.

Border areas outside of Arizona have seen significant street releases, some coming in recent weeks. These releases directly onto city streets are inhumane and leave migrants vulnerable to the elements and bad actors intent on preying upon the most vulnerable.

The Administration's continued failures on the border places Arizona communities and our nation's security at risk. The ongoing influx of migrants puts serious strain on our CBP resources, and it forces our Border Patrol agents out of the field and into processing and administrative roles.

With the sudden announcement that Title 42 will be terminated in December, I am extremely worried that DHS is not ready and that border communities and migrants will suffer the costs for this lack of preparation. It is obvious that the current strategy being implemented at our Southwest Border is not working and that change is necessary.

Secretary Mayorkas, thank you for being here today. These current levels of migration are unprecedented. Following the D.C. Circuit's recent ruling regarding Title 42, Arizonans are concerned that we will soon see these numbers surge even higher, and we need to send a clear message to potential migrants that we will be

fair and humane, but we will secure our border and enforce our laws.

Given the recent developments regarding Title 42, do you have a plan to ensure that those who enter without inspection are facing swifter and more certain consequences?

Secretary MAYORKAS. We do, Senator, and at the outset thank you very much for recognizing the tragedy that our Air and Marine Operations personnel within CBP suffered off the coast of Puerto Rico, and we pray for the family of the officer who lost his life and we pray for the swift recovery of those who have been injured.

We do. We do have a plan, and I think there are a number of examples. One is how we have approached the increased number of encounters of Venezuelan nationals, by building a lawful pathway for them to arrive in a safely and orderly way in the United States, should they qualify and should they pass through our screening and vetting, and to deliver a consequence regime should they not avail themselves of that lawful pathway.

The asylum rule that we have promulgated is a way of taking a broken asylum system, and we are grateful for your bipartisan work with Senator Cornyn in your proposed bill, as a starting point to fix a broken asylum system. But we promulgated a regulation in the absence of much-needed legislation to fix the system, which takes a six-to eight-year asylum period, which is just unmanageable, and reduces it potentially to under a year, which is going to change the migratory patterns of individuals seeking asylum in this country.

Also with respect to the fact that you mentioned that Border Patrol agents have not been out in the field, we have actually surged resources to the Southern Border, not only from different parts of our department but contract personnel, an incredible number of contract personnel, so that we can get those agents out in the field, doing what they swore to uphold, which is the detection and interdiction of individuals, to enhance their swift removal should they not qualify for relief, and their ability to remain in the United States should the law so permit.

Senator SINEMA. Thank you. Secretary, according to data from the Executive Office for Immigration Review (EOIR), in fiscal year 2022, over 20 percent of initial cases were completed with an in absentia removal order. While that is a steep decline from the 50 percent mark that we reached in fiscal year 2022, that number is still far too high.

In order for our immigration system to function we must ensure that individuals who refuse to comply with our immigration laws and are ordered removed from the United States actually experience that enhanced consequence regime. How is DHS planning to ensure that people who willfully defy our immigration process are promptly removed from the country?

Secretary MAYORKAS. Senator, I would say two things. No. 1, the data evidence is quite powerful, that individuals who are represented by counsel have a much higher appearance rate in the immigration enforcement proceedings that we commence. The immigration system is extraordinarily complex, and we are dealing with vulnerable populations without counsel.

No. 2, we have expanded our alternatives to detention and technologized our ability to keep track of individuals, not just by the rather primitive ankle bracelets but by a phone system that does not allow people to make calls. It is not a phone inoperable in that sense, but actually enables us to keep track and make sure that they are checking in with us.

The expansion of the alternatives to detention is an effort that we have very well underway.

Senator SINEMA. My Bipartisan Border Solutions Act, which you just referenced and of course highlighted in our budget hearing earlier this year, creates regional processing centers across the United States. These centers would co-locate offices and agencies that play a role in the asylum process which would enhance the processing of migrants seeking asylum to the United States. I believe that these centers are key to any reforms intended to limit the strain currently placed on DHS.

As introduced, the text placed Border Patrol in charge of detention, but this year, as noted earlier, we have seen additional agents being pulled out of the field due to processing needs, which has limited some of the operational control.

Which DHS component would be best suited to take over the responsibility of those processing centers?

Secretary MAYORKAS. Senator, your bipartisan bill with Senator Cornyn is a very important start to fix a broken asylum system. I would want to study actually which personnel would be best suited. Our goal is to make sure that our Border Patrol agents are out in the field, doing the work that they signed up to do, and that, frankly, they are funded to do.

We have made tremendous strides in getting them out in the field. This is a problem that arose last year, given the increase in the number of encounters. We really have made tremendous strides, and I could provide specific data.

But with respect to your detailed question, I would want to study the profile of the individuals that should maintain the custody of migrants encountered and placed in those processing centers at the border.

Senator SINEMA. Mr. Chairman, I know that my time has expired. May I ask one quick follow-up question?

Chairman PETERS. We do have a second round, but be real quick.

Senator SINEMA. Thanks. I have heard concerns that some of the timelines in the bill that Cornyn and I introduced may be too restrictive. So now that you have had some time to implement the asylum processing rule we would like to get your feedback on what a more feasible timeline would be in which credible fear interviews could be performed.

Secretary MAYORKAS. We would be pleased to provide that.

Senator SINEMA. Thank you. Thank you, Mr. Chair.

Chairman PETERS. Thank you, Senator Sinema.

We have, for our witnesses, we have one, perhaps two Senators to finish up the first round. Then we will take a five-minute break to let you stretch your legs a little bit, and then we will be back for the second round.

Senator Padilla, you are recognized for your questions.

OPENING STATEMENT OF SENATOR PADILLA

Senator PADILLA. Thank you, Mr. Chair. Thank you all for being here today.

The first question is going to be for Secretary Mayorkas. As you recall, Mr. Secretary, last year I expressed significant concerns about the critical incident teams with Customs and Border Protection and their involvement with internal investigations of CBP agents. These units, as we understand, have operated since 1987, but their investigations were never authorized because they are not legitimate Federal criminal investigators and their actions seem to shield CBP agents from liability.

I was pleased to hear that Commissioner Magnus issued a directive to end the use of critical incident teams by the end of the fiscal year, prior to his resignation. However, the existence of such an entity for over three decades is disturbing and undermines the transparency needed with the nation's largest law enforcement agency.

I hope you share my concerns regarding the need to protect the integrity of DHS and all its components. Do you agree that there is no place for shadow police units within Customs and Border Patrol, and can you speak to any of the efforts that the Department has taken to ensure that entities similar to the critical incident teams are not reestablished?

Secretary MAYORKAS. Senator, there is no place for a shadow investigative authority in any part of the Department or any part of the government, and what we have done is actually commenced a wholesale review, department-wide, of our investigative discipline and accountability processes.

Senator PADILLA. How is the status of the termination or phase-out?

Secretary MAYORKAS. I will check and get back to you with respect to the status of their termination.

Senator PADILLA. Please do.

Next question is both for you and Director Wray. Earlier this year, the Department released a report that detailed the need for improvements to information sharing as a means to addressing violent extremist activity. Mr. Secretary, I was pleased to see that your agency planned to develop a central case management system, an information-sharing mechanism for investigating allegations.

Can you provide an update on where DHS is with these developments and whether there have been any significant roadblocks?

Secretary MAYORKAS. Senator, I am not aware of any significant roadblocks, and in partnership with the Federal Bureau of Investigation we have promulgated more products, more information-sharing products than I can remember for the Department of Homeland Security in the many years that I have been there.

The National Terrorism Advisory System (NTAS) Bulletin, other less formal bulletins and alerts to our State and local, tribal, territorial campus partners. We have really built a very cohesive operation in disseminating threat information throughout the country, to really ensure that our local communities are aware of the threat information and law enforcement is able to prevent it, to the best of its capabilities.

Senator PADILLA. Director Wray, the Department of Justice similarly responded to President Biden's National Strategy for Coun-

tering Domestic Terrorism by highlighting the changes it would make to improve information-sharing with State, local, tribal, and territorial partners as well. What specific changes have been made at the FBI to eliminate any gaps in information-sharing?

Mr. WRAY. I think we engage in information-sharing on this with State and local partners in two principal ways, the biggest one being through our Joint Terrorism Task Forces, where we have lots of State and local law enforcement agencies as task force officers on those task forces. One of the things that we have done over the last little while now is improve the amount of training that we provide to participants on those task forces and to State and local agencies, more broadly, about indicators of violence, indicators of mobilization to violence, symbology, iconography, things like that, to put them in a better position to be the eyes and ears that we need them to be and then have information flow kind of in a virtual cycle back with us. That would be one of the things that I mentioned.

Obviously the bulletins that Secretary Mayorkas referenced is a product of great work between the FBI and the Department of Homeland Security to share information, and including with the Fusion Centers, which is a very important piece of the information-sharing infrastructure, if you will, that exists in this country.

Senator PADILLA. In that spirit, a couple of the most critical areas in which to apply improved information-sharing is when it comes to combating gun violence and domestic terrorism.

According to a joint report issued in May of last year, the FBI and DHS determined that the greatest domestic terrorism threat is posed by lone offenders who are radicalized online, and who look to attack soft targets with easily accessible weapons. Sadly, we have seen too many instances, even since Highland Park, Uvalde, Buffalo, and even in my home State of California at the Geneva Presbyterian Church. The common threat here in each case was the ease with which the perpetrator acquired a weapon.

Can you detail what steps are being taken by the bureau to ensure that threats to our schools and places of worship and other important places are identified and neutralized?

Mr. WRAY. I guess there are a number of things that we do on that front. When it comes schools specifically we have been engaged in a very proactive outreach campaign to schools. We have done active shooter training, for example, at schools. Lots of our field offices meet with school officials in their areas of responsibility to help them identify better what to be on the lookout for.

Because one of the things that we have learned in studying this issue over time, when it comes to school shootings, for example, is that there is almost always somebody—a classmate, a teacher, a family member, someone—who saw the transformation in the person, and that if they had known to speak up, known to report, it might have been preventable. In those instances where we have successfully prevented a school shooting, for example, those often do not get reported. But there are any number in which we have successfully prevent, have almost always been because somebody in that situation did report. We are trying to get the word out that way.

Obviously, our National Instant Criminal Background Check System (NICS), which does the background checks, to ensure the people who are legally prohibited from having firearms do not get them, is very active processing background checks. Of course, with the recently passed legislation there will be additional steps we are taking to implement that.

Senator PADILLA. Thank you very much. Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Padilla.

Senator Ossoff, you are recognized for your questions, and after these questions we will take a five-minute break.

OPENING STATEMENT OF SENATOR OSSOFF

Senator OSSOFF. Thank you, Mr. Chairman, and thank you to our panelists for your service to the country and the national defense, the defense of public safety.

Director Wray, always a pleasure to see a fellow Georgian, and thank you for your continued service as well. Each time we have engaged in a setting like this one I have asked you to assess the drivers of elevated levels of violent crime, in Georgia and nationwide.

According to FBI data, violent crime did increase from 2020 to 2021. Could you please provide the Committee with an updated assessment of what is driving this dynamic?

Mr. WRAY. There are a lot of things driving the violent crime crisis that is occurring in this country, in Georgia and elsewhere. There are a few things. First I would say the traditional drivers are all there—drugs, illegal gun trafficking, gangs, socioeconomic factors. Those are all still present.

But in addition to that we are seeing—and I hear this from chiefs and sheriffs all the time as well as from our own agents—an alarming uptick in the incidence of juveniles engaging in violence, often graduating from carjackings to even worse violence. That is a real challenge for the legal system because we are not set up to very effectively deal with crimes committed by minors.

We are also seeing, not everywhere but in an awful lot of places, we are seeing way too many dangerous offenders getting back out on the streets. The only thing more frustrating to the hard-working men and women of law enforcement than having to arrest somebody who should have been behind bars is having to arrest the same person over and over again. That is a product of any number of things. It could be backlogs. It could be certain prosecution practices, certain kind of bail practices. Of course, the juvenile issue that I mentioned.

So those are some of the things that are driving it. In Georgia in particular, pretty much every week I feel like our Atlanta field office is engaging in some kind of operation where they are seizing drugs, guns, cash, whether it is meth, whether it is fentanyl. And so they are experiencing a lot of the same things that we are seeing nationally. Certainly neighborhood gangs are a big phenomenon in our home State.

We are also seeing two other things that have a little bit of a Georgia wrinkle to it. One is juveniles who post-COVID have not returned to school, and so that may contribute to the juvenile ef-

fect. And we are seeing violent criminals who are either detained or imprisoned because they are serving a sentence who still have access to their cellular phones and are able to continue to participate in the activity, despite best efforts by the corrections officials, to continue to participate in the violent activity.

Those are some of the things. I guess one last one, an alarming phenomenon of switches which convert otherwise lawful weapons into fully automatic, and that, of course, increases the violent potential.

Senator OSSOFF. Thank you, Director Wray. You have a new Special Agent in Charge (SAC) in that Atlanta office, and I welcomed her upon her arrival, and I wish her and her team the best.

What can the FBI continue to do, and what more can you do to help protect communities in Georgia who are fearful, who are fearful that they may face carjacking or mugging or aggravated assault out on the sidewalk or at a shopping mall? What are you doing and what more can you do, and will you continue to work with local law enforcement in Georgia to crack down on the violent crime that is preying on innocent citizens?

Mr. WRAY. Violent crime is a major priority for the FBI. As I think I said in response to an earlier question, it still continues to be the place where we have the most single allocation of resources in terms of personnel. We have Safe Streets Task Forces that focus on sort of the gang violence. We have other kinds of violent crime task forces, all of which allow us to bring together what the FBI has to bear with State and local partners who participate on those task forces.

We do active shooter training and things like that to help the community better protect itself. Our lab, close to half of the work that they do, from a forensic side, is in support of violent crime cases often for our State and local partners. Senator Scott and I had a conversation about the tip line that we have in West Virginia, where we prioritize getting threats to life out to State and local partners on the violent crime side.

There is a whole host of things that we are doing, but this remains top of mind for me and for my team. When I am talking to chiefs and sheriffs this is always the first topic we talk about and the last topic we talk about, because it is so much on everyone's mind.

Senator OSSOFF. Thank you, Director.

Mr. Secretary, thank you for joining us. Could you please assess the most significant threats to port infrastructure in the United States? Of course we have, in Georgia, the Port of Savannah. It is the fourth-busiest deepwater port in the country.

Secretary MAYORKAS. With respect to the infrastructure itself?

Senator OSSOFF. To ports.

Secretary MAYORKAS. To ports? One of the concerns that we have is, of course, the cybersecurity threat to ports. We are increasing the level of technology by which our ports operate, and that is why not only does Customs and Border Protection have a focus on cybersecurity but so do does the United States Coast Guard (USCG).

I would identify, with respect to our ports, cybersecurity as a significant threat stream, and we are, of course, very focused on defending against it and strengthening our cybersecurity.

Senator OSSOFF. Thank you, Mr. Secretary. Will you and your staff continue to work with the Georgia Ports Authority, State and local law enforcement in Georgia to help harden the Port of Savannah and other critical port infrastructure in Georgia against that threat and other threats?

Secretary MAYORKAS. We absolutely will, and, through the infrastructure bill that has been passed fortunately we have tremendous funding to dedicate to not only the improvement of the infrastructure itself but also its hardening.

Senator OSSOFF. I want to close very briefly, Secretary Mayorkas. I thank you for your cooperation in providing to the Permanent Subcommittee on Investigations (PSI) the documents and records that allowed us to conduct an 18-month investigation of medical mistreatment of women in detention. We held that hearing, as you likely know, earlier this week. The bipartisan findings that Senator Ron Johnson of Wisconsin and I have presented are deeply disturbing and suggest there are major gaps in the vetting and oversight of DHS contracted physicians who treat the detainee population.

I ask that you review those findings in detail and that we will have a follow-up engagement to discuss the steps that DHS is taking and needs to take to ensure that the dignity and human rights and constitutional rights of all detainees are upheld.

Secretary MAYORKAS. I look forward to doing so, Senator.

Senator OSSOFF. Thank you, Mr. Secretary. Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Ossoff.

To our witnesses, we have had you there for quite some time so we are going to take a brief break. We will come back for a second round for those Senators who want a second round, but the time will be just five minutes in the second round. But let us take a recess for five minutes and we will reconvene. [Recess.]

The Committee will come back into order. Senator Ossoff, you are recognized for a second round.

Senator OSSOFF. Thank you for the extraordinary courtesy, Mr. Chairman, and welcome back to our panel.

I would like to begin, Director Wray, by requesting an update—to the extent you are able to provide details it would be appreciated—on your efforts to defend Historically Black Colleges and Universities (HBCUs) in Georgia and across the country from threats. Of course, threats have targeted Spelman College, other HBCUs in the State of Georgia. This is of deep concern to me and the whole community. Please provide an update on your efforts.

Mr. WRAY. Senator, certainly we share your concern. The fear and disruption that those threats have caused is utterly unconscionable, and this investigation, or really, I should say these investigations, plural, have been a priority for the FBI, including multiple field offices, Joint Terrorism Task Forces, et cetera.

The update that I can give is that for the first tranche of the threats nationwide, the ones that generated probably the most initial media attention, if you will, there has been a recent development. An individual, who is a juvenile, a little bit like the exchange that we had right before the break, has been identified, and because of the Federal limitations on Federal charging of juveniles for

most relevant offenses, we have worked with State prosecutors on an unrelated State charge which ensures restrictions and monitoring of the individual and disruption of his behavior.

Now that still leaves two other subsequent tranches of threats against Historically Black Colleges and Universities and other historically Black religious institutions, for example, that we are still very much actively investigating. Because of that there is not much I can share on those, but suffice it say we have a lot of people working on this and we are determined to see it through.

Senator OSSOFF. Thank you, Director Wray.

Director Abizaid, I have not had a chance yet to ask you a question, and I would like to hear from you what do you assess to be the most significant threats to the United States when it comes to transnational terrorism?

Ms. ABIZAID. By far it is ISIS and al-Qaeda in terms of transnational terrorism, though racially and ethnically motivated extremists also present a dramatic threat. The hierarchically organized groups like al-Qaeda and ISIS are actually transitioning their way of attacking to lone actor type threats and inspired violence here in the United States homeland, and we see very similar trends in the racially and ethnically motivated violent extremist bucket of ideologically motivated threats as well.

Senator OSSOFF. Thank you, ma'am. Thank you all. Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Ossoff.

The authorization from the Office of Countering Weapons of Mass Destruction (CWMD) is set to expire next year. In preparation, Senator Portman and I introduced a bill that reauthorizes CWMD Office and empowers the newly created Office of Health Security (OHS) at DHS. The bill clarifies roles and responsibilities for both offices and adds important accountability and oversight measures.

Secretary Mayorkas, could you explain to this Committee how the expiration of the authorization for CWMD would impact it if it expires, and particularly, how important the legislation is to deal with local, tribal, and territorial partners on this critical issue?

Secretary MAYORKAS. Mr. Chairman, the Office of Countering Weapons of Mass Destruction is of vital importance to the Department of Homeland Security. I think if we look back in time and we see the use of chemical weapons in Syria and the tragedies that that inflicted on the people there, that is one powerful example, and we do not have to look that far back in history to understand the importance of the office.

Just the fact that the potential, the specter of the use of nuclear weapons was discussed in public fora in light of Russia's unprovoked aggression against Ukraine speaks of the criticality of this office, and we do hope that the bipartisan bill that you have presented is passed. We need this office reauthorized.

Chairman PETERS. Thank you, Secretary.

Director Abizaid, how has the threat from weapons of mass destruction (WMD) increased or decreased over the last five years?

Ms. ABIZAID. The threat that terrorists would use WMD, and particularly CBRN capabilities I think has been sustained over that five -year time period, certainly.

Chairman PETERS. Very good.

Secretary Mayorkas, you ordered an internal review of DHS after the tragic shootings in Buffalo and Uvalde to assess whether the Department was effectively using its resources to address domestic terrorism and targeted violence. As a result of that review that you did you announced the appointment of Nick Rasmussen as the full-time Counterterrorism Coordinator.

What goals have you asked him to accomplish and what is the timeframe for him to achieve those goals?

Secretary MAYORKAS. Mr. Chairman, Nick Rasmussen comes with impeccable credentials to be the Counterterrorism Coordinator for the Department of Homeland Security. He used to be the Director of the National Counterterrorism Center, and just a distinguished career.

What I have asked him to do in the first instance is take a look at our counterterrorism efforts across the Department and make sure that we are being as impactful and effective as possible. One of the efforts that I have across the Department in every mission set is to drive greater cohesion so that our impact is maximized. That is the first thing that I have asked him to take a look at, and I am actually meeting with him in a few days to discuss the setting of a timeline and incremental goals along the way. I look forward to discussing that with you.

Chairman PETERS. Great. We will look forward to that. Certainly we do have to have a coordinator overseeing all of this, so I appreciate the efforts that you are making in that area.

The Administration just released an updated strategy and implementation plan on countering biological threats. This new strategy implements recommendations learned from the ongoing COVID–19 pandemic and the monkeypox public health emergency. Certainly global shortcomings in preparedness for the pandemic and biosecurity may inspire adversaries to develop and use biological weapons in the future, certainly a major concern for all of us.

Secretary Mayorkas, could you discuss how DHS is working to implement the National Biodefense Strategy and how has the creation of the Office of Health Security better aligned DHS efforts in this space?

Secretary MAYORKAS. Mr. Chairman, that strategy really speaks of a whole-of-society approach. It is not something that the Federal Government can do alone, but we need State and local partners and private citizens, nonprofit organizations, academia. It is a very holistic, inclusive approach to the problem, and that is the approach that we are taking in the Department through CWMD, the Office of Health Affairs, and importantly, our Office of Science and Technology (OSTP), with the research and development (R&D) that it spearheads. I am grateful to this Committee for really moving forward with the confirmation of Dimitri Kusnezov as our new Under Secretary for the Office of Science and Technology.

It is really a very all-of-society approach, and our leader of the Office of Health Affairs, our Chief Medical Officer (CMO) is a tremendous leader in identifying what are the greatest threats that are imminent or upon us, and developing a strategy to address it. He was instrumental in our protocols to address COVID–19 in immigration detention centers along the Southwest Border, working

with border communities to develop a real infrastructure to address that.

We are taking an all-of-department approach in the context of an all-of-society approach that the strategy calls for.

Chairman PETERS. That is good. This Committee will deal with this issue extensively over the next couple of years so I look forward to working closely with your team to address the challenge and the threat.

Senator Hawley, you are recognized for your questions.

Senator HAWLEY. Thank you very much, Mr. Chairman. Thanks again to the witnesses for being here.

Mr. Secretary, nice to see you. I did not get to visit with you last time so let us start with you. I think my colleagues have established, given what we are seeing on the Southern Border, the massive increase in illegality there, that that is clearly not a priority for your agency, so let us talk about what appears to be and that is spying on Americans and censoring their speech. You have turned your agency into a censorship machine.

Now you said earlier this year that you disbanded the Disinformation Governance Board (DGB), which I thought was totally unconstitutional, but that turns out to be, at best, misleading. That is just the tip of the iceberg in terms of what you are doing.

Your own Quadrennial Review, which was just reported in the press, says that disinformation is going to be the new focus at DHS. The Quad Review says that DHS plans to target—I am quoting now—"inaccurate information domestically on a wide array of subjects, including the origins of the COVID–19 pandemic, the efficacy of COVID–19 vaccines, racial justice, U.S. withdrawal from Afghanistan, and the nature of U.S. support for Ukraine." This is what you are devoting your agency's resources to.

I guess my first question is, is an American citizen who criticizes COVID mandates now to be treated as a domestic terrorist?

Secretary MAYORKAS. Of course, and I would like to say three things since you have three inaccuracies in the question you posed to me. No. 1, border security is a priority of ours. No. 2, the Department does not censor speech. And No. 3, we did not publish a Quadrennial Review.

Senator HAWLEY. Does it exist, the Quadrennial Review?

Secretary MAYORKAS. I believe it is being worked on.

Senator HAWLEY. It has been published in the media. Will you make it public?

Secretary MAYORKAS. When it is final it will be public.

Senator HAWLEY. Mr. Chairman, without objection I would like to enter this article called "The Truth Cops," published in The Intercept.[1]

Chairman PETERS. Without objection.

Senator HAWLEY. Here is my question then. If you are not censoring speech and if you are not treating Americans as domestic terrorists, then why is it that you are pressuring Big Tech to treat American citizens as if they are threats to the homeland? Why are you pressuring them to censor speech?

[1] The article referenced by Senator Hawley appears in the Appendix on page 138.

Let us take a look at some new documents that have come to light that show what your administration is doing, this Administration is doing to censor speech. Let us take a look at this email from July 16, 2021. It is over my shoulder here. Facebook emailing the Department of Health and Human Services (HHS) saying, "I know our teams met today to better understand the scope of what the White House expects from us on misinformation going forward." Are you familiar with that email?

Secretary MAYORKAS. No.

Senator HAWLEY. Let us try another one.

Here is one from July 20, 2021. The White House emails Facebook, saying, "Any way we can get this pulled down?" Forty-six seconds later, Facebook responds, "Yep. We are on it." Are you familiar with that email?

Secretary MAYORKAS. No.

Senator HAWLEY. OK. How about this one? July 23, 2021. Facebook employee writes to HHS and says, "Thank you for taking the time to meet today. Wanted to make sure you saw the steps we took just this past week to adjust policies on what we are removing with respect to misinformation." Are you familiar with that one?

Secretary MAYORKAS. Senator, we do not instruct——

Senator HAWLEY. Just yes or no.

Secretary MAYORKAS. No, because I am the Secretary of DHS.

Senator HAWLEY. I am asking you that because it is funny you say that. A Federal judge has just found, as a finding of fact, Mr. Secretary, that your office, and I am going to quote now, is "supervising the nerve center of federally directed censorship." It is a Federal judge in a Federal lawsuit. You are supervising the nerve center of federally directed censorship."

Here is another email, August 20, 2021. Facebook writes again to HHS and highlights that Facebook is "increasing the strength of our demotions for COVID and vaccine-related content." April 16, 2021. Rob Flaherty at the White House circulates a Zoom meeting invitation to Twitter employees, stating, "White House staff will be briefed by Twitter on vaccine misinformation."

We have example after example of this Administration, coordinated apparently, according to a Federal court, by your agency, pressuring, coercing social media companies to engage in censorship. Is that constitutional?

Secretary MAYORKAS. That is unequivocally false.

Senator HAWLEY. It is what the emails show.

Secretary MAYORKAS. It is unequivocally false, Senator.

Senator HAWLEY. You are not pressuring the Big Tech companies to take down accounts. You are not meeting with them to ask them to censor on your behalf.

Secretary MAYORKAS. That is correct. We are not.

Senator HAWLEY. You are not having any meetings with them whatsoever.

Secretary MAYORKAS. We meet with the tech companies——

Senator HAWLEY. How often?

Secretary MAYORKAS [continuing]. To address the homeland security mission.

Senator HAWLEY. How often do you meet with them?

Secretary MAYORKAS. For example, online child sexual exploitation is a scourge in this country, and we have an obligation to address it.

Senator HAWLEY. You are saying that no one in your office has ever met with, coordinated, or otherwise engaged in any contact with a social media company in which you spoke to them about vaccine mandates, about COVID mask mandates, about the withdrawal from Afghanistan, about the current U.S. involvement in Ukraine. None of that has ever happened.

Secretary MAYORKAS. I do not what you are referring to, Senator, and I can——

Senator HAWLEY. Read the emails.

Secretary MAYORKAS [continuing]. I can tell you this. You have actually cited emails outside of our department.

Senator HAWLEY. I have cited Federal judge who says your department is engaged in supervising the nerve center of federally directed censorship.

Here is my point, Mr. Secretary. It has been established for years in this country, as you very well know because you are a lawyer, that the Federal Government may not use private third parties to engage in activities that are unconstitutional. That is exactly what you and this Administration are doing. You are leveraging private companies to carry out censorship on your behalf. It is dystopian, but worse than that, it is unconstitutional.

Secretary MAYORKAS. It is also false.

Chairman PETERS. Thank you, Senator Hawley.

Seeing no other Senator here I want to thank our witnesses once again for joining us today. We recognize that you all have very busy schedules and we appreciate you joining us to help the Committee better understand some of the most pressing security issues that our nation is facing. This Committee will continue to work to address many of the issues that we discussed today. For example, as we heard today, the threat posed by drones is extremely serious, and we cannot let legislation that protects Americans from unmanned aircraft system expire in December. I look forward to working with my colleagues here in the Senate and in the House to ensure that the Federal Government is effectively managing this threat.

I will also continue to work with the Department and the FBI on improving the government's response to the threat posed by domestic violent extremism. I appreciate the Administration's efforts to tackle this issue but more can and must be done. Without a more data-driven approach to understand the threat, the government will continue to face challenges addressing this issue.

I will also continue to press the Administration on meeting mandatory congressional reporting requirements so that we can ensure the Federal Government has the authorities and the resources needed to help prevent deadly incidents, like the tragic shooting in Buffalo, from occurring again.

Finally, as several Members have done, on behalf of everyone on this Committee, I would like to express our sincere condolences on the absolutely tragic news of loss and injury to CBP Air and Marine Operations agents. Each and every day throughout the pandemic the frontline personnel of DHS have put their lives on the

line to protect Americans from serious threats that we have discussed today, and we all thank them for their commitment.

While we have spent several productive hours this morning examining our nation's greatest security threats, there is more work to do for our Committee to continue conducting oversight and ensuring national security agencies are effectively focused on their critical mission.

For the record, this hearing will remain open for 15 days, until 5 p.m. on December 2, 2022, for the submission of statements and questions for the record.

This hearing is now adjourned.

[Whereupon, at 12:43 p.m., the hearing was adjourned.]

A P P E N D I X

Opening Statement of Chairman Gary Peters
"Threats to the Homeland"
November 17, 2022

The Committee will come to order.

Thank you to our witnesses for joining us and for your continued service to the American people. This hearing is an important opportunity for this Committee to hear from our nation's top national security and law enforcement officials about the threats facing our nations –and how Congress can ensure the federal government is prepared to protect our communities from them.

More than twenty years ago – the September 11th terrorist attacks changed our nation forever. In response – Congress created the Department of Homeland Security and our entire national security apparatus focused on keeping Americans safe from international terrorism.

However – in the more than two decades following those attacks – the threats to our communities have evolved and become increasingly complex.

While we must continue to monitor international terror threats – there is no question that we must be better prepared to defend against what top national security officials – including those before us today – have called the most lethal terrorist threat to Americans: domestic terrorism fueled by white nationalist and anti-government ideologies.

Yesterday – I released a report detailing the results of my investigation. Alarmingly – my investigation found that DHS and FBI have not adequately addressed the evolving domestic terrorism threat. Despite a requirement in law – written by myself and Senator Johnson – DHS and FBI have failed to effectively measure and share comprehensive data on the threat posed by violent domestic extremists – and specifically white supremacist and anti-government violence.

Without this comprehensive data – it is impossible for Congress – and this Committee – to determine whether our nation's counterterrorism resources are effectively aligned to tackle the domestic terrorism threat. We need a data-driven approach to preventing deadly incidents like the January 6th Capitol breach – the tragic shooting in Buffalo – and countless other domestic terrorist attacks that have been fueled by hateful extremist ideologies. I look forward to hearing from our witnesses today about what resources and tools their agencies need to effectively collect data on domestic terrorism and prevent these crimes.

Today – we'll also have the opportunity to discuss the significant threat that cyber-attacks pose to our national and economic security.

I'm proud of the bipartisan work Senator Portman and I have led this Congress to enact some of the most significant reforms to our nation's cybersecurity policy in history. Our reforms will ensure that DHS has the tools – resources – and authorities needed to protect critical infrastructure – state and local governments – and other targets from cyber-attacks. However – there is more that must be done to continue securing our vulnerabilities from criminal hackers and foreign adversaries – and I look forward to discussing those topics today.

One of the most serious threats – and one of the toughest to tackle – is the threat posed by increasingly severe natural disasters and climate change.

This is an existential threat to our planet – and unless it is addressed – it will have a significant impact on our homeland security. Today – we'll hear more about how our national security agencies are tracking these challenges and how they are planning to address the security threats they present now and in the future.

We also have a challenging situation at our Southern Border – and today we'll discuss the Administration's work to secure both our Northern and Southern borders – and prevent illegal trafficking and stop the flow of deadly illicit drugs like fentanyl into our communities.

Those are difficult missions that must be accomplished ensuring that lawful international trade and travel can continue to flow smoothly at our ports of entry — and keep states like my home state of Michigan a hub for international commerce.

As our national security agencies continue to tackle these long standing threats – they must also be prepared to counter emerging ones. Over the last few years the threat posed by unmanned aerial systems, or drones, has become increasingly perilous. Small drones, which can be purchased off the shelf at any electronic store, can be weaponized by malicious actors to damage our nation's critical infrastructure or inflict mass casualties. Today's drones could be used to launch remote attacks on everything from government buildings to crowds at public events, including large sports stadiums. We cannot let the current authorities that help address this grave threat expire in December – and I will continue working to ensure those important authorities are extended and updated.

Similarly – weaponized biological – chemical – nuclear – and radioactive materials – also remain a significant threat to our homeland security. I have introduced bipartisan legislation with Sen. Portman to reauthorize and strengthen the office in DHS charged with overseeing these threats – and I will continue working with my colleagues to pass it as soon as possible.

The scope and volume of these – and many other national security threats – requires Congress and the Administration to work together to ensure we are doing everything we can to keep Americans safe.

Today I am pleased to welcome back each of our witnesses to hear more about how their agencies are working to effectively carry out this daunting and essential mission. I look forward to a productive discussion.

Before I turn things over – I want to take a moment to recognize Senator Portman – who is retiring this year.

Rob – it has been a real pleasure leading this committee with you for the past two years. I'm grateful for all of your hard work to help pass so much meaningful legislation through our committee – from providing important financial relief to the U.S. Postal Service – strengthening

our ability to detect and deter cyber-attacks – and working to make our nation more secure and our government more effective for taxpayers.

I'd also like to thank your Staff Director Pam Thiessen and the exceptional team you have put together for all of their hard work over the past two years.
I've really appreciated how well our teams have worked together and I'm looking forward to celebrating all of our successes as we wrap up this Congress.

And I will now turn it over to you, Ranking Member Portman, for your opening remarks.

Opening Statement
Ranking Member Rob Portman
U.S. SENATE COMMITTEE ON HOMELAND SECURITY
& GOVERNMENTAL AFFAIRS
"THREATS TO THE HOMELAND"
NOVEMBER 17, 2022

Thank you, Chairman Peters, for convening this hearing. We have a lot to discuss today regarding the proliferation of historic threats facing the homeland, and the right people are here to speak about what the Administration is doing to counter those threats. I have been honored to serve on this Committee alongside Senator Peters, whom I sincerely thank for his willingness to find common ground and solve problems for the American people. I also want to extend my gratitude to David Weinberg and the rest of your staff.

Welcome, Secretary Mayorkas, Director Wray, and Director Abizaid.

As the respective leaders of your agencies, you are responsible for overseeing the career men and women of DHS, the FBI, and the National Counterterrorism Center whose mission is to safeguard our nation. This Committee is deeply appreciative of the work these patriots do to further that mission.

Every fall since the terrorist attacks on 9/11, we hold this hearing to examine America's security challenges and discuss how we can work together to address potential and active threats. I can think of no greater priority for my last hearing as Ranking Member than to sound the alarm about our current security threats.

I will start with the growing disaster at the border.

President Biden's failed border policy has ensured that not only our nation's borders remain unsecure but foreign adversaries, transnational criminal organizations, and other nefarious actors know they can enter our country and threaten the safety and security of the American public with virtual impunity.

In the past year, Border Patrol apprehended more than 2 million total unlawful migrants. This is up 143 percent since 2019. And that figure does not include the number of "got-aways," or individuals who crossed our border undetected. Criminals who traffic both humans and drugs across our border are able to do so with ease because our Border Patrol is using most of its time to process unlawful migrants into the country.

Those drugs include record levels of deadly fentanyl seizures causing record numbers of overdose deaths.

The first two years of the Biden administration have been by far the worst two years of unlawful migration and deadly drug seizures in our nation's history.

Another historic failure of the Biden Administration with regard to our nation's security was its chaotic withdrawal from Afghanistan. Afghans who had stood with us and our allies were left behind to suffer under Taliban rule. Meanwhile, more than 36,000 Afghans with no record of ever partnering with us, some of whom have apparent ties to terrorism. Were paroled into our country without proper screening and vetting.

Despite three reports from two Inspectors General documenting the failures of DHS vetting and then paroling known or suspected terrorists into our communities, DHS continues to deny any problem. Yet, President Biden requested and received an additional $15 million for the FBI to conduct counter-terror investigations of known or suspected terrorists among the Afghan evacuees released into our country by DHS. In other words, Director Wray is responsible for cleaning up the mess created by DHS -- so perhaps we have divergent views on this panel about this subject.

We all recognize the grave threat posed by our adversaries, such as Russia, Iran, and China, who rely on disinformation tactics to weaken our democracy. But at home, we must be much more careful around issues of domestic speech. We must respond to imminent threats of violence, but censoring constitutionally-protected speech is another matter entirely. To be precise, it is a redline.

I hope we can all agree that the United States government should not censor the speech of our own citizens. Americans' speech, differences of opinion, and political viewpoints are not a threat to democracy, but rather a bedrock of it.

We know now that while DHS disbanded its disturbing Disinformation Governance Board after significant public outcry, it has continued its efforts to curb speech under the guise of countering mis- or dis-information. The entanglement of the FBI and DHS with social media platforms for the purposes of controlling narratives is of deep concern.

Recent reports allege that DHS is colluding with Big Tech to moderate content in a way that conforms with the Biden administration's politically-skewed viewpoint including on the Afghanistan withdrawal and the origin of Covid.

Our democracy is also under threat because Congress and the Administration have been unwilling to confront the systematic theft of US intellectual property by China which is undermining our national security and economic security. To those who believe that research security is not important, I will remind you the recent comments by Director Wray said "there is no country that presents a broader, more severe threat to our innovation, our ideas, and our economic security than China." I couldn't agree more.

Every day, China reinforces the findings of our various investigations, showing the staggering extent of the Chinese Government's efforts to conduct influence and espionage operations in our country, and to steal American technology, research, and information for their own military and economic benefit. Addressing this threat is more urgent than ever and yet the Safeguarding American Innovation Act, which was reported out of this Committee, has been blocked from becoming law because of the unwillingness of Congress to confront this issue.

Cyberattacks are another significant issue facing every sector of our country. They are a force multiplier for our adversaries, who understand our economic and security dependence on technology. Compounding that problem is the inherent difficulty of attributing cyberattacks to specific nation-states or criminal groups.

Terrorism and targeted violence also remain serious threats to our nation. This year, an Islamist terrorist gained entry to the United States and attacked a synagogue in Colleyville, Texas. In a separate incident, an Ohio-based Islamic State operative plotted to assassinate former President Bush.

I remain concerned about the threat posed by foreign terrorist organizations, especially in the wake of our hasty withdrawal from Afghanistan. Al-Qaeda continues to pose a threat to the United States. The Islamic State continues to expand and mobilize. Iranian-sponsored Shi'a terrorist groups target key U.S. interests and government officials. We must remain vigilant as these terrorist organizations regroup and evolve.

We must restore confidence in the American public that we're committed to protect this nation from terrorism, espionage, and other homeland security threats. This effort should be bipartisan. We all have the same goal, a safe, secure American homeland.

With that said, I look forward to your testimony, but most importantly, your responses to our questions regarding your record addressing these threats. I will note that only last week did we finally receive overdue answers to questions from

last year's hearing. I hope this Committee will receive prompt responses this time around.

Thank you, Mr. Chairman.

TESTIMONY OF

Alejandro N. Mayorkas
Secretary
U.S. Department of Homeland Security

BEFORE

Committee Homeland Security and Governmental Affairs
United States Senate

ON

"Threats to the Homeland"

November 17, 2022
Washington, DC

Chairman Peters, Ranking Member Portman, 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 cyberspace, our adversaries—hostile nations and non-nation state cybercriminals—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 cybercriminals 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 gatherings; 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 11th 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 homegrown 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-Qa'ida 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 online 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-Qa'ida-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-Qa'ida'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 US 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 ongoing 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 FY 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 authenticate 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 online. 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 online 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 three 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

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

announced 43 TVTP grant awards to entities in 20 states, totaling $20 million, for Fiscal Year (FY) 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 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 online, 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 FY 2021 levels, for a total of $250 million. The FY 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 FY2021 and FY2022. This means that between FY 2021 and FY 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 FY 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 FY 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), online 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 foreign 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 cybercriminals around the world, continually grow more sophisticated and create more adverse consequences.

Within the past two years, we have seen numerous cybersecurity incidents impacting organizations of all sizes and disrupting critical services, from the SolarWinds supply chain compromise to the widespread 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, widespread threat, and Iran may choose to leverage its cyber access for disruptive or destructive attacks.

In the last two 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 cybercriminals 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 cybercrimes. 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. Cybercrimes 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 cybercrimes.

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 FY 2022, $183.5 million was made available under the SLCGP, with varying funding amounts allocated over four 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 response 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 UN 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 two-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 worldwide 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 cybercrimes, 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 FY 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 cyberspace, 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 FY21. 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 frontline 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 towards 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 FY 2021 and 14,700 pounds in FY 2022. This compares to 2,804 pounds in FY 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 U.S. 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 FY 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 FY 2022. Additionally, in FY 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 FY 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 one year ago. Reporting from the U.S. Agency for International Development (USAID) suggests that nearly one in four Venezuelans have fled their home since 2014, approximately seven million people. At least one in three 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 four 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 FY 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 NGOs – 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 FY22, 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 FY21.

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 FY 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 FY22. 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 online child sexual exploitation and abuse (CSEA) has increased dramatically in recent years. Reports of online 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 FY21, 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 FY 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 towards 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 FY 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 FY 2021 to 40 in FY 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 U.S., 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 unclassified 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 three-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 two 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.

Department of Justice

STATEMENT OF

CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED

"THREATS TO THE HOMELAND"

PRESENTED

NOVEMBER 17, 2022

STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

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

AT A HEARING ENTITLED
"THREATS TO THE HOMELAND"

PRESENTED
NOVEMBER 17, 2022

Good morning, Chairman Peters, Ranking Member Portman, 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 homegrown 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 U.S. The breadth of these threats and challenges are as complex as any time in our history. And 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 understands 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 number one 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 online, and who primarily use easily accessible weapons to attack soft targets. We see the lone offender threat with both Domestic Violent Extremists ("DVEs") and Homegrown 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 Homegrown 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 three of the four 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 four lethal attacks, resulting in 13 deaths. DVEs with mixed or personalized ideologies committed two of the four attacks. The other two 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 two-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 primarily 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-Qa'ida 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-Qa'ida 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' 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-Qa'ida 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-Qa'ida 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-Qa'ida 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 worldwide. 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 two 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 SolarWinds-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 cybercriminal activity begins. Some cybercriminals contract or sell services to nation-states; some nation-state actors moonlight as cybercriminals 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 cybercriminals 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 cybercrime 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 cybercrime 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% 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 worldwide 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—worldwide. 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 UK'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 cyberspace.

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 U.S. 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 dialogue 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 two 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 six 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 investigative 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% – 20% 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 U.S.

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 online 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 online 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 four 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 nationwide.

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 widespread 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 number one 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-online 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 three U.S. sailors and severely wounded eight 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 Peters, Ranking Member Portman, and Members of the Committee, thank you for the opportunity to testify today. I am happy to answer any questions you might have.

United States Senate Committee on Homeland Security and Government Affairs

Annual Threat Assessment to the Homeland

Statement for the Record

Ms. Christine Abizaid

Director, National Counterterrorism Center

November 17, 2022

Good morning, Chairman Peters, Ranking Member Portman, 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 ongoing 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-Qa'ida 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 worldwide 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-Qa'ida 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 extremist 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-Qa'ida or ISIS, compared to eight 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 online 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-Qa'ida 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 online platforms. Even as technology companies improve their capabilities to detect and respond to violent extremist content online, 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 worldwide continue to inspire followers and enable attack plotting against the United States, Americans, and other Western countries. ISIS and al-Qa'ida, 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 three 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 two and injured 21. Pro-ISIS supporter groups have also helped augment ISIS's media presence by creating, archiving, translating, and disseminating multilingual propaganda online. 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-Qa'ida post-Zawahiri

The death of al-Qa'ida's longtime leader Ayman al-Zawahiri, this past July in Kabul, Afghanistan, dealt an important strategic and symbolic blow to the al-Qa'ida network, which he led from relative isolation for more than a decade. Zawahiri was a respected ideological leader among the al-Qa'ida global network who strove to enhance interconnectivity across al-Qa'ida'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-Qa'ida 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-Qa'ida's sworn enemies. Other, less prominent al-Qa'ida 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-Qa'ida network.

Al-Qa'ida's global network

Al-Qa'ida'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-Qa'ida'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-Qa'ida 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-Qa'ida in the Islamic Maghreb (AQIM) has experienced setbacks from CT pressure since early 2018, but probably provides guidance to other al-Qa'ida 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-Qa'ida'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-Qa'ida 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-Qa'ida 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-Qa'ida's South Asia affiliate, al-Qa'ida in the Indian Sub-continent (AQIS), is the weakest group in the organization's global network. Al-Qa'ida 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-Qa'ida 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 twenty-one 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.

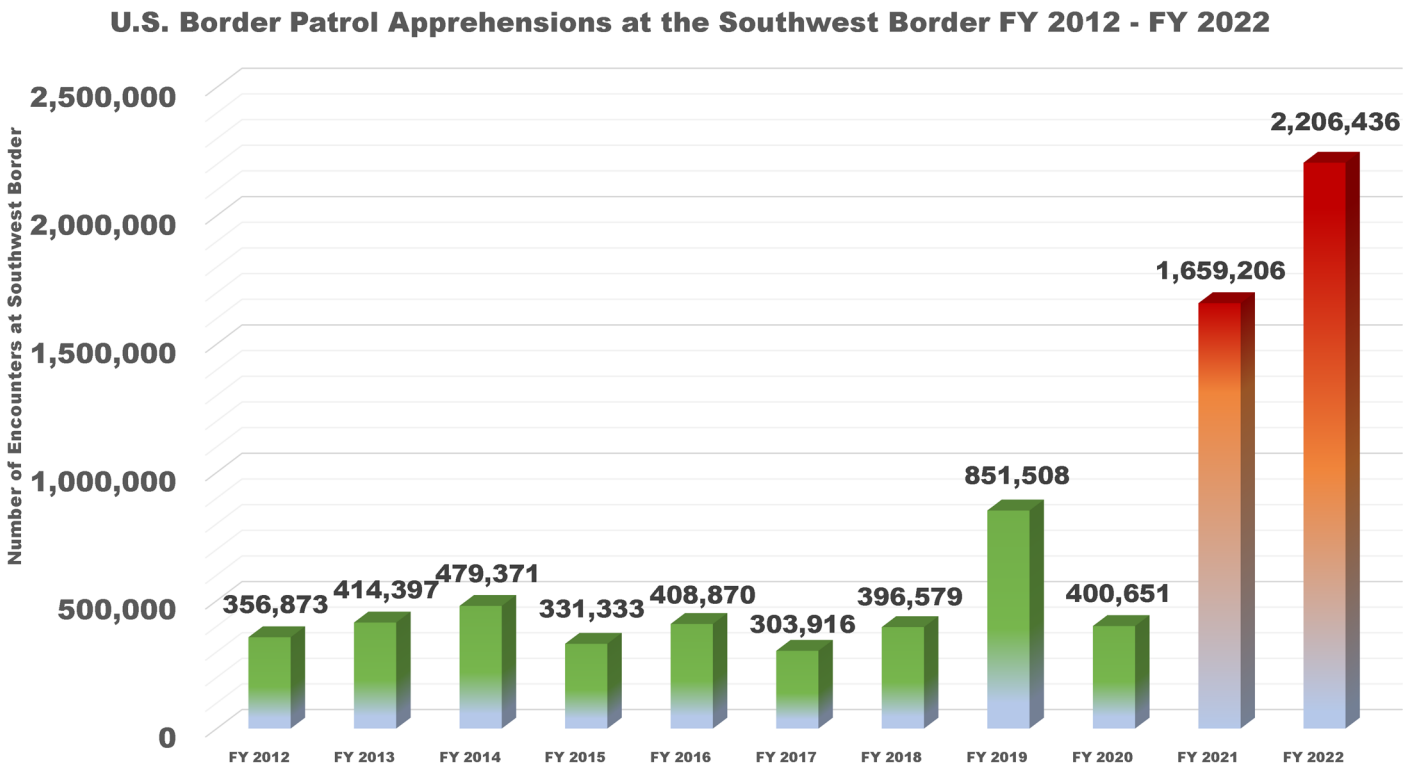
CT in a time of competing priorities requires very purposeful and transparent decisions about when and where resource shifts can be made to retain as much of the hallmark

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 ongoing 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.



SOURCE: U.S. Border Patrol, *Total Illegal Apprehensions by Month*

Co-Authored by:

TLP:CLEAR

Product ID: AA22-320A

November 16, 2022

Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester

SUMMARY

From mid-June through mid-July 2022, CISA conducted an incident response engagement at a Federal Civilian Executive Branch (FCEB) organization where CISA observed suspected advanced persistent threat (APT) activity. In the course of incident response activities, CISA determined that cyber threat actors exploited the Log4Shell vulnerability in an unpatched VMware Horizon server, installed XMRig crypto mining software, moved laterally to the domain controller (DC), compromised credentials, and then implanted Ngrok reverse proxies on several hosts to maintain persistence. CISA and the Federal Bureau of Investigation (FBI) assess that the FCEB network was compromised by Iranian government-sponsored APT actors.

CISA and FBI are releasing this Cybersecurity Advisory (CSA) providing the suspected Iranian government-sponsored actors' tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help network defenders detect and protect against related compromises.

CISA and FBI encourage all organizations with affected VMware systems that did not immediately apply available patches or workarounds to assume compromise and initiate threat hunting activities. If suspected initial access or compromise is detected based on IOCs or TTPs described in this CSA, CISA and FBI encourage organizations to assume lateral movement by threat actors, investigate connected systems (including the DC), and audit privileged accounts. All organizations, regardless of identified evidence of compromise, should apply the recommendations in the Mitigations section of this CSA to protect against similar malicious cyber activity.

For more information on Iranian government-sponsored Iranian malicious cyber activity, see CISA's Iran Cyber Threat Overview and Advisories webpage and FBI's Iran Threats webpage.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282- 0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 12. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques with corresponding mitigation and/or detection recommendations.

Overview

In April 2022, CISA conducted retrospective analysis using EINSTEIN—an FCEB-wide intrusion detection system (IDS) operated and monitored by CISA—and identified suspected APT activity on an FCEB organization's network. CISA observed bi-directional traffic between the network and a known malicious IP address associated with exploitation of the Log4Shell vulnerability (CVE-2021-44228) in VMware Horizon servers. In coordination with the FCEB organization, CISA initiated threat hunting incident response activities; however, prior to deploying an incident response team, CISA observed additional suspected APT activity. Specifically, CISA observed HTTPS activity from IP address `51.89.181[.]64` to the organization's VMware server. Based on trusted third-party reporting, `51.89.181[.]64` is a Lightweight Directory Access Protocol (LDAP) server associated with threat actors exploiting Log4Shell. Following HTTPS activity, CISA observed a suspected LDAP callback on port 443 to this IP address. CISA also observed a DNS query for `us-nation-ny[.]cf` that resolved back to `51.89.181[.]64` when the victim server was returning this Log4Shell LDAP callback to the actors' server.

CISA assessed that this traffic indicated a confirmed compromise based on the successful callback to the indicator and informed the organization of these findings; the organization investigated the activity and found signs of compromise. As trusted-third party reporting associated Log4Shell activity from `51.89.181[.]64` with lateral movement and targeting of DCs, CISA suspected the threat actors had moved laterally and compromised the organization's DC.

From mid-June through mid-July 2022, CISA conducted an onsite incident response engagement and determined that the organization was compromised as early as February 2022, by likely Iranian government-sponsored APT actors who installed XMRig crypto mining software. The threat actors also moved laterally to the domain controller, compromised credentials, and implanted Ngrok reverse proxies.

Threat Actor Activity

In February 2022, the threat actors exploited Log4Shell [T1190] for initial access [TA0001] to the organization's unpatched VMware Horizon server. As part of their initial exploitation, CISA observed a connection to known malicious IP address `182.54.217[.]2` lasting 17.6 seconds.

The actors' exploit payload ran the following PowerShell command [T1059.001] that added an exclusion tool to Windows Defender [T1562.001]:

```
powershell try{Add-MpPreference -ExclusionPath 'C:\'; Write-Host 'added-
exclusion'} catch {Write-Host 'adding-exclusion-failed' }; powershell -enc
"$BASE64 encoded payload to download next stage and execute it"
```

The exclusion tool allowlisted the entire `c:\drive`, enabling threat actors to download tools to the `c:\drive` without virus scans. The exploit payload then downloaded `mdeploy.text` from `182.54.217[.]2/mdepoy.txt` to `C:\users\public\mde.ps1` [T1105]. When executed, `mde.ps1` downloaded `file.zip` from `182.54.217[.]2` and removed `mde.ps1` from the disk [T1070.004].

`file.zip` contained XMRig cryptocurrency mining software and associated configuration files.

- `WinRing0x64.sys` – XMRig Miner driver
- `wuacltservice.exe` – XMRig Miner
- `config.json` – XMRig miner configuration
- `RuntimeBroker.exe` – Associated file. This file can create a local user account [T1136.001] and tests for internet connectivity by pinging `8.8.8.8` [T1016.001]. The exploit payload created a Scheduled Task [T1053.005] that executed `RuntimeBroker.exe` daily as `SYSTEM`. **Note**: By exploiting Log4Shell, the actors gained access to a VMware service account with administrator and system level access. The Scheduled Task was named `RuntimeBrokerService.exe` to masquerade as a legitimate Windows task.

See MAR 10387061-1.v1 for additional information, including IOCs, on these four files.

After obtaining initial access and installing XMRig on the VMWare Horizon server, the actors used RDP [T1021.001] and the built-in Windows user account `DefaultAccount` [T1078.001] to move laterally [TA0008] to a VMware VDI-KMS host. Once the threat actor established themselves on the VDI-KMS host, CISA observed the actors download around 30 megabytes of files from `transfer[.]sh` server associated with `144.76.136[.]153`. The actors downloaded the following tools:

- PsExec – a Microsoft signed tool for system administrators.
- Mimikatz – a credential theft tool.
- Ngrok – a reverse proxy tool for proxying an internal service out onto an Ngrok domain, which the user can then access at a randomly generated subdomain at `*.ngrok[.]io`. CISA has observed this tool in use by some commercial products for benign purposes; however, this process bypasses typical firewall controls and may be a potentially unwanted application in production environments. Ngrok is known to be used for malicious purposes.[1]

The threat actors then executed Mimikatz on VDI-KMS to harvest credentials and created a rogue domain administrator account [T1136.002]. Using the newly created account, the actors leveraged RDP to propagate to several hosts within the network. Upon logging into each host, the actors manually disabled Windows Defender via the Graphical User Interface (GUI) and implanted Ngrok executables and configuration files. The threat actors were able to implant Ngrok on multiple hosts to ensure Ngrok's persistence should they lose access to a machine during a routine reboot. The actors were able to proxy [T1090] RDP sessions, which were only observable on the local network as outgoing HTTPS port 443 connections to `tunnel.us.ngrok[.]com` and `korgn.su.lennut[.]com`

(the prior domain in reverse). It is possible, but was not observed, that the threat actors configured a custom domain, or used other Ngrok tunnel domains, wildcarded here as `*.ngrok[.]com`, `*.ngrok[.]io`, `ngrok.*.tunnel[.]com`, or `korgn.*.lennut[.]com`.

Once the threat actors established a deep foothold in the network and moved laterally to the domain controller, they executed the following PowerShell command on the Active Directory to obtain a list of all machines attached to the domain [T1018]:

```
Powershell.exe get-adcomputer -filter * -properties * | select
name,operatingsystem,ipv4address &gt;
```

The threat actors also changed the password for the local administrator account [T1098] on several hosts as a backup should the rogue domain administrator account get detected and terminated. Additionally, the threat actor was observed attempting to dump the Local Security Authority Subsystem Service (LSASS) process [T1003.001] with task manager but this was stopped by additional anti-virus the FCEB organization had installed.

MITRE ATT&CK TACTICS AND TECHNIQUES

See table 1 for all referenced threat actor tactics and techniques in this advisory, as well as corresponding detection and/or mitigation recommendations. For additional mitigations, see the Mitigations section.

Table 1: Cyber Threat Actors ATT&CK Techniques for Enterprise

Initial Access			
Technique Title	**ID**	**Use**	**Recommendations**
Exploit Public-Facing Application	T1190	The actors exploited Log4Shell for initial access to the organization's VMware Horizon server.	**Mitigation/Detection:** Use a firewall or web-application firewall and enable logging to prevent and detect potential Log4Shell exploitation attempts [M1050]. **Mitigation:** Perform regular vulnerability scanning to detect Log4J vulnerabilities and update Log4J software using vendor provided patches [M1016],[M1051].

Execution			
Technique Title	**ID**	**Use**	**Recommendation**
Command and Scripting Interpreter: PowerShell	T1059.001	The actors ran PowerShell commands that added an exclusion tool to Windows Defender. The actors executed PowerShell on the AD to obtain a list of machines on the domain.	**Mitigation:** Disable or remove PowerShell for non-administrative users [M1042],[M1026] or enable code-signing to execute only signed scripts [M1045]. **Mitigation:** Employ anti-malware to automatically detect and quarantine malicious scripts [M1049].
Persistence			
Technique Title	**ID**	**Use**	**Recommendations**
Account Manipulation	T1098	The actors changed the password for the local administrator account on several hosts.	**Mitigation:** Use multifactor authentication for user and privileged accounts [M1032]. **Detection:** Monitor events for changes to account objects and/or permissions on systems and the domain, such as event IDs `4738`, `4728`, and `4670`. Monitor for modification of accounts in correlation with other suspicious activity [DS0002].
Create Account: Local Account	T1136.001	The actors' malware can create local user accounts.	**Mitigation:** Configure access controls and firewalls to limit access to domain controllers and systems used to create and manage accounts. **Detection:** Monitor executed commands and arguments for actions that are associated with local account creation, such as `net`

			`user /add` , `useradd`, and `dscl -create` [DS0017]. **Detection:** Enable logging for new user creation [DS0002].
Create Account: Domain Account	T1136.002	The actors used Mimikatz to create a rogue domain administrator account.	**Mitigation:** Configure access controls and firewalls to limit access to domain controllers and systems used to create and manage accounts. **Detection:** Enable logging for new user creation, especially domain administrator accounts [DS0002].
Scheduled Task/Job: Scheduled Task	T1053.005	The actors' exploit payload created Scheduled Task `RuntimeBrokerService.exe`, which executed `RuntimeBroker.exe` daily as `SYSTEM`.	**Mitigation:** Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as `SYSTEM` [M1028]. **Detection:** Monitor for newly constructed processes and/or command-lines that execute from the `svchost.exe` in Windows 10 and the Windows Task Scheduler `taskeng.exe` for older versions of Windows [DS0009] **Detection:** Monitor for newly constructed scheduled jobs by enabling the `Microsoft-Windows-TaskScheduler/Operational` setting within the event logging service [DS0003].
Valid Accounts: Default Accounts	T1078.001	The actors used built-in Windows user account `DefaultAccount`.	**Mitigation:** Change default usernames and passwords immediately after the installation and before deployment to a production environment [M1027].

			Detection: Develop rules to monitor logon behavior across default accounts that have been activated or logged into [DS0028].
Defense Evasion			
Technique Title	**ID**	**Use**	**Recommendations**
Impair Defenses: Disable or Modify Tools	T1562.001	The actors added an exclusion tool to Windows Defender. The tool allowlisted the entire `c:\drive`, enabling the actors to bypass virus scans for tools they downloaded to the `c:\drive`. The actors manually disabled Windows Defender via the GUI.	**Mitigation:** Ensure proper user permissions are in place to prevent adversaries from disabling or interfering with security services. [M1018]. **Detection:** Monitor for changes made to Windows Registry keys and/or values related to services and startup programs that correspond to security tools such as `HKLM:\SOFTWARE\Policies\Microsoft\Windows` Defender [DS0024]. **Detection:** Monitor for telemetry that provides context for modification or deletion of information related to security software processes or services such as Windows Defender definition files in Windows and System log files in Linux [DS0013]. **Detection:** Monitor processes for unexpected termination related to security tools/services [DS0009].
Indicator Removal on Host: File Deletion	T1070.004	The actors removed malicious file `mde.ps1` from the dis.	**Detection:** Monitor executed commands and arguments for actions that could be utilized to unlink, rename, or delete files [DS0017].

			Detection: Monitor for unexpected deletion of files from the system [DS0022].
Credential Access			
Technique Title	**ID**	**Use**	**Recommendations**
OS Credential Dumping: LSASS Memory	T1003.001	The actors were observed trying to dump LSASS process.	**Mitigation:** With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping [M1043] **Mitigation:** On Windows 10, enable Attack Surface Reduction (ASR) rules to secure LSASS and prevent credential stealing [M1040]. **Mitigation:** Ensure that local administrator accounts have complex, unique passwords across all systems on the network [M1027]. **Detection:** Monitor for unexpected processes interacting with `LSASS.exe`. Common credential dumpers such as Mimikatz access `LSASS.exe` by opening the process, locating the LSA secrets key, and decrypting the sections in memory where credential details are stored. [DS0009]. **Detection:** Monitor executed commands and arguments that may attempt to access credential material stored in the process memory of the LSASS [DS0017].

Credentials from Password Stores	T1555	The actors used Mimikatz to harvest credentials.	**Mitigation:** Organizations may consider weighing the risk of storing credentials in password stores and web browsers. If system, software, or web browser credential disclosure is a significant concern, technical controls, policy, and user training may be used to prevent storage of credentials in improper locations [M1027]. **Detection:** Monitor for processes being accessed that may search for common password storage locations to obtain user credentials [DS0009]. **Detection:** Monitor executed commands and arguments that may search for common password storage locations to obtain user credentials [DS0017].
Discovery			
Technique Title	**ID**	**Use**	**Recommendations**
Remote System Discovery	T1018	The actors executed a PowerShell command on the AD to obtain a list of all machines attached to the domain.	**Detection:** Monitor executed commands and arguments that may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for lateral movement [DS0017]. **Detection:** Monitor for newly constructed network connections associated with pings/scans that may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for lateral movement [DS0029].

			Detection: Monitor for newly executed processes that can be used to discover remote systems, such as ping.exe and tracert.exe, especially when executed in quick succession [DS0009].
System Network Configuration Discovery: Internet Connection Discovery	T1016.001	The actors' malware tests for internet connectivity by pinging `8.8.8.8`.	**Mitigation:** Monitor executed commands, arguments [DS0017] and executed processes (e.g., `tracert` or `ping`) [DS0009] that may check for internet connectivity on compromised systems.
Lateral Movement			
Technique Title	**ID**	**Use**	**Recommendations**
Remote Services: Remote Desktop Protocol	T1021.001	The actors used RDP to move laterally to multiple hosts on the network.	**Mitigation:** Use MFA for remote logins [M1032]. **Mitigation:** Disable the RDP service if it is unnecessary [M1042]. **Mitigation:** Do not leave RDP accessible from the internet. Enable firewall rules to block RDP traffic between network security zones within a network [M1030]. **Mitigation:** Consider removing the local Administrators group from the list of groups allowed to log in through RDP [M1026]. **Detection:** Monitor for user accounts logged into systems associated with RDP (ex: Windows EID `4624` Logon Type 10). Other factors, such as access patterns (ex: multiple systems over a relatively short period of time) and activity that occurs after a remote login, may indicate suspicious or

			malicious behavior with RDP [DS0028].
Command and Control			
Technique Title	**ID**	**Use**	**Recommendations**
Proxy	T1090	The actors used Ngrok to proxy RDP connections and to perform command and control.	**Mitigation:** Traffic to known anonymity networks and C2 infrastructure can be blocked through the use of network allow and block lists [M1037]. **Detection:** Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g., extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure) [DS0029].
Ingress Tool Transfer	T1105	The actors downloaded malware and multiple tools to the network, including PsExec, Mimikatz, and Ngrok.	**Mitigation:** Employ anti-malware to automatically detect and quarantine malicious scripts [M1049].

INCIDENT RESPONSE

If suspected initial access or compromise is detected based on IOCs or TTPs in this CSA, CISA encourages organizations to assume lateral movement by threat actors and investigate connected systems and the DC.

CISA recommends organizations apply the following steps **before applying** any mitigations, including patching.

1. Immediately isolate affected systems.
2. Collect and review relevant logs, data, and artifacts. Take a memory capture of the device(s) and a forensic image capture for detailed analysis.

3. Consider soliciting support from a third-party incident response organization that can provide subject matter expertise to ensure the actor is eradicated from the network and to avoid residual issues that could enable follow-on exploitation.
4. Report incidents to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870) or your local FBI field office or FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov.

MITIGATIONS

CISA and FBI recommend implementing the mitigations below and in table 1 to improve your organization's cybersecurity posture on the basis of threat actor behaviors.

- **Install updated builds to ensure affected VMware Horizon and UAG systems are updated to the latest version**.
    - If updates or workarounds were not promptly applied following VMware's release of updates for Log4Shell in December 2021, treat those VMware Horizon systems as compromised. Follow the pro-active incident response procedures outlined above prior to applying updates. If no compromise is detected, apply these updates as soon as possible.
        - See VMware Security Advisory VMSA-2021-0028.13 and VMware Knowledge Base (KB) 87073 to determine which VMware Horizon components are vulnerable.
        - **Note:** Until the update is fully implemented, consider removing vulnerable components from the internet to limit the scope of traffic. While installing the updates, ensure network perimeter access controls are as restrictive as possible.
        - If upgrading is not immediately feasible, see KB87073 and KB87092 for vendor-provided temporary workarounds. Implement temporary solutions using an account with administrative privileges. Note that these temporary solutions should not be treated as permanent fixes; vulnerable components should be upgraded to the latest build as soon as possible.
        - Prior to implementing any temporary solution, ensure appropriate backups have been completed.
        - Verify successful implementation of mitigations by executing the vendor supplied script `Horizon_Windows_Log4j_Mitigations.zip` without parameters to ensure that no vulnerabilities remain. See KB87073 for details.
- **Keep all software up to date** and prioritize patching known exploited vulnerabilities (KEVs).
- **Minimize the internet-facing attack surface** by hosting essential services on a segregated DMZ, ensuring strict network perimeter access controls, and not hosting internet-facing services that are not essential to business operations. Where possible, implement regularly updated web application firewalls (WAF) in front of public-facing services. WAFs can protect against web-based exploitation using signatures and heuristics that are likely to block or alert on malicious traffic.

- **Use best practices for identity and access management (IAM)** by implementing phishing resistant MFA, enforcing use of strong passwords, regularly auditing administrator accounts and permissions, and limiting user access through the principle of least privilege. Disable inactive accounts uniformly across the AD, MFA systems, etc.
    - If using Windows 10 version 1607 or Windows Server 2016 or later, monitor or disable Windows `DefaultAccount`, also known as the Default System Managed Account (DSMA).
- **Audit domain controllers to log** successful Kerberos Ticket Granting Service (TGS) requests and ensure the events are monitored for anomalous activity.
    - Secure accounts.
    - Enforce the principle of least privilege. Administrator accounts should have the minimum permission necessary to complete their tasks.
    - Ensure there are unique and distinct administrative accounts for each set of administrative tasks.
    - Create non-privileged accounts for privileged users and ensure they use the non-privileged accounts for all non-privileged access (e.g., web browsing, email access).
- **Create a deny list of known compromised credentials** and prevent users from using known-compromised passwords.
- **Secure credentials by restricting where accounts and credentials can be used** and by using local device credential protection features.
    - Use virtualizing solutions on modern hardware and software to ensure credentials are securely stored.
    - Ensure storage of clear text passwords in LSASS memory is disabled. **Note:** For Windows 8, this is enabled by default. For more information see Microsoft Security Advisory Update to Improve Credentials Protection and Management.
    - Consider disabling or limiting NTLM and WDigest Authentication.
    - Implement Credential Guard for Windows 10 and Server 2016 (refer to Microsoft: Manage Windows Defender Credential Guard for more information). For Windows Server 2012R2, enable Protected Process Light for Local Security Authority (LSA).
    - Minimize the AD attack surface to reduce malicious ticket-granting activity. Malicious activity such as "Kerberoasting" takes advantage of Kerberos' TGS and can be used to obtain hashed credentials that threat actors attempt to crack.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, CISA and FBI recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. CISA and FBI recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see table 1).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA and FBI recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

REFERENCES

[1] MITRE ATT&CK Version 12: Software – Ngrok

1

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF FLORIDA

PENSACOLA DIVISION

- - - - - - - - - - - - - - - - - x

STATE OF FLORIDA, :

Plaintiff, :

vs. : Case No.

THE UNITED STATES OF AMERICA, : 3:21-cv-1066

et al., :

Defendants. :

- - - - - - - - - - - - - - - - - x

Arlington, Virginia

Thursday, July 28, 2022

Videotaped Deposition of RAUL L. ORTIZ, a witness herein, called for examination by counsel for Plaintiff in the above-entitled matter, pursuant to notice, taken at the offices of Henderson Legal Services, 2300 Wilson Boulevard, Seventh Floor, Arlington, Virginia, at 9:32 a.m. on Thursday, July 28, 2022, and the proceedings being taken down by stenotype by and transcribed by KAREN YOUNG.

APPEARANCES:

On Behalf of the Plaintiff:

JOHN GUARD, ESQ.
JAMES H. PERCIVAL, ESQ.
ANITA J. PATEL, ESQ.
NATALIE CHRISTMAS, ESQ.
Office of the Attorney General
State of Florida
PL-01 The Capitol
Tallahassee, Florida 32399-1050
John.Guard@myfloridalegal.com
James.Percival@myfloridalegal.com
Anita.Patel@myfloridalegal.com
Natalie.Christmas@myfloridalegal.com
(850) 245-0147

On Behalf of the Defendants:

JOSEPH A. DARROW, ESQ.
ERIN RYAN, ESQ.
U.S. Department of Justice
P.O. Box 868, Ben Franklin Station
Washington, D.C. 20044
joseph.a.darrow@usdoj.gov
(202) 598-7537

ALSO PRESENT:

Michelle Tonelli, Esq., DHS
Stephanie Muffett, Esq., CBP
Krishna Sharma, Videographer

40

understanding is there one that -- where ICE agrees to provide transportation from the border?

A. Yes.

Q. All right. Does ICE also agree to transport aliens back to their country of origin as part of the memorandum?

A. Yes.

Q. Okay. And another I guess relationship that ICE and Border Patrol has is that ICE agrees to accept transfer aliens that need to be detained; is that correct?

A. That's correct.

Q. All right. And for -- strike that. Would it be fair to say that Border Patrol often detains aliens that it encountered at the southern border until they can be processed and turned over to ICE?

A. Yes.

Q. Would you agree, Chief Ortiz, that the southern border is currently in crisis?

MR. DARROW: Objection.

A. Yes.

Q. Would you agree, Chief Ortiz, that historic

41

numbers of aliens are illegally entering the United States through the southern border?

MR. DARROW: Objection.

A. Yes.

Q. Would you agree, Chief Ortiz, that unprecedented numbers of aliens are illegally entering the United States right now?

MR. DARROW: Objection.

A. Yes.

Q. Would you agree, Chief Ortiz, that more aliens are going through the southern border than we have seen in the last 20 years?

A. Yes.

Q. Would you agree -- would you agree, Chief Ortiz, the Border Patrol has never had as many encounters with aliens in a physical year as it has had in the last two years?

MR. DARROW: Objection.

A. Yes.

Q. Chief Ortiz, do you expect the historic number of aliens illegally entering the United States to increase in the near term?

59

Prior to January 20th, 2021 when President Biden was inaugurated, from your experience as a Border Patrol agent, did aliens have a favorable view or unfavorable view of Trump's immigration policies?

MR. DARROW: Objection.

A. They had an unfavorable view.

Q. Okay. Would an unfavorable view of Trump's immigration policies kept aliens from coming the border?

MR. DARROW: Objection.

A. Some.

Q. Okay. When President Biden was elected, did the number of aliens trying to illegally enter the United States increase or decrease?

MR. DARROW: Objection.

A. Increase.

Q. Okay. Did caravans restart to the border after President Biden was elected?

MR. DARROW: Objection.

A. Caravans are a recent phenomenon that we've seen over the last couple of years.

Q. Okay. Since President Biden was elected,

to admit them or to repatriate them, right?

MR. DARROW: Objection.

A. Yes.

Q. Now, if you look at the next paragraph in your statement -- first let me ask you this because I forgot to ask it, and you can take a minute if you'd like to take a minute, but are the paragraphs here that -- where it says transcript of U.S. Border Patrol Chief Ortiz, are they accurate?

A. Yes.

Q. Okay. If you look at the last paragraph, the first sentence says, "The smugglers leverage misinformation to mislead people. Some of that information is focused on TPS." First, what is TPS?

A. Temporary protective status.

Q. All right. And what are smugglers doing with information on TPS?

A. They are telling -- or they were telling the migrant population that regardless of when you entered or were processed, that you would be allowed to stay in the United States.

Q. Would you agree, Chief Ortiz, that the

68

aliens who cite favorable immigration policy as a reason to come to the United States are perceiving what actually is happening in the United States?

MR. DARROW: Objection.

A. Yes.

Q. Prior to President Biden being elected, did you review Candidate Biden's immigration proposals?

MR. DARROW: Objection.

THE WITNESS: No.

MR. GUARD: If this is a good time to take a break, we can take a break because I did not write down my tab number on --

THE WITNESS: Yeah.

MR. GUARD: -- this exhibit, and we've been going for a while.

THE WITNESS: That'll work.

MR. GUARD: Okay.

THE VIDEOGRAPHER: We are now off the record at 10:48.

(Recessed at 10:48 a.m.)

(Reconvened at 10:57 a.m.)

THE VIDEOGRAPHER: We're now back on the

On July 16, 2021, Facebook emailed somebody at HHS, stating, "I know our teams met today to better understand the scope of what the White House expects from us on misinformation going forward."

Four days later, on July 20, the White House emailed Facebook, saying, "any way we can get this pulled down?" The White House included a link to an Instagram account purporting to be Anthony Fauci. Less than one minute later, Facebook responded, **"Yep, on it!"**

From: [redacted]@fb.com]
Sent: 7/20/2021 1:24:46 PM
To: Humphrey, Clarke E. EOP/WHO [redacted]@who.eop.gov]; [redacted](IG) [redacted]@fb.com]
CC: Flaherty, Rob R. EOP/WHO [redacted]@who.eop.gov]; [redacted](NIH/NIAID) [E] [redacted]@niaid.nih.gov]
Subject: Re: Deactivating fake Fauci IG?

Yep, on it!

From: Humphrey, Clarke E. EOP/WHO <[redacted]@who.eop.gov>
Date: Tuesday, July 20, 2021 at 1:24 PM
To: [redacted]<[redacted]@fb.com>, [redacted](IG) <davesommer@fb.com>
Cc: Flaherty, Rob R. EOP/WHO <[redacted]@who.eop.gov>, [redacted](NIH/NIAID) [E] <[redacted]@niaid.nih.gov>
Subject: Deactivating fake Fauci IG?

Hi there – any way we can get this pulled down? It is not actually one of ours:

https://www.instagram.com/anthonyfauciofficial/

Clarke Humphrey
Digital Director, COVID-19 Response Team
The White House
[redacted]

From: [redacted] ([redacted]@fb.com]
Sent: 7/19/2021 1:34:04 PM
To: [redacted](HHS/OASH) [redacted]@hhs.gov]
CC: [redacted]@fb.com] [redacted](HHS/OASH) [redacted]@hhs.gov]; [redacted](HHS/OASH) [redacted]@hhs.gov]; [redacted] [redacted]@fb.com]; [redacted] [redacted]@fb.com]
Subject: Re: Message from [redacted]

Hi [redacted]

Thanks so much for getting back to me – really appreciate that.

Adding [redacted] and [redacted] here to liaise with your office to find a time asap which is convenient for you – I'm in Spain right now but hopefully time differences can be navigated so that we speak soon enough.

All best

[redacted]

From: "[redacted](HHS/OASH)" <[redacted]@hhs.gov>
Date: Monday, July 19, 2021 at 3:29 PM
To: [redacted] <[redacted]@fb.com>
Cc: [redacted] <[redacted]@fb.com>, [redacted](HHS/OASH)" <[redacted]@hhs.gov>, [redacted] (HHS/OASH)" <[redacted]@hhs.gov>
Subject: Re: Message from [redacted]

Hi [redacted]

Thanks for reaching out and for sharing your concerns. I know the last few days have been challenging. I'd be happy to speak directly about how we move forward. Let me know the best way to schedule some time later this week and we'll make it happen.

Best wishes and will talk soon,
[redacted]

--

[redacted]
U.S. Surgeon General
Vice Admiral, U.S. Public Health Service

From: [redacted] <[redacted]@fb.com>
Sent: Friday, July 16, 2021 5:43 PM
To: [redacted] (HHS/OASH) <[redacted]@hhs.gov>
Cc: [redacted] <[redacted]@fb.com>
Subject: Message from [redacted]

Dear [redacted]

Reaching out after what has transpired over the past few days following the publication of the misinformation advisory, and culminating today in the President's remarks about us. I know our teams met today to better understand the scope of what the White House expects from us on misinformation going forward.

In our previous conversations I've appreciated the way you and your team have approached our engagement, and we have worked hard to meet the moment — we've dedicated enormous time and resources to fighting this pandemic and consider ourselves to be partners in fighting the same battle. Certainly we understand (and have understood for some time) that there is disagreement on some of the policies governing our approach and how they are being enforced – even as your team has acknowledged the unprecedented scale of our efforts to provide authoritative information to millions of Americans and to help them get vaccinated. But I thought the way we were singled out over the past few days has been both surprising and misleading, and I believe unproductive to our joint efforts too.

I would appreciate the opportunity to speak directly to discuss a path forward with you and how we can continue to work toward what I sincerely believe are shared goals.

Yours
[redacted]

The Intercept_

TRUTH COPS

Leaked Documents Outline DHS's Plans to Police Disinformation

The U.S. Department of Homeland Security logo is seen displayed on a smartphone. Photo Illustration: Rafael Henrique/SOPA Images/LightRocket via Getty Images

Ken Klippenstein, Lee Fang

October 31 2022, 5:00 a.m.

The Department of Homeland Security is quietly broadening its efforts to curb speech it considers dangerous, an investigation by The Intercept has found. Years of internal DHS memos, emails, and documents — obtained via leaks and an ongoing lawsuit, as well as public documents — illustrate an expansive effort by the agency to influence tech platforms.

The work, much of which remains unknown to the American public, came into clearer view earlier this year when DHS announced a new "Disinformation Governance Board": a panel designed to police misinformation (false information spread unintentionally), disinformation (false information spread intentionally), and malinformation (factual information shared, typically out of context, with harmful intent) that allegedly threatens U.S. interests. While the board was widely ridiculed, immediately scaled back, and then shut down within a few months, other initiatives are underway as DHS pivots to monitoring social media now that its original mandate — the war on terror — has been wound down.

Behind closed doors, and through pressure on private platforms, the U.S. government has used its power to try to shape online discourse. According to meeting minutes and other records appended to a lawsuit filed by Missouri Attorney General Eric Schmitt, a Republican who is also running for Senate, discussions have ranged from the scale and scope of government intervention in online discourse to the mechanics of streamlining takedown requests for false or intentionally misleading information.

"Platforms have got to get comfortable with gov't. It's really interesting how hesitant they remain," Microsoft executive Matt Masterson, a former DHS official, texted Jen Easterly, a DHS director, in February.

Key Takeaways

- Though DHS shuttered its controversial Disinformation Governance Board, a strategic document reveals the underlying work is ongoing.
- DHS plans to target inaccurate information on "the origins of

In a March meeting, Laura Dehmlow, an FBI official, warned that the threat of subversive information on social media could undermine support for the U.S. government. Dehmlow, according to notes of the discussion attended by senior executives from Twitter and JPMorgan Chase, stressed that "we need a media infrastructure that is held accountable."

the COVID-19 pandemic and the efficacy of COVID-19 vaccines, racial justice, U.S. withdrawal from Afghanistan, and the nature of U.S. support to Ukraine."

- Facebook created a special portal for DHS and government partners to report disinformation directly.

"We do not coordinate with other entities when making content moderation decisions, and we independently evaluate content in line with the Twitter Rules," a spokesperson for Twitter wrote in a statement to The Intercept.

There is also a formalized process for government officials to directly flag content on Facebook or Instagram and request that it be throttled or suppressed through a special Facebook portal that requires a government or law enforcement email to use. At the time of writing, the "content request system" at facebook.com/xtakedowns/login is still live. DHS and Meta, the parent company of Facebook, did not respond to a request for comment. The FBI declined to comment.

DHS's mission to fight disinformation, stemming from concerns around Russian influence in the 2016 presidential election, began taking shape during the 2020 election and over efforts to shape discussions around vaccine policy during the coronavirus pandemic. Documents collected by The Intercept from a variety of sources, including current officials

and publicly available reports, reveal the evolution of more active measures by DHS.

According to a draft copy of DHS's Quadrennial Homeland Security Review, DHS's capstone report outlining the department's strategy and priorities in the coming years, the department plans to target "inaccurate information" on a wide range of topics, including "the origins of the COVID-19 pandemic and the efficacy of COVID-19 vaccines, racial justice, U.S. withdrawal from Afghanistan, and the nature of U.S. support to Ukraine."

"The challenge is particularly acute in marginalized communities," the report states, "which are often the targets of false or misleading information, such as false information on voting procedures targeting people of color."

The inclusion of the 2021 U.S. withdrawal from Afghanistan is particularly noteworthy, given that House Republicans, should they take the majority in the midterms, have vowed to investigate. "This makes Benghazi look like a much smaller issue," said Rep. Mike Johnson, R-La., a member of the Armed Services Committee, adding that finding answers "will be a top priority."

How disinformation is defined by the government has not been clearly articulated, and the inherently subjective nature of what constitutes disinformation provides a broad opening for DHS officials to make politically motivated determinations about what constitutes dangerous speech.

DHS justifies these goals — which have expanded far beyond its original purview on foreign threats to encompass disinformation originat-

The inherently subjective nature of what constitutes

ing domestically — by claiming that terrorist threats can be "exacerbated by misinformation and disinformation spread online." But the laudable goal of protecting Americans from danger has often been used to conceal political maneuvering. In 2004, for instance, DHS officials faced pressure from the George W. Bush administration to heighten the national threat level for terrorism, in a bid to influence voters prior to the election, according to former DHS Secretary Tom Ridge. U.S. officials have routinely lied about an array of issues, from the causes of its wars in Vietnam and Iraq to their more recent obfuscation around the role of the National Institutes of Health in funding the Wuhan Institute of Virology's coronavirus research.

disinformation provides a broad opening for DHS officials to make politically motivated determinations about what constitutes dangerous speech.

That track record has not prevented the U.S. government from seeking to become arbiters of what constitutes false or dangerous information on inherently political topics. Earlier this year, Republican Gov. Ron DeSantis signed a law known by supporters as the "Stop WOKE Act," which bans private employers from workplace trainings asserting an individual's moral character is privileged or oppressed based on his or her race, color, sex, or national origin. The law, critics charged, amounted to a broad suppression of speech deemed offensive. The Foundation for Individual Rights and Expression, or FIRE, has since filed a lawsuit against DeSantis, alleging "unconstitutional censorship." A federal judge temporarily blocked parts of the Stop WOKE Act, ruling that the law had violated workers' First Amendment rights.

"Florida's legislators may well find plaintiffs' speech 'repugnant.' But under our constitutional scheme, the 'remedy' for repugnant speech is more speech, not enforced silence," wrote Judge Mark Walker, in a colorful opinion castigating the law.

The extent to which the DHS initiatives affect Americans' daily social feeds is unclear. During the 2020 election, the government flagged numerous posts as suspicious, many of which were then taken down, documents cited in the Missouri attorney general's lawsuit disclosed. And a 2021 report by the Election Integrity Partnership at Stanford University found that of nearly 4,800 flagged items, technology platforms took action on 35 percent — either removing, labeling, or soft-blocking speech, meaning the users were only able to view content after bypassing a warning screen. The research was done "in consultation with CISA," the Cybersecurity and Infrastructure Security Agency.

Prior to the 2020 election, tech companies including Twitter, Facebook, Reddit, Discord, Wikipedia, Microsoft, LinkedIn, and Verizon Media met on a monthly basis with the FBI, CISA, and other government representatives. According to NBC News, the meetings were part of an initiative, still ongoing, between the private sector and government to discuss how firms would handle misinformation during the election.

Homeland Security Secretary Kirstjen Nielsen stands alongside President Donald Trump as he speaks prior to signing the Cybersecurity and Infrastructure Security Agency Act in the Oval Office of the White House in Washington, D.C., on Nov. 16, 2018. Photo: Saul Loeb/AFP via Getty Images

The stepped up counter-disinformation effort began in 2018 following high-profile hacking incidents of U.S. firms, when Congress passed and President Donald Trump signed the Cybersecurity and Infrastructure Security Agency Act, forming a new wing of DHS devoted to protecting critical national infrastructure. An August 2022 report by the DHS Office of Inspector General sketches the rapidly accelerating move toward policing disinformation.

From the outset, CISA boasted of an "evolved mission" to monitor social media discussions while "routing disinformation concerns" to private sector platforms.

In 2018, then-DHS Secretary Kirstjen Nielsen created the Countering Foreign Influence Task Force to respond to election disinformation. The task force, which included members of CISA as well as its Office of Intelligence and Analysis, generated "threat intelligence" about the election and notified social media platforms and law enforcement. At the same time, DHS began notifying social media companies about voting-related disinformation appearing on social platforms.

In 2019, DHS created a separate entity called the Foreign Influence and Interference Branch to generate more detailed intelligence about disinformation, the inspector general report shows. That year, its staff grew to include 15 full- and part-time staff dedicated to disinformation analysis. In 2020, the disinformation focus expanded to include Covid-19, according to a Homeland Threat Assessment issued by Acting Secretary Chad Wolf.

This apparatus had a dry run during the 2020 election, when CISA began working with other

Key Takeaways, Cont'd.

- The work is primarily done by CISA, a DHS sub-agency tasked with protecting critical national infrastructure.
- DHS, the FBI, and several media entities are having biweekly meetings as recently as August.
- DHS considered countering disinformation relating to content that undermines trust in financial systems and courts.
- The FBI agent who primed social media platforms to take down the Hunter Biden laptop story continued to have a role in DHS policy discussions.

members of the U.S. intelligence community. Office of Intelligence and Analysis personnel attended "weekly teleconferences to coordinate Intelligence Community activities to counter election-related disinformation." According to the IG report, meetings have continued to take place every two weeks since the elections.

Emails between DHS officials, Twitter, and the Center for Internet Security outline the process for such takedown requests during the period leading up to November 2020. Meeting notes show that the tech platforms would be called upon to "process reports and provide timely responses, to include the removal of reported misinformation from the platform where possible." In practice, this often meant state election officials sent examples of potential forms of disinformation to CISA, which would then forward them on to social media companies for a response.

Under President Joe Biden, the shifting focus on disinformation has continued. In January 2021, CISA replaced the Countering Foreign Influence Task force with the "Misinformation, Disinformation and Malinformation" team, which was created "to promote more flexibility to focus on general MDM." By now, the scope of the effort had expanded beyond disinformation produced by foreign governments to include domestic versions. The MDM team, according to one CISA official quoted in the IG report, "counters all types of disinformation, to be responsive to current events."

Jen Easterly, Biden's appointed director of CISA, swiftly made it clear that she would continue to shift resources in the agency to combat the spread of dangerous forms of information on social media. "One could argue we're in the business of critical infrastructure, and the most critical infrastructure is our cognitive infrastructure, so building that resilience to misinformation and disinformation, I think, is incredibly important," said Easterly, speaking at a conference in November 2021.

CISA's domain has gradually expanded to encompass more subjects it believes amount to critical infrastructure. Last year, The Intercept reported on the existence of a series of DHS field intelligence reports warning of attacks on cell towers, which it has tied to conspiracy theorists who believe 5G towers spread Covid-19. One intelligence report pointed out that these conspiracy theories "are inciting attacks against the communications infrastructure."

CISA has defended its burgeoning social media monitoring authorities, stating that "once CISA notified a social media platform of disinformation, the social media platform could independently decide whether to remove or modify the post." But, as documents revealed by the Missouri lawsuit show, CISA's goal is to make platforms more responsive to their suggestions.

In late February, Easterly texted with Matthew Masterson, a representative at Microsoft who formerly worked at CISA, that she is "trying to get us in a place where Fed can work with platforms to better understand mis/dis trends so relevant agencies can try to prebunk/debunk as useful."

Meeting records of the CISA Cybersecurity Advisory Committee, the main subcommittee that handles disinformation policy at CISA, show a constant effort to expand the scope of the agency's tools to foil disinformation.

In June, the same DHS advisory committee of CISA — which includes Twitter head of legal policy, trust, and safety Vijaya Gadde and University of Washington professor Kate Starbird — drafted a report to the CISA director calling for an expansive role for the agency in shaping the "information ecosystem." The report called on the agency to closely monitor "social media platforms of all sizes, mainstream media, cable news, hyper partisan media, talk radio and other online resources." They argued that the agency needed to take steps to halt the "spread of

false and misleading information," with a focus on information that undermines "key democratic institutions, such as the courts, or by other sectors such as the financial system, or public health measures."

To accomplish these broad goals, the report said, CISA should invest in external research to evaluate the "efficacy of interventions," specifically with research looking at how alleged disinformation can be countered and how quickly messages spread. Geoff Hale, the director of the Election Security Initiative at CISA, recommended the use of third-party information-sharing nonprofits as a "clearing house for information to avoid the appearance of government propaganda."

Last Thursday, immediately following billionaire Elon Musk's completed acquisition of Twitter, Gadde was terminated from the company.

Alejandro Mayorkas, secretary of the Department of Homeland Security, speaks during a new conference in Brownsville, Texas, on Aug. 12, 2021. Photo: Veronica G. Cardenas/Bloomberg via Getty Images

The Biden administration, however, did take a stab at making part of this infrastructure public in April 2022, with the announcement of the Disinformation Governance Board. The exact functions of the board, and how it would accomplish its goal of defining and combating MDM, were never made clear.

The board faced immediate backlash across the political spectrum. "Who among us thinks the government should add to its work list the job of determining what is true and what is disinformation? And who thinks the government is capable of telling the truth?" wrote Politico media critic Jack Shafer. "Our government produces lies and disinformation at industrial scale and always has. It overclassifies vital information to block its own citizens from becoming any the wiser. It pays thousands of press aides to play hide the salami with facts."

DHS Secretary Alejandro Mayorkas alluded to broad scope of the agency's disinformation effort when he told the Senate Homeland Security and Governmental Affairs Committee that the role of the board — which by that point had been downgraded to a "working group" — is to "actually develop guidelines, standards, guardrails to ensure that the work that has been ongoing for nearly 10 years does not infringe on people's free speech rights, rights of privacy, civil rights, and civil liberties."

"It was quite disconcerting, frankly," he added, "that the disinformation work that was well underway for many years across different independent administrations was not guided by guardrails."

DHS eventually scrapped the Disinformation Governance Board in August. While free speech advocates cheered the dissolution of the board, other government efforts to root out disinformation have not only continued but expanded to encompass additional DHS sub-agencies like Customs and Border Protection, which "determines whether infor-

mation about the component spread through social media platforms like Facebook and Twitter is accurate." Other agencies such as Immigration and Customs Enforcement, the Science and Technology Directorate (whose responsibilities include "determining whether social media accounts were bots or humans and how the mayhem caused by bots affects behavior"), and the Secret Service have also expanded their purview to include disinformation, according to the inspector general report.

The draft copy of DHS's 2022 Quadrennial Homeland Security Review reviewed by The Intercept also confirms that DHS views the issue of tackling disinformation and misinformation as a growing portion of its core duties. While "counterterrorism remains the first and most important mission of the Department," it notes, the agency's "work on these missions is evolving and dynamic" and must now adapt to terror threats "exacerbated by misinformation and disinformation spread online" including by "domestic violent extremists."

To accomplish this, the draft quadrennial review calls for DHS to "leverage advanced data analytics technology and hire and train skilled specialists to better understand how threat actors use online platforms to introduce and spread toxic narratives intended to inspire or incite violence, as well as work with NGOs and other parts of civil society to build resilience to the impacts of false information."

The broad definition of "threat actors" posing risks to vaguely defined critical infrastructure — an area as broad as trust in government, public health, elections, and financial markets — has concerned civil libertarians. "No matter your political allegiances, all of us have good reason to be concerned about government efforts to pressure private social media platforms into reaching the government's preferred decisions about what content we can see online," said Adam Goldstein, the vice president of research at FIRE.

"Any governmental requests to social media platforms to review or remove certain content," he added, "should be made with extreme transparency."

A tweet about the FBI is displayed during a Senate Homeland Security and Governmental Affairs Committee hearing regarding social media's impact on homeland security on Capitol Hill in Washington, D.C., on Sept. 14, 2022. Photo: Stefani Reynolds/AFP via Getty Images

DHS's expansion into misinformation, disinformation, and malinformation represents an important strategic retooling for the agency, which was founded in 2002 in response to the 9/11 attacks as a bulwark to coordinate intelligence and security operations across the government. At the same time, the FBI deployed thousands of agents to focus on counterterrorism efforts, through building informant networks and intelligence operations designed to prevent similar attacks.

But traditional forms of terrorism, posed by groups like Al Qaeda, evolved with the rise of social media, with groups like the Islamic State using platforms such as Facebook to recruit and radicalize new members. After initial reluctance, social media giants worked closely with the FBI and DHS to help monitor and remove ISIS-affiliated accounts.

FBI Director James Comey told the Senate Intelligence Committee that law enforcement agencies needed to rapidly "adapt and confront the challenges" posed by terror networks that had proven adept at tapping into social media. Intelligence agencies backed new startups designed to monitor the vast flow of information across social networks to better understand emerging narratives and risks.

"The Department has not been fully reauthorized since its inception over fifteen years ago," the Senate Homeland Security Committee warned in 2018. "As the threat landscape continues to evolve, the Department adjusted its organization and activities to address emerging threats and protect the U.S. homeland. This evolution of the Department's duties and organization, including the structure and operations of the DHS Headquarters, has never been codified in statute."

The subsequent military defeat of ISIS forces in Syria and Iraq, along with the withdrawal from Afghanistan, left the homeland security apparatus without a target. Meanwhile, a new threat entered the discourse. The allegation that Russian agents had seeded disinformation on Facebook that tipped the 2016 election toward Donald Trump resulted in the FBI forming the Foreign Influence Task Force, a team devoted to preventing foreign meddling in American elections.

According to DHS meeting minutes from March, the FBI's Foreign Influence Task Force this year includes 80 individuals focused on curbing "subversive data utilized to drive a wedge between the populace and the government."

"The Department will spearhead initiatives to raise awareness of disinformation campaigns targeting communities in the United States, providing citizens the tools necessary to identify and halt the spread of information operations intended to promote radicalization to violent extremism or mobilization to violence," DHS Acting Secretary Kevin McAleenan said in a September 2019 strategic framework.

DHS also began to broaden its watch to include a wide array of domestic actors viewed as potential sources of radicalization and upheaval. An FBI official interviewed by The Intercept described how, in the summer of 2020, amid the George Floyd protests, he was reassigned from his normal job of countering foreign intelligence services to monitoring American social media accounts. (The official, not authorized to speak publicly, described the reassignment on condition of anonymity.)

And a June 2020 memo bearing the subject line "Actions to Address the Threat Posed by Domestic Terrorists and Other Domestic Extremists" prepared by DHS headquarters for Wolf, Trump's acting DHS secretary, delineates plans to "expand information sharing with the tech sector" in order to "identify disinformation campaigns used by DT [domestic terrorism] actors to incite violence against infrastructure, ethnic, racial or religious groups, or individuals." The memo outlines plans to work with private tech sector partners to share unclassified DHS intelligence on "DT actors and their tactics" so that platforms can "move effectively

use their own tools to enforce user agreements/terms of service and remove DT content."

Biden also prioritized such efforts. Last year, the Biden administration released the first National Strategy for Countering Domestic Terrorism. The strategy identified a "broader priority: enhancing faith in government and addressing the extreme polarization, fueled by a crisis of disinformation and misinformation often channeled through social media platforms, which can tear Americans apart and lead some to violence."

"We are working with like-minded governments, civil society, and the technology sector to address terrorist and violent extremist content online, including through innovative research collaborations," the strategy document continued, adding that the administration was "addressing the crisis of disinformation and misinformation, often channeled through social and other media platforms, that can fuel extreme polarization and lead some individuals to violence."

Last year, a top FBI counterterrorism official came under fire when she falsely denied to Congress that the FBI monitors Americans' social media and had therefore missed threats leading up to the attack on the U.S. Capitol on January 6, 2021. In fact, the FBI has spent millions of dollars on social media tracking software like Babel X and Dataminr. According to the bureau's official guidelines, authorized activities include "proactively surfing the Internet to find publicly accessible websites and services through which recruitment by terrorist organizations and promotion of terrorist crimes is openly taking place."

Another FBI official, a joint terrorism task force officer, described to The Intercept being reassigned this year from the bureau's international terrorism division, where they had primarily worked on cases involving Al Qaeda and the Islamic State group, to the domestic terrorism division to investigate Americans, including anti-government individuals such as racially motivated violent extremists, sovereign citizens,

militias, and anarchists. They work on an undercover basis online to penetrate social networking chat rooms, online forums, and blogs to detect, enter, dismantle, and disrupt existing and emerging terrorist organizations via online forums, chat rooms, bulletin boards, blogs, websites, and social networking, said the FBI official, who did not have permission to speak on the record.

The Privacy Act of 1974, enacted following the Watergate scandal, restricts government data collection of Americans exercising their First Amendment rights, a safeguard that civil liberty groups have argued limits the ability of DHS and the FBI to engage in surveillance of American political speech expressed on social media. The statute, however, maintains exemptions for information collected for the purposes of a criminal or law enforcement investigation.

"There are no specific legal constraints on the FBI's use of social media," Faiza Patel, senior director of the Brennan Center for Justice's liberty and national security program told The Intercept. "The attorney general guidelines permit agents to look at social media before there is any investigation at all. So it's kind of a Wild West out there."

The first FBI official, whom The Intercept interviewed in 2020 amid the George Floyd riots, lamented the drift toward warrantless monitoring of Americans saying, "Man, I don't even know what's legal anymore."

In retrospect, the New York Post reporting on the contents of Hunter Biden's laptop ahead of the 2020 election provides an elucidating case study of how this works in an increasingly partisan environment.

Much of the public ignored the reporting or assumed it was false, as over 50 former intelligence officials charged that the laptop story was a creation of a "Russian disinformation" campaign. The mainstream media was primed by allegations of election interference in 2016 — and, to be sure, Trump did attempt to use the laptop to disrupt the Biden cam-

paign. Twitter ended up banning links to the New York Post's report on the contents of the laptop during the crucial weeks leading up to the election. Facebook also throttled users' ability to view the story.

In recent months, a clearer picture of the government's influence has emerged.

In an appearance on Joe Rogan's podcast in August, Meta CEO Mark Zuckerberg revealed that Facebook had limited sharing of the New York Post's reporting after a conversation with the FBI. "The background here is that the FBI came to us — some folks on our team — and was like, 'Hey, just so you know, you should be on high alert that there was a lot of Russian propaganda in the 2016 election,'" Zuckerberg told Rogan. The FBI told them, Zuckerberg said, that "'We have it on notice that basically there's about to be some kind of dump.'" When the Post's story came out in October 2020, Facebook thought it "fit that pattern" the FBI had told them to look out for.

Zuckerberg said he regretted the decision, as did Jack Dorsey, the CEO of Twitter at the time. Despite claims that the laptop's contents were forged, the Washington Post confirmed that at least some of the emails on the laptop were authentic. The New York Times authenticated emails from the laptop — many of which were cited in the original New York Post reporting from October 2020 — that prosecutors have examined as part of the Justice Department's probe into whether the president's son violated the law on a range of issues, including money laundering, tax-related offenses, and foreign lobbying registration.

Documents filed in federal court as part of a lawsuit by the attorneys general of Missouri and Louisiana add a layer of new detail to Zuckerberg's anecdote, revealing that officials leading the push to expand the government's reach into disinformation also played a quiet role in shaping the decisions of social media giants around the New York Post story.

According to records filed in federal court, two previously unnamed FBI agents — Elvis Chan, an FBI special agent in the San Francisco field office, and Dehmlow, the section chief of the FBI's Foreign Influence Task Force — were involved in high-level communications that allegedly "led to Facebook's suppression" of the Post's reporting.

The Hunter Biden laptop story was only the most high-profile example of law enforcement agencies pressuring technology firms. In many cases, the Facebook and Twitter accounts flagged by DHS or its partners as dangerous forms of disinformation or potential foreign influence were clearly parody accounts or accounts with virtually no followers or influence.

In May, Missouri Attorney General Eric Schmitt took the lead in filing a lawsuit to combat what he views as sweeping efforts by the Biden administration to pressure social media companies to moderate certain forms of content appearing on their platforms.

The suit alleges governmentwide efforts to censor certain stories, especially ones related to the pandemic. It also names multiple agencies across the government that have participated in efforts to monitor speech and "open collusion" between the administration and social media companies. It identifies, for example, emails between officials from the National Institutes of Health, including Dr. Anthony Fauci, and

Zuckerberg at the beginning of the pandemic, and reveals ongoing discussions between senior Biden administration officials with Meta executives on developing content moderation policies on a range of issues, including issues related to elections and vaccines.

Attorneys for the Biden administration have responded in court by claiming that the plaintiffs lack standing and that social media firms pursued content moderation policies on their own volition, without any "coercive" influence from the government. On October 21, the judge presiding over the case granted the attorneys general permission to depose Fauci, CISA officials, and communication specialists from the White House.

While the lawsuit has a definite partisan slant, pointing the finger at the Biden administration for allegedly seeking to control private speech, many of the subpoenas request information that spans into the Trump era and provides a window into the absurdity of the ongoing effort.

"There is growing evidence that the legislative and executive branch officials are using social media companies to engage in censorship by surrogate," said Jonathan Turley, a professor of law at George Washington University, who has written about the lawsuit. "It is axiomatic that the government cannot do indirectly what it is prohibited from doing directly. If government officials are directing or facilitating such censorship, it raises serious First Amendment questions."

During the 2020 election, the Department of Homeland Security, in an email to an official at Twitter, forwarded information about a potential threat to critical U.S. infrastructure, citing FBI warnings, in this case about an account that could imperil election system integrity.

The Twitter user in question had 56 followers, along with a bio that read "dm us your weed store locations (hoes be mad, but this is a par-

ody account)," under a banner image of Blucifer, the 32-foot-tall demonic horse sculpture featured at the entrance of the Denver International Airport.

"We are not sure if there's any action that can be taken, but we wanted to flag them for consideration," wrote a state official on the email thread, forwarding on other examples of accounts that could be confused with official government entities. The Twitter representative responded: "We will escalate. Thank you."

Each email in the chain carried a disclaimer that the agency "neither has nor seeks the ability to remove or edit what information is made available on social media platforms."

That tagline, however, concerns free speech advocates, who note that the agency is attempting to make an end run around the First Amendment by exerting continual pressure on private sector social media firms. "When the government suggests things, it's not too hard to pull off the velvet glove, and you get the mail fist," said Adam Candeub, a professor of law at Michigan State University. "And I would consider such actions, especially when it's bureaucratized, as essentially state action and government collusion with the platforms."

"If a foreign authoritarian government sent these messages," noted Nadine Strossen, the former president of the American Civil Liberties Union, "there is no doubt we would call it censorship."

Correction: November 2, 2022

Due to an editing error, after publication on November 1, the piece briefly stated that a DHS official had texted a Microsoft official that "Platforms have got to get comfortable with gov't." In fact, it was the other way around: Microsoft executive Matt Masterson, a former DHS official, texted Jen Easterly, a DHS director.

Post-Hearing Questions for the Record
Submitted to the Honorable Alejandro N. Mayorkas
From Senator James Lankford

Threats to the Homeland
November 17, 2022

Question: On March 17, 2022, DHS held a briefing with staff from the authorizing committees of Congress. During that briefing, a briefer from the DHS Office of Intelligence & Analysis (I&A) shared with the authorizing committees that 10,000s of migrants are already located south of the border in Mexico and could surge to the U.S./Mexico border within hours or days once Title 42 is lifted; 100,000s of migrants are currently located throughout central and south Mexico and could surge to the U.S./Mexico border within days to weeks of Title 42's termination; and millions of migrants and displaced persons were located in south Mexico and the Northern Triangle and could make their way to the U.S./Mexico border within weeks to a month of Title 42's termination. After this briefing, DHS no longer publicly relied on the I&A numbers and instead relied on a series of projections developed by the Office of Immigration Statistics, which stated that 18,000 migrants would cross the border per day after Title 42 was terminated.

In the Department's response to Question for the Record 21 from the HSGAC hearing entitled "Securing and Ensuring Order on the Southwest Border" (May 5, 2022), Acting Assistant Secretary for Border and Immigration Policy Blas Nunez-Neto stated: "The metric of 18,000 encounters per day was designed for planning purposes to describe a scenario in which termination of Title 42 on a target date would cause encounters of noncitizens from numerous countries to surge to levels beyond the highest ever observed. It does not reflect the number of encounters CBP anticipates seeing."

What are DHS's actual projections for the migration surge that will occur when Title 42 is terminated on December 21, 2022? Please share at your earliest convenience all intelligence products and any other documents that underlie your response to this question.

Response: The U.S. Department of Homeland Security (DHS) would be pleased to coordinate with your staff to schedule a briefing regarding projections for when the U.S. Department of Health and Human Services' (HHS) Centers for Disease Control and Prevention's Title 42 public health Order is no longer being implemented.

Question#:	2
Topic:	Favorable Policies
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: Chief of U.S. Border Patrol Raul Ortiz recently admitted under oath that the migrants who have crossed the border have done so because they view the President's immigration policies as "favorable" and "perceive that they will be able to enter and remain in the United States."

Do you agree with Chief Ortiz's sworn testimony? Please fully explain.

Chief Ortiz testified under oath in a recent deposition that migrant flows increase "when there are no consequences" and "if migrant populations are told that there's a potential that they may be released." Do you agree with his testimony? Please fully explain.

Response: As stated throughout the DHS Southwest Border Security and Preparedness plan, the Department is committed to administering consequences for unlawful entry, including removal, detention, and prosecution.

To this end, DHS is maximizing the use of expedited removal for populations where removal is possible or likely and working to streamline expedited removal processes across relevant federal agencies to be able to quickly remove those who do not claim fear or who receive a negative credible fear finding, absent another lawful basis to remain in the United States. Increased use of expedited removal is a means of efficiently removing those with no lawful basis to remain in the United States, consistent with core due process protection. Those removed pursuant to expedited removal also face a five-year ban on admission from the date of removal and potential criminal prosecution if they seek to unlawfully re-enter.

DHS is increasing the availability of interview spaces and U.S. Citizenship and Immigration Services (USCIS) officers to conduct credible fear interviews and working with partner countries throughout the hemisphere to significantly improve our ability to quickly remove and repatriate individuals with final orders of removal.

Individuals in expedited removal who establish a credible fear of persecution or torture generally are referred to an immigration court for full consideration of their applications for asylum and related protection, which can be a years-long process. Under the Asylum Processing Interim Final Rule (IFR) implemented on May 31, 2022, USCIS may instead retain jurisdiction over these cases and adjudicate the asylum application in the first instance. If USCIS does not grant asylum, the case is referred to immigration court for streamlined removal proceedings under the rule. The process provided for in the IFR allows DHS and the U.S. Department of Justice (DOJ) to conclude asylum cases processed under the rule in months instead of years, meaning that those deemed ineligible for asylum and ordered removed can be removed more quickly.

Question#:	3
Topic:	Detention Expansion
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: Is DHS making every effort to expand detention of the migrants who are crossing the southern border? Please explain how.

Response: As stated throughout the DHS Southwest Border Security and Preparedness plan, the Department is committed to administering consequences for unlawful entry, including removal, detention, and prosecution. However, U.S. Immigration and Customs Enforcement (ICE) has limited bedspace compared to the number of noncitizens seeking to cross the border. Additionally, at present, ICE's access to its inventory of bedspace is limited by various court orders and settlement agreements affecting the intake of noncitizens, an increase in detention facility contract terminations, and the ongoing COVID-19 pandemic, which impacts facility staffing and population levels. However, ICE will continue to judiciously use its detention resources to detain noncitizens when required by law or when an ICE officer determines during the custody determination process that a noncitizen poses a public safety or flight risk that cannot be mitigated.

Question#:	4
Topic:	Magnus Press Conference
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: You have previously stated that the images of the Horse Patrol agents in Del Rio "horrified us in terms of what they suggest and what they conjure up" and "Our nation saw horrifying images that do not reflect who we are. We know that those images painfully conjured up the worst elements of our nation's ongoing battle against systemic racism." The Heritage Foundation uncovered emails from FOIA litigation finding that a press officer informed you that the photographer of those pictures stated that he and his colleagues "never saw agents whipping anyone."

Never in the Department's history has a press conference been held to discuss proposed disciplinary actions against a sworn law enforcement officer. As you are aware, CBP Commissioner Chris Magnus held a press conference to discuss disciplinary actions against 4 Border Patrol agents in light of the Del Rio photographs. As you likely also may be aware, the disciplinary process at that time had not yet been completed.

Do you believe that Commissioner Magnus' press conference was improper? Why or why not?

Were you or any other DHS Headquarters officials aware that this press conference was going to occur?

If so, which DHS components were involved and what was the extent of their involvement in the decision-making around this press conference?

Response: This is a mischaracterization of Secretary Mayorkas's direct response to a reporter's question at the White House Press Conference. His full quote stated:

> SECRETARY MAYORKAS: *First of all, the images, as I expressed earlier—the images horrified us in terms of what they suggest and what they conjure up, in terms of not only our nation's history, but, unfortunately, the fact that that page of history has not been turned entirely. And that means that there is much work to do, and we are very focused on doing it.*
>
> *But I will not prejudge the facts. I do not, in any way, want to impair the integrity of the investigative process. We have investigators who are looking at it independently. They will draw their conclusions according to their standard operating procedures, and then the results of that investigation will be determined by the facts that are adduced.*
>
> As the quote makes clear, Secretary Mayorkas explicitly declined to prejudge any conclusion of what did or did not occur and judiciously deferred to the independent investigation that was underway and the conclusions it would reach.

Question#:	4
Topic:	Magnus Press Conference
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

That investigation concluded that there were failures at multiple levels of the agency, a lack of appropriate policies and training, and unprofessional and dangerous behavior by several individual Agents. The investigation included over 30 interviews and the review of numerous videos, photographs, and documents related to the incident. Those interviewed included U.S. Border Patrol (USBP) management officials, USBP Agents, Texas Department of Public Safety troopers, and others who were present during the incident, as well as USBP personnel associated with the Horse Patrol Program. The investigation also included the review of court filings by the migrants involved in this incident and videos and photos of the incident as captured by U.S. Customs and Border Protection (CBP) Air and Marine Operations and members of the media who were present during the incident.

The full 511-page Report of Investigation has been made public, consistent with our commitment to transparency.

Question#:	5
Topic:	Venezuelan Migrants
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: It is my understanding that the new DHS Venezuela Program is contingent on Title 42's continued operation and that, once Title 42 goes away, the Venezuelan nationals who have been expelled will be allowed to enter into the country and be processed under Title 8, likely following the same catch-and-release policies that the Biden Administration has employed prior to this program.

Has DHS produced any intelligence reports regarding how many Venezuelan nationals are between the Darien Gap and the U.S./Mexico border (as of December 21, 2022 or earlier)? If so, please share such reports with the Committee.

What is the plan to stop the flow of migrants from Venezuela when Title 42 ends?

Response: The United States and the Government of Mexico are both encouraged by the significant reduction in migration from Cuba, Haiti, Nicaragua, and Venezuela (CHNV) that has resulted from the processes implemented as of January 5, 2023, which combined a streamlined opportunity for eligible individuals to come to the United States via a lawful pathway, with consequences for those who do not avail themselves of this lawful pathway and instead cross the Southwest Border without authorization. Both governments have been discussing how to continue to implement these processes once Title 42 is lifted and DHS returns to processing all noncitizens at the border under Title 8 authority. However, as of mid-February 2023, there is no agreement to effectuate Title 8 returns of these nationalities to Mexico. As a reminder, our ability to return people to Mexico under the CHNV process is contingent on Mexico's independent decision to accept these returns, which Mexico has indicated depends on our continuing ability and willingness to parole CHNV nationals pursuant to the process put in place.

DHS would be pleased to work with your office to schedule a briefing on reporting relating to flows through the Darien Gap.

Question#:	6
Topic:	Pregnant Minors
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: Last week, HHS released an updated guidance for processing pregnant unaccompanied minors, with the focus of the guidance being on promoting access to abortion for pregnant minors. I am extremely concerned that despite historic numbers of migrants, including children flooding across the border, this administration remains focused on prioritizing their access to abortion. Instead of taking steps to solve the problems at the boarder that would actually prevent and appropriately respond to the sexual violence that migrants experience on the dangerous journey to the US border, this administration is responding by pushing pregnant minors toward abortions.

To what extent did DHS collaborate with HHS in the drafting of ORR's Field Guidance #21, which promotes abortion and abortion tourism for unaccompanied minors in Federal care?

Response: DHS did not collaborate with HHS on the drafting of Field Guidance #21.

Question: Has DHS ever transported an unaccompanied minor to a different sector for the purposes of avoiding abortion laws in the sector in which they were interdicted?

Response: No. Both the Homeland Security Act of 2002 (HSA) and the Trafficking Victims Protection Reauthorization Act of 2008 (TVPRA) transferred the authority to care for unaccompanied children (UC) to HHS. DHS generally transfers UCs into the care and custody of the HHS Office of Refugee Resettlement (ORR) pursuant to the TVPRA and HSA. Placement designations are determined by HHS; therefore, the location to which UCs are transferred is determined by HHS.

Question: Has DHS ever done so knowing that the unaccompanied minor was pregnant?

Has DHS ever done so knowing that the unaccompanied minor was a victim of a sexual-based crime and at risk of becoming pregnant?

Response: No. As stated in the above response, DHS generally transfers UCs into the care and custody of ORR, pursuant to the TVPRA and HSA. Placement designations are determined by HHS; therefore, the location to which UCs are transferred is determined by HHS.

Question#:	7
Topic:	Child Sexual Abuse
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: What data has DHS collected and provided to HHS on child sexual abuse of unaccompanied minors attempting to cross the Southwest Border? Please provide my office with a copy of this data.

Response: ICE's Homeland Security Investigations (HSI) has not collected or provided data to HHS regarding child sexual abuse of unaccompanied minors attempting to cross the Southwest Border.

Question: What measures is DHS taking to combat abuse and trafficking of unaccompanied minors who are traveling to the Southwest Border?

Response: Since the implementation of the TVPRA, as a matter of both law and policy, CBP has screened all unaccompanied children, as defined in 6 U.S.C. § 279(g)(2), to determine whether the child has been a victim of a severe form of trafficking as defined in the TVPRA. In September 2018, CBP revised its screening tool, CBP Form 93, in response to a 2015 Government Accountability Office audit to improve the screening process. In 2019, CBP implemented a revised training course to improve the screening of these children. CBP continues to maintain an annual training requirement for the processing of unaccompanied children defined in 6 U.S.C. § 279(g)(2).

The DHS Center for Countering Human Trafficking (CCHT), which is led by HSI, oversees the DHS mission to combat human trafficking and the importation of goods produced with forced labor. By co-locating and augmenting existing DHS functions in a single integrated center, the CCHT provides a "whole of government" approach to combating these crimes and supports HSI with its victim-centered investigations of human trafficking. HSI has long been a leader in the global fight against transnational human trafficking organizations, using the full breadth of its criminal, immigration, and customs authorities to proactively identify, disrupt, and dismantle cross-border human trafficking organizations.

While human trafficking is a heinous crime and remains a top priority for DHS, it is not geographically isolated to one specific region of the United States. Human trafficking is an exploitation-based crime that does not necessitate the crossing of an international border. DHS applies a victim-centered approach, focusing on the safety and well-being of the victim, while aggressively targeting human traffickers. The CCHT, in coordination with the DHS Blue Campaign, has created training materials to bring greater awareness to the crime of human trafficking.

Question#:	7
Topic:	Child Sexual Abuse
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Along the Southwest Border, HSI routinely collaborates with CBP to initiate investigations related to transnational crime. The CCHT has increased its outreach campaign to begin educating frontline CBP officers about the potential indicators of human trafficking. When an encountered individual is suspected of being a potential victim of human trafficking, HSI is contacted by CBP at the ports of entry (POEs) or central processing centers. HSI special agents conduct interviews and, if the individual is found to be a victim of human trafficking within the United States, the individual is offered assistance through HSI's field-office-based victim assistance specialists (VASs). VASs are responsible for connecting victims with appropriate services and informing them of their rights.

HSI is very active in investigating child abuse cases at the Southwest Border. Along with interagency federal law enforcement agency partners, HSI collaborates with state and local law enforcement, nongovernmental organizations (NGOs), victim/witness service providers, and the National Human Trafficking Hotline on a regular basis. These partnerships allow HSI to robustly investigate human trafficking referrals, including crimes related to minors.

When HSI is notified of any critical incidents regarding unaccompanied minors, HSI will respond immediately and conduct interviews of the unaccompanied individuals. HSI will coordinate with VASs and local NGOs to provide victim services for these individuals. If HSI discovers sexual abuse or trafficking of an unaccompanied minor has occurred, a criminal investigation will be initiated and HSI will coordinate with HHS to notify them of the investigation and ensure safe placement of the unaccompanied minor.

Additionally, in the instances where HSI is provided leads from federal, state, or local agencies regarding any incidents involving unaccompanied minors, HSI will thoroughly investigate all incidents and coordinate with HHS.

Question#:	8
Topic:	Afghan Vetting
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: The DHS and DOD IGs have both found that DHS's vetting of the Afghan parolee population was severely deficient and led to significant security failures. The DHS IG specifically noted that DHS's lack of vetting allowed at least one individual who was liberated from prison by the Taliban to board a flight to the United States. At the same time, you have told me and other Congressional offices that DHS has vigorous and vehement disagreements with the DOD and DHS IG's findings. Walk me through why DHS disagrees that there were significant vetting issues with this population.

What are your reasons for objecting to the IG findings?

Will DHS provide any report or other written communication to Congress explaining its reasons for these objections?

Response: DHS appreciates the important work conducted by the U.S Department of Defense (DoD) and DHS Office of the Inspector General (OIG). DHS has previously raised concerns about the process underlying both of the reports as well as some of their data and findings.

Afghan evacuees underwent a multi-layered screening and vetting process that begins overseas and was conducted by intelligence, law enforcement, and counterterrorism professionals from the U.S. Department of State (DOS), DHS, DoD, Federal Bureau of Investigation (FBI), National Counterterrorism Center (NCTC), and additional Intelligence Community partners.

Upon evacuation from Afghanistan and before being cleared to travel to the United States, Afghan evacuees were brought to international transit points where the U.S. government collected and reviewed biometric (e.g., facial images and fingerprints) and biographic (e.g., name, date of birth, and ID number) information. Biometric data was compared against DoD, DHS, and FBI repositories. Biographic information was vetted by NCTC, FBI, and other Intelligence Community partners. Only those evacuees who cleared these checks were approved for onward travel to the United States, when insufficient derogatory information was identified in advance.

As with other arrivals at U.S. POEs, Afghan nationals underwent a primary inspection when they arrived at a U.S. airport. Individuals who were identified by CBP as requiring further review as a result of primary inspection were referred to secondary inspection, where additional reviews of information were conducted by CBP officers and other federal partners, as required. If any information of concern was found, several tools could be leveraged to ensure the continued protection of our national security, including the placement of individuals into expedited removal or removal proceedings.

Question#:	8
Topic:	Afghan Vetting
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

The screening and vetting process is recurrent to ensure the continued protection of public safety and national security. If individuals engage in criminal activity or additional information becomes available that raises a concern, the U.S. government takes action, which can include prosecution, revocation of parole, and placement into removal proceedings.

Neither the DHS OIG nor DoD reports acknowledged the fact that vetting is not a static process. New intelligence and information may arise that can identify information on an individual. This is why DHS ensures that all parolees undergo continuous and recurrent vetting.

DHS notes that the DHS OIG report failed to consider evidence provided to the OIG via briefings and documentation. For example, the DHS OIG report highlights a claim that CBP was unable to appropriately "screen, vet, and inspect" all Afghan nationals during the recent operation. This inaccurate conclusion fails to place CBP within the full spectrum of U.S. screening and vetting process for OAW and to subsequently inspect all Afghan nationals at the POE. Parole, by statue, requires a CBP officer to screen and inspect every applicant pursuant to the Immigration and Nationality Act (INA). The DHS OIG report also states that CBP admitted or paroled individuals into the United States without proper identification or documentation. DHS believes the OIG reached this erroneous conclusion because the OIG misunderstood the procedures that are administered for parole. Specifically, the report appears to assume that all individuals must travel on a valid travel document (such as a passport) to be inspected and granted admission or parole into the United States. Again, as established by statute, when CBP personnel process individuals for parole, they may accept an identification document, such as a traveler's birth certificate, foreign driver's license, or other national identity document, to establish identity pursuant to the INA. The vast majority of Afghans had some form of identification or documentation demonstrating their identity, such as birth certificates or national identification documents.

Further, DHS provided documentation and evidence to the OIG multiple times showing that all paroled Afghan nationals undergo recurrent vetting processes for the duration of their parole. Despite this, the report goes on to recommend that DHS establish recurrent vetting for parolees, failing to acknowledge that individuals paroled into the United States as part of Operation Allies Welcome (OAW) are already subject to continuous vetting. In addition. OIG requested evidence that vetting results were negative on individuals rather than accepting that vetting would only return derogatory information (i.e. positive results) and no results would be considered negative.

The DHS OIG report also uses specific examples to allege the vetting system does not work, when in fact, these examples show the process is working as intended. Specifically, the draft report stated that two individuals were paroled into the United States while having derogatory information in their vetting records, which is incorrect. DHS provided the OIG evidence that

Question#:	8
Topic:	Afghan Vetting
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

these individuals were cleared by the interagency vetting process at the time of travel and no derogatory information was reported prior to their parole into the United States. DHS was alerted to new derogatory information available *after* the individuals were admitted to the United States. As expected, DHS and our interagency partners immediately acted upon this new derogatory information, indicating a vetting system that is working as designed.

DHS and our vetting partners have provided several briefings on this topic and my staff can provide additional information in an appropriate setting.

Question#:	9
Topic:	Parole Termination
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: Of those Afghans who are here in the U.S. with either derogatory information or who have engaged in criminal acts, has their parole been terminated? If not, why not?

Response: ICE Enforcement and Removal Operations (ERO) tracks OAW-associated individuals paroled into the United States (OAW parolees) if they have been taken into ICE custody and only while they remain in ICE custody. ICE will only be aware of OAW parolees with derogatory information or those engaging in criminal acts if they have been encountered by ICE, or ICE is made aware of the derogatory information or criminal activity by another federal, state, or local agency. Due to policies that may limit a law enforcement agency's cooperation with ICE, ICE is not made aware of the arrest of every noncitizen.

As of December 27, 2022, 32 OAW parolees have been taken into ICE custody due to either derogatory information or information that the OAW parolee engaged in criminal activity. The existence of derogatory information or information about criminal activity, however, does not necessarily render an OAW parolee in violation of the conditions of his or her parole. In cases where derogatory information or information about criminal activity is present, a discretionary decision must be made as to whether additional conditions of parole would satisfy concerns raised by such information or whether parole should be revoked or terminated. Parole may be terminated through the issuance of a Notice to Appear (NTA) and the placement of a noncitizen into removal proceedings. The discretionary decision to issue an NTA and terminate parole is a function of the nature of the underlying derogative information and informed by whether the noncitizen is the subject of an active criminal investigation.

Question: How many Afghan nationals have had their parole terminated based on derogatory information that came to light after release from government custody at the military bases?

Response: As discussed above, as of December 27, 2022, 32 OAW-associated individuals have been taken into ICE custody. The existence of derogatory information, however, does not necessarily render an OAW parolee in violation of the conditions of his or her parole. In cases where derogatory information is present, a discretionary decision must be made as to whether additional conditions of parole would satisfy concerns raised by the derogatory information, or whether parole should be revoked or terminated. Parole may be terminated through the issuance of an NTA and the placement of a noncitizen into removal proceedings. The discretionary decision to issue an NTA and terminate parole is a function of the nature of the underlying derogative information and informed by whether the OAW parolee is the subject of an active criminal investigation.

Question#:	9
Topic:	Parole Termination
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: How many Afghan nationals have had their parole terminated due to criminal activity here in the U.S.?

Response: As of December 27, 2022, six OAW individuals have had their parole terminated due to criminal activity in the United States and have been issued NTAs by ICE. As mentioned in the above response, ICE will only be aware of OAW parolees engaging in criminal acts if they have been encountered by ICE or ICE is made aware of the criminal activity by another federal, state, or local agency. Due to policies that may limit a law enforcement agency's cooperation with ICE, ICE is not made aware of the arrest of every noncitizen.

Question#:	10
Topic:	Terrorism-Related Grounds of Inadmissibility
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: I understand that you had to revise the policies around the Terrorism-Related Grounds of Inadmissibility (TRIG) to allow for individuals who worked for the Taliban to still qualify for asylum. If you are revising this policy in such a broad manner, then it suggests that this is a known vetting issue that has occurred for a number of individuals. How many individuals would not receive asylum if DHS and the Department of State did not issue this waiver?

Response: Under INA section 212(d)(3)(B)(i), the Secretary of State and the Secretary of Homeland Security each have the unreviewable discretion, following consultations with one another and the Attorney General, to determine whether select terrorism-related inadmissibility grounds (TRIG) of the INA shall not apply to a particular group or individual with a TRIG exemption. This is a deliberate and thorough process to ensure that any exercise of TRIG exemption authority is appropriate and necessary and does not compromise public safety or national security. Since Congress provided the statutory authority for the exercise of TRIG exemptions, DHS and DOS have exercised this exemption authority a number of times in various contexts after careful deliberation.

After one or both Secretaries has issued an exercise of their discretionary exemption authority under INA section 212(d)(3)(B)(i), adjudicators make discretionary exemption decisions on a case-by-case basis and considering the totality of circumstances, pursuant to the relevant exercise of the exemption authority and its requirements. Exemptions generally allow, but do not require, USCIS officers to exempt certain specified TRIG provisions only when an individual:

- is otherwise eligible for the benefit or protection being sought;
- has undergone and passed all required security and background checks;
- has fully disclosed, to the best of their knowledge, in all relevant applications and/or interviews with U.S. government representatives and agents, the nature and circumstances of any material support provided and any other activity or association implicating TRIG, as well as all contact with a terrorist organization and its members;
- has established that they pose no danger to the safety or security of the United States; and
- meets all additional requirements enumerated in the applicable Exercise of Authority (if applicable).

On June 8, 2022, the Secretary of Homeland Security and the Secretary of State, in consultation with each other and the Attorney General, exercised their discretionary authority to exempt the application of INA Section 212(a)(3)(B), excluding subclause (i)(II), to certain individuals who were employed as civil servants in Afghanistan at any time from September 27, 1996 to

Question#:	10
Topic:	Terrorism-Related Grounds of Inadmissibility
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

December 22, 2001, or from August 15, 2021, or thereafter.[1] USCIS provides an annual report to Congress on the number and category of TRIG exemptions applied in accordance with INA section 212(d)(3)(B)(ii), through "The Secretary's Application of the Discretionary Authority Contained in Section 212(d)(3)(B)(i) of the Immigration and Nationality Act," submitted to the Chairs and Ranking Members of the House Committees on the Judiciary, Foreign Affairs, and Homeland Security, and to the Chairs and Ranking Members on the Senate Committees on the Judiciary, Foreign Relations, and Homeland Security and Government Affairs.

In Fiscal Year (FY) 2022, USCIS granted 11 Afghan Civil Servant exemptions. None of these exemptions related to asylum applicants.

[1] DHS and DOS, *Exercise of Authority Under Section 212(d)(3)(B)(i) of the Immigration and Nationality Act*, 87 FR 37523 (June 23, 2022), https://www.federalregister.gov/documents/2022/06/23/2022-13474/exercise-of-authority-under-section-212d3bi-of-the-immigration-and-nationality-ac

Question#:	11
Topic:	Vulnerability Assessments I
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: During our ongoing correspondence regarding the vulnerability assessments conducted during the Biden Administration's resumption of the Migrant Protection Protocols, DHS stated: "... Our officers and agents are both trained and well-versed in making vulnerability assessments, consistent with guidance ... as to the particular categories to consider. In fact, this is something CBP officers and agents do every day when determining appropriate immigration pathways for individuals it processes. This case-by-case analysis is based on rigorous vetting and assessment of individuals' needs and circumstances that may impact them if processed for subsequent detention, release, or in this case processed into MPP. It would not make sense - nor be needed - for additional training or guidance to be issued in this case." (See: Email from DHS Office of Legislative Affairs staff to HSGAC GovOps Subcommittee Minority staff, Subject Line: "Follow up re documents," sent at 5:56PM EDT on Nov. 6, 2022.)

Does the Department have any documents, training materials, emails, or other written documentation which trains, instructs, and/or guides DHS officers and agents - regardless of whether or not it applies to the Biden Administration's resumption of the Migrant Protection Protocols - on how to make a "vulnerability assessment" or otherwise evaluate a case on a case-by-case basis with regards to "those with a known mental or physical health issue, including a disability or medical condition related to pregnancy"? Please answer yes or no.

If yes, please share with the Committee any documents, training materials, emails, or other written documentation which trains, instructs, and/or guides DHS officers and agents on how to make a "vulnerability assessment" or otherwise evaluate a case on a case-by-case basis with regards to "those with a known mental or physical health issue, including a disability or medical condition related to pregnancy."

Response: The decision to except individuals from the Migrant Protection Protocols (MPP) was made on a case-by-case basis after evaluating the totality of circumstances. There were no specific guidance or training materials prepared regarding exercise of these exceptions; rather, the decision to except individuals from MPP was entrusted to U.S. Border Patrol Agents, who use discretion daily in determining processing pathways or case dispositions. Border Patrol Agents balance law enforcement needs with humanitarian and safety considerations when deciding which consequences are appropriate to apply for those who attempt to cross the border without authorization.

The following guidance generally governs considerations regarding vulnerable individuals in DHS custody.

Question#:	11
Topic:	Vulnerability Assessments I
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

The DHS *Standards to Prevent, Detect, and Respond to Sexual Abuse and Assault in Confinement Facilities,* a federal rule published to implement the Prison Rape Elimination Act (PREA), sets forth the requirement to assess detained individuals for risk of sexual victimization and abusiveness before they are placed in a holding facility.

In accordance with 6 C.F.R. § 115.141(c) of the DHS PREA rule, *Assessment for Risk of Sexual Victimization and Abusiveness*, officers and agents consider, to the extent that the information is available, the following criteria to assess detainees for risk of sexual victimization:

- Whether the detainee has or demonstrates a mental, physical, or developmental disability;
- Whether the detainee has an observed or reported serious physical/mental injury or illness;
- The age of the detainee;
- The physical build and appearance of the detainee;
- Whether the detainee has indicated that she is pregnant or nursing;
- The detainee's own stated concerns about his or her physical safety;
- Whether the detainee has self-identified as gay, lesbian, bisexual, transgender, intersex, or gender-nonconforming;
- Whether the detainee has self-identified as having previously experienced sexual victimization; and
- Whether the detainee has previously been incarcerated or detained (this should include the nature of the detainee's criminal or violent history, and/or gang affiliation, and whether the detainee has any convictions for sex offenses against an adult or child).

Pursuant to 6 C.F.R. § 115.141(d), if a detainee is assessed as having a high risk of victimization, the detainees must be provided with heightened protection, to include continuous direct sight and sound supervision, single-cell housing, or placement in a cell actively monitored on video by a staff member sufficiently proximate to intervene, unless there is no such feasible option.

CBP will provide the following documents to the Senator's office, including training materials, or other written documentation which trains, instructs, and/or guides officers and/or agents on how to assess risk of sexual victimization and/or abusiveness:

- CBP Policy on Zero Tolerance of Sexual Abuse and Assault (*March 11, 2015*)
- CBP Directive No. 2130-030 - Prevention, Detection, and Response to Sexual Abuse and/or Assault in CBP Holding Facilities (*January 19, 2021*)
- CBP National Standards on Transport, Escort, Detention, and Search (*October 2015*)

Question#:	11
Topic:	Vulnerability Assessments I
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

- Office of Field Operations (OFO) Memorandum – Standards to Prevent, Detect, and Respond to Sexual Abuse and Assault in CBP Holding Facilities (*August 12, 2014*)
- Instrument – OFO Detainee Assessment for Transport, Escort, Detention (*May 28, 2019*)
- USBP Memorandum and Instrument – Issuance of the Prison Rape Elimination Act Risk Assessment Instrument (*June 2, 2022*)
- USBP Memorandum – Implementation of the Standards to Prevent, Detect, and Respond to Sexual Abuse and Assault in CBP Holding Facilities (*August 13, 2014*)
- Job Aid – 6 C.F.R. 115.141 – Assessment for risk of victimization and abusiveness; 6 C.F.R. 115.162 – Agency protection duties.
- Job Aid – Risk Assessments – What's Required?
- Job Aid – PREA Definitions to Assess Detainees for Risk of Victimization
- Training – Preventing and Addressing Sexual Abuse in CBP Holding Facilities, TRAEN Code: G0797004-01

Question#:	12
Topic:	Vulnerability Assessments II
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: Does the Department have any documents, training materials, emails, or other written documentation which trains, instructs, and/or guides DHS officers and agents - regardless of whether or not it applies to the Biden Administration's resumption of the Migrant Protection Protocols - on how to make a "vulnerability assessment" or otherwise evaluate a case on a case-by-case basis with regards to "those with particular vulnerabilities given their advanced age"? Please answer yes or no.

If yes, please share with the Committee any documents, training materials, emails, or other written documentation which trains, instructs, and/or guides DHS officers and agents on how to make a "vulnerability assessment" or otherwise evaluate a case on a case-by-case basis with regards to "those with particular vulnerabilities given their advanced age."

Response: The decision to except individuals from the MPP was made on a case-by-case basis after evaluating the totality of circumstances. There were no specific guidance or training materials prepared regarding exercise of these exceptions; rather, the decision to except individuals from MPP was entrusted to U.S. Border Patrol Agents, who use discretion daily in determining a processing pathways or case dispositions. Border Patrol Agents balance law enforcement needs with humanitarian and safety considerations when deciding which consequences are appropriate to apply for those who attempt to cross the border without authorization.

Question#:	13
Topic:	Vulnerability Assessments III
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: Does the Department have any documents, training materials, emails, or other written documentation which trains, instructs, and/or guides DHS officers and agents - regardless of whether or not it applies to the Biden Administration's resumption of the Migrant Protection Protocols - on how to make a "vulnerability assessment" or otherwise evaluate a case on a case-by-case basis with regards to "those at increased risk of harm in Mexico due to their sexual orientation or gender identity"? Please answer yes or no.

If yes, please share with the Committee any documents, training materials, emails, or other written documentation which trains, instructs, and/or guides DHS officers and agents on how to make a "vulnerability assessment" or otherwise evaluate a case on a case-by-case basis with regards to "those at increased risk of harm in Mexico due to their sexual orientation or gender identity."

Response: The decision to except individuals from MPP was made on a case-by-case basis after evaluating the totality of circumstances. There were no specific guidance or training materials prepared regarding exercise of these exceptions; rather, the decision to except individuals from MPP was entrusted to U.S. Border Patrol Agents, who use discretion daily in determining processing pathways or case dispositions. Border Patrol Agents balance law enforcement needs with humanitarian and safety considerations when deciding which consequences are appropriate to apply for those who attempt to cross the border without authorization.

Question#:	14
Topic:	Rigorous Vetting
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: The email from the Department (quoted above) states that DHS and its personnel conduct "rigorous vetting and assessment of individuals' needs and circumstances that may impact them if processed for subsequent detention, release, or in this case processed into MPP." Please provide all documents which outline how DHS conducts "rigorous vetting" while conducting the case-by-case analysis described in the email from the Department.

Response: Case-by-case analysis is made when looking at the totality of circumstances. Medical evaluations are conducted onsite by medical professionals, biometric records checks are run, biographical information is acquired, and interviews are conducted numerous times during custody. All these actions and findings are used when making a case-by-case decision. There is no set of documents to provide for these actions because of the individualized nature of each determination.

Question#:	15
Topic:	CNMI Parole Program Risks
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: For the hearing entitled "Resources and Authorities Needed to Protect and Secure the Homeland" on May 4, 2022, I asked a series of Questions for the Record regarding the CNMI parole program for Chinese nationals. DHS, in responding to those questions, deferred to the State Department. However, the State Department does not have primary jurisdiction over the operation of the CNMI parole program. DHS retains that jurisdiction.

Has DHS, whether through the Office of Intelligence & Analysis or through another office or component, ever studied any national security risks related to the CNMI parole program? If so, please share any such report, analysis, bulletin, or other such document with the Committee.

In your response to Question 8 of the Questions for the Record I submitted following the May 4, 2022 hearing, you discuss the security vetting process for applying for a tourist visa. As you are aware, the CNMI parole program allow for Chinese nationals to step foot on U.S. soil without applying for a tourist visa. Furthermore, this program is operated by the Department of Homeland Security and not the State Department.

Do you believe that the CNMI parole program poses security risks to the Homeland? If so, why? If not, why not? Please share with the Committee any report, analysis, bulletin, or other material that you consulted in answering this question.

Response: Parole decisions under 8 USC § 1182(d)(5)(A) are made on a case-by-case basis through vetting and screening of individuals for inadmissibility and National Security purposes by CBP at the POE. In addition, CBP is developing an online travel authorization to facilitate Chinese nationals to apply electronically prior to their travel to the Commonwealth of the Northern Mariana Islands (CNMI). Individuals who are paroled into the CNMI for tourism or business are geographically limited to travel only within the islands of the CNMI. CBP maintains pre-inspection screening of all passengers who are departing the CNMI for other parts of the United States (currently there are only flights to Guam). This limits any travel further into the United States and minimizes security risks.

Question#:	16
Topic:	CNMI Birth Tourism
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: In your response to Question 9 of the Questions for the Record I submitted following the May 4, 2022 hearing, you deferred to the State Department. In that question, I asked whether DHS had any data regarding the prevalence of birth tourism in the CNMI. Such data could be held separately from the State Department, since the CNMI parole program is operated by DHS and not the State Department.

Does DHS or its components have any data regarding the prevalence of birth tourism in the CNMI? If so, please share with the Committee. If not, why not?

Response: DHS does not track data regarding the prevalence of birth tourism.

Question#:	17
Topic:	Charter Flights
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: In your response to Question 10 of the Questions for the Record I submitted following the May 4, 2022 hearing, you deferred to the State Department. However, DHS has the primary responsibility to vet manifests of flights prior to the flights' arrival on U.S. soil. DHS also, in vetting individuals who would enter the U.S. on parole through one of the 3 ports of entry at CNMI, would also inspect passengers as they go through customs.

What information does DHS obtain and/or analyze regarding charter flights, travel agents, local hotels, properties, and manifest information for charter flights and passengers of such flights who may be participating in the birth tourism trade? Please share with the Committee a description of such information and a description of how DHS vets individuals who may be suspected to be coming to the United States for birth tourism.

Response: DHS must respectfully defer to DOS for data concerning the birth tourism trade.

However, all flights arriving from outside of the United States, whether commercial, private, or charter, are required to submit manifest data per 19 C.F.R. § 122.22 (private) and 19 C.F.R. § 122.49a (commercial and charter). The manifest data is vetted at the National Targeting Center prior to arrival and is also vetted by local Passenger Analysis Units.

Each applicant for admission is inspected in accordance with the Immigration and Nationality Act and if the applicant for admission cannot overcome all grounds of inadmissibility, the applicant for admission would be inadmissible to enter the United States and processed accordingly. While medical treatment in the United States is a permissible activity for visitors for pleasure, those seeking medical treatment must establish that they are not intending on using public assistance for the medical treatment or remaining longer than authorized.

Question#:	18
Topic:	Completing the Border Wall
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: By what date do you anticipate completing the Yuma Morelos Dam Project, including closing the gaps between the border wall? In answering this question, please share with the Committee a project timeline.

Response: CBP has two contracts to support closing the four gaps at the Yuma Morelos Dam. Design is currently underway for both contracts. Construction is estimated to start in January 2023 and be completed in July 2023.

Question#:	19
Topic:	Funding Transfer
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: What is the status of the funding that had been transferred from DOD to DHS for border wall completion?

Response: No funding has been offered by DoD or transferred from DoD to DHS for border wall completion, to include make-safe activities. DHS is using its prior year appropriated barrier funding for former DoD project sites that had been turned over to DHS, for activities necessary to address life, safety, environmental, and remediation requirements.

Question: What is the status of the funding that had been appropriated from prior Congresses for border wall completion?

In answering these questions, please provide the Committee with a detailed timeline and breakdown of all spending related to border wall contract suspension, termination, resumption, and construction costs for each project.

Response: CBP continues to execute prior year border barrier funding in accordance with the DHS "Border Wall Plan Pursuant to Presidential Proclamation 10142" and Plan Amendment, which sets forth the guiding principles for DHS-funded border barrier construction going forward. Provided below is a summary of the projects funded through DHS appropriations between FY 2017 and 2021.

The contract award costs listed below do not include any additional costs that may be incurred as a result of the suspension and/or termination (if applicable) of any of the contracts. However, termination costs cannot exceed the total contract value. CBP will not know the final cost impacts of the pause in construction until final negotiations by the U.S. Army Corps of Engineers (USACE) are completed with the contractors, which is anticipated to be completed in 2023. Factors that go into the final costs will include material and disposal costs, contractor overhead, delay costs, and others. Once the final negotiations are completed with the various contractors, CBP will be able to provide the total cost information.

Question#:	19
Topic:	Funding Transfer
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

NOTE: Award amounts below may not be the final contract value as many contracts may be modified for scope changes or descoped work. The estimated contract values are listed below. Completion dates for original projects prior to January 20, 2021, reflect when barrier was completed and does not necessarily reflect the entire project completion date.

DHS FY 2017 | $341.2M ***Executed by USACE***	**Miles**	**Amount ($M)**	**Start Date**	**Complete Date**	**Completed Miles**
San Diego Primary Border Barrier System Project*	~14 miles	$ 147.0	5/31/2018	8/9/2019	~13.6 miles
El Centro Primary Border Barrier System Project*	~2 miles	$ 23.0	2/15/2018	10/4/2018	~2.3 miles
El Paso Primary Border Barrier System Project*	~20 miles	$ 79.0	4/9/2018	10/3/2018	~19.8 miles
El Paso Primary Border Barrier System Project*	~4 miles	$ 23.0	9/22/2018	4/8/2019	~4.2 miles
Rio Grande Valley Sector Gates	34 (QTY)	$ 18.0	11/28/2018	Jun-2023	10 (QTY)
Programmatic Costs/Change Management	-	$ 34.1	-	-	-
DHS Reprogramming	-	$ 17.1	-	-	-
TOTAL	**~40 miles**	**$ 341.2**	**-**	**-**	**~40 miles**

**Project is entirely complete.*

Question#:	19
Topic:	Funding Transfer
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

DHS FY 2018 | $1.375B **Executed by USACE & CBP**	**Miles**	**Amount ($M)**	**Start Date**	**Complete Date**	**Completed Miles**
San Diego Secondary Border Barrier System Project*	~12 mi	$ 131.0	2/18/2019	12/17/2020	~11.8 miles
San Diego (Tecate) Primary Border Barrier System Project*	~4 mi	$ 41.0	5/21/2019	7/31/2020	~3.7 miles
San Diego Secondary Gap Closure Project	~750 ft	$ 2.0	7/6/2020	1/15/2022	~700 ft
San Diego Tijuana River Border Crossing Project (CBP)	~0.2 mi	$ 48.0	11/4/2022	Jun-2024	0 miles
San Diego Friendship Circle Primary Border Barrier Project (CBP)	~0.3 mi	$ 8.4	TBD	TBD	0 miles
San Diego Friendship Circle Secondary Border Barrier Project (CBP)	~0.3 miles	$ 5.1	2/13/2023	TBD	0 miles
El Centro Primary Border Barrier System Project*	~11 miles	$ 116.0	6/10/2019	6/9/2020	~10.5 miles

Question#:	19
Topic:	Funding Transfer
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

El Centro Calexico Primary Replacement Project (CBP)	~0.5 miles	$	4.2	TBD	*PAUSED*	0 miles
El Centro Utility Relocation Project (CBP)*	N/A	$	3.5	9/15/202	8/27/2021	N/A
El Centro Train Gate (CBP)	N/A	$	1.0	May-23	Oct-2023	0 miles
El Centro New River Border Barrier Project (CBP)	~100'	$	5.1	7/15/2022	Apr-2023	0 miles
Yuma Primary Border Barrier System Project*	~22 miles	$	245.0	4/24/2019	11/26/2019	~21.9 miles
Yuma Primary Border Barrier System Project*	~4 miles	$	29.0	1/27/2020	5/8/2020	~4.0 miles
Yuma Andrade Border Barrier Project	~0.5 miles	$	10.0	TBD	*PAUSED*	0 miles
Rio Grande Valley Border Barrier System Project (RGV-07)	~13 miles	$	72.4**	8/4/2020	*CONTRACT CANCELLED*	0 miles
Rio Grande Valley Levee Barrier System Project (RGV-02)	~8 miles	$	167.0	8/19/2019	*CONTRACT CANCELLED*	~3.4 miles

Question#:	19
Topic:	Funding Transfer
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Rio Grande Valley Levee Barrier System Project (RGV-03)	~6 miles	$ 145.0	4/3/2019	*CONTRACT CANCELLED*	~0.9 mile
San Diego Erosion Control Measures (Tin Can Hill)	-	$ 5.3	3/23/2023	Feb-2024	-
San Diego Grates	-	$ 7.2	10/15/2022	Aug-23	-
Programmatic Costs/Change Management	-	$ 224.2	-	-	-
DHS Reprogramming	-	$ 100.6	-	-	-
U.S. Fish & Wildlife Service Environmental Mitigation Funding	-	$ 4.0	-	-	-
TOTAL	**~80 miles**	**$ 1,375.0**	**-**	**-**	**~56 miles**

**Project is entirely complete.*

***Net of recoveries.*

DHS FY 2019 | $1.375B **Executed by USACE**	**Miles**	**Amount ($M)**	**Start Date**	**Complete Date**	**Completed Miles**
Rio Grande Valley Levee Barrier System Project (RGV-04)	~11 miles	$ 308.0	3/26/2020	*CONTRACT CANCELLED*	~5.3 miles

Question#:	19
Topic:	Funding Transfer
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Rio Grande Valley Border Barrier System Project (RGV-05)*	~3 miles	$ 43.0	11/4/2019	6/25/2020	~3 miles
Rio Grande Valley Border Barrier System Project (RGV-06)	~3 miles	$ 17.2**	7/1/2020	*CONTRACT CANCELLED*	0 miles
Rio Grande Valley Border Barrier System Project (RGV-08)	~21 miles	$ 184.4**	4/22/2020	*CONTRACT CANCELLED*	~1.5 miles
Rio Grande Valley Border Barrier System Project (RGV-09)	~22 miles	$ 209.6**	7/6/2020	*CONTRACT CANCELLED*	~1.7 miles
Rio Grande Valley Border Barrier System Project (RGV-10)	~21 miles	$ 252.5**	6/4/2020	*CONTRACT CANCELLED*	~5.3 miles

Question#:	19
Topic:	Funding Transfer
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

DOI USFWS Transfer for Environmental Mitigation	-	$ 37.5	-	-	-
U.S. Geological Survey Environmental Mitigation Funding		$ 2.0			
Programmatic Costs/Change Management	-	$ 167.0	-	-	-
DHS Reprogramming	-	$ 68.7	-	-	-
Current Balance	-	$ 85.1	-	-	-
TOTAL	**~81 miles**	**$ 1,375.0**	**-**	**-**	**~17 miles**

**Project is entirely complete.*

***Net of recoveries.*

DHS FY 2020 | $1.375B **Executed by USACE & CBP**	**Miles**	**Amount ($M)**	**Start Date**	**Complete Date**	**Completed Miles**
Laredo North Border Barrier System Project (USACE executed)	~13 miles	$ 2.6*	N/A	*CONTRACT CANCELLED*	0 miles

Question#:	19
Topic:	Funding Transfer
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Laredo South Border Barrier System Project (USACE executed)	~26 miles	$ 6.2*	N/A	*CONTRACT CANCELLED*	0 miles
Laredo North Border Barrier System Project (CBP executed)	~14 miles	$ 55.6*	N/A	*CONTRACT CANCELLED*	0 miles
Laredo South Border Barrier System Project (CBP executed)	~17 miles	$ 16.8*	N/A	*CONTRACT CANCELLED*	0 miles
Programmatic Costs/Change Management	-	$ 68.0	-	-	-
DHS Reprogramming	-	$ 68.8	-	-	-
Current Balance	-	$ 1,157.1*	-	-	-
TOTAL	**~70 miles**	**$ 1,375.0**			**0 miles**

**Net of recoveries.*

DHS FY 2021 | $1.375B **Executed by CBP**	**Miles**	**Amount ($M)**	**Start Date**	**Complete Date**	**Completed Miles**

Question#:	19
Topic:	Funding Transfer
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Formerly DoD 284 San Diego & El Centro Make-Safe Projects	N/A	$ 73.0	Apr-23	Sep-23	N/A
Formerly DoD 284 Tucson Make-Safe Projects	N/A	$ 184.0	10/1/2022	Dec-24	N/A
Formerly DoD 284 El Paso Make-Safe Projects	N/A	$ 114.0	12/12/2022	Oct-23	N/A
Yuma Morelos Dam Projects (formerly DoD 2808 Project)	N/A	$ 13.9	1/7/2023	Jul-2023	N/A
San Diego Erosion Control (Tin Can Hill)	N/A	$ 1.9	3/23/2023	Sep-2023	N/A
Yuma Hill Gap Closure	N/A	$ 3.1	2/15/2023	Aug-2023	N/A
El Paso Train Gate	N/A	$ 2.7	Oct-2023	Dec-2023	N/A
Yuma Make-Safe San Luis Gate Operators	N/A	$ 1.0	10/12/2022	3/15/2023	N/A
Programmatic Costs/Change Management	-	$ 50.7	-	-	-
DHS Reprogramming	-	$ 68.7	-	-	-
Current Balance	-	$ 862.0	-	-	-
TOTAL	**N/A**	**$ 1,375.0**	**-**	**-**	**-**

Question#:	20
Topic:	Contract Status
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: What is the status of the materials and contracts acquired by the Trump Administration to complete the border wall?

Response: At the time of the Presidential Proclamation issued in January 2021, for the DHS-funded projects, CBP had steel for projects in the Rio Grande Valley (RGV) and Laredo Sectors. As part of the contract negotiations for the two Laredo contracts with procured steel, the contractors were responsible for disposal of the materials which was completed in September 2021. For the remaining steel in the RGV Sector, as final terminations are made for these contracts, CBP will evaluate if steel will be disposed of or used for any possible future projects. At this time, the contractors remain responsible for storage of the steel until final determinations are made.

For make-safe projects that have been approved by DHS for continuation, CBP has been able to utilize previously procured steel bollards for the Friendship Circle Project and Yuma Gap Project. Additionally, CBP is using rip-rap (rock/aggregate), gate hardware and operators, and some concrete culvert pipes for the CBP make-safe projects at the former DoD incomplete project sites.

Some contracts for DHS-funded incomplete border barrier system projects have been terminated or are in the process of being terminated, in accordance with the DHS "Border Wall Plan Pursuant to Presidential Proclamation 10142." Other contracts remain in place to complete exception work.

Question: Have those materials been used in any border wall projects undertaken by the Biden Administration? If not, what are the Biden Administration's plans for using these materials?

Response: CBP continues to evaluate the necessity of the steel materials for possible future projects, in accordance with the DHS "Border Wall Plan Pursuant to Presidential Proclamation 10142." As noted above, CBP has been able to utilize previously procured steel bollards for the Friendship Circle Project and Yuma Gap Project. CBP is also using rip-rap (rock/aggregate), gate hardware and operators, and some concrete culvert pipes from former DoD incomplete projects for the CBP make-safe projects at the former DoD project sites.

Question#:	21
Topic:	Costs Incurred
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: What costs has the Department incurred by choosing to acquire new, 6 foot steel bollards rather than using the materials acquired by the Trump Administration? In answering this question, please provide the Subcommittee with a detailed cost breakdown for every project site where the Department has decided to acquire such new bollards.

Response: CBP, in coordination with USACE, was able to use existing steel bollards that were cut down to support the 6-foot guardrails on top of the levees. CBP has not acquired any new bollards since the start of the current Administration.

Question#:	22
Topic:	Ukraine Program
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: How many parole applications for Ukrainian nationals through the Uniting4Ukraine program have been approved? How many applications have been denied?

How many sponsor applications have been approved? How many have been denied?

Response: As of December 20, 2022, USCIS received nearly 187,800 Form I-134 supporter applications. Of those, USCIS confirmed approximately 161,300 submissions and non-confirmed over 14,700 submissions. As of December 20, 2022, over 97,000 noncitizens were paroled into the United States at a POE under the Uniting for Ukraine process.

Question#:	23
Topic:	RAIO Training
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: Has the following USCIS document entitled "RAIO Combined Training Course, GUIDANCE FOR ADJUDICATING LESBIAN, GAY, BISEXUAL, TRANSGENDER, AND INTERSEX (LGBTI) REFUGEE AND ASYLUM CLAIMS TRAINING MODULE" been updated or replaced since November 06, 2015? If so, please share with the Committee a copy of the most recently updated draft or the document that replaced this document and a copy of each U.S. Government-generated document that is cited within such document.

Response: The USCIS Refugee, Asylum and International Operations Directorate Training Division updated the "GUIDANCE FOR ADJUDICATING LESBIAN, GAY, BISEXUAL, TRANSGENDER, AND INTERSEX (LGBTI) REFUGEE AND ASYLUM CLAIMS" lesson plan in December 2019 and has provided a copy of that document.

Question#:	24
Topic:	GAO Review
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: Please share with the Committee all guidance documents that DHS and its components shared with the Government Accountability Office during GAO's review entitled: "SOUTHWEST BORDER Challenges and Efforts Implementing New Processes for Noncitizen Families" (GAO-22-105456).

Response: Please see attachment.

Question#:	25
Topic:	Not Reported
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: To date, how many migrants who received a NTR or Parole/ATD and have not reported to ICE within 60 days have been arrested? How many have been removed?

Response: Once an individual has been served a charging document to initiate removal proceedings, the immigration court process can take quite some time. In the last two fiscal years, the average time that pending cases have been waiting in immigration court was between 2-2.5 years. As a result, relatively few cases that proceed through the immigration courts would be appropriate for removal if they entered under this Administration. This is another symptom of our broken immigration system, where under-resourced immigration courts and lengthy delays frustrate our ability to swiftly deliver just and fair outcomes and enforcement consequences.

When noncitizens are released from CBP custody at the border, USBP and ICE officers fill out paperwork (associated with the NTA) with further instructions for the noncitizen on the next steps in their immigration proceedings. This paperwork includes instructions on how to change their address if they move and reminds them of the importance of keeping their addresses up to date with both DOJ Executive Office for Immigration Review (EOIR) and ICE. These requirements are given to noncitizens upon their release in their native language.

ICE ERO's mission is to protect the homeland through the arrest and removal of noncitizens who undermine national security, the safety of our communities, and the integrity of U.S. immigration laws. ICE officers carefully assess whether noncitizens are appropriate for arrest, detention, and removal based on the specifics of an individual's case and use intelligence-driven leads to make the most effective use of its limited resources. Prior to release from custody, ICE assesses whether an individual presents a risk of flight or to public safety. Overall, ICE officers make enforcement and custody decisions on a case-by-case basis to focus on the greatest threats to homeland security in a professional and responsible manner informed by their experience as law enforcement officers. Noncitizens who do not comply with instructions to report to an ICE field office within the given timeframe for further processing may become a priority for further enforcement action.

Many individuals who had been released by CBP on a Notice to Report (NTR) or Parole+ATD report to ICE during their 60-day window but individuals also report beyond their 60-day window. Between March 21, 2021, and December 8, 2022, of the 96,368 noncitizens who were released with an NTR or under Parole+ATD and who checked in with ICE outside of their 60-

Question#:	25
Topic:	Not Reported
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

day window, 57,901 were issued charging documents in person or by mail.[2] Of the 96,368 noncitizens described above, 59 were removed as of December 8, 2022.[3]

Question: To date, how many migrants who received an NTR or Parole/ATD and have not reported to ICE whatsoever have been arrested? How many have been removed?

Response: Between March 21, 2021, and December 8, 2022, of the 249,708 noncitizens who were released by CBP on an NTR or Parole+ATD and did not check in with ICE, 84,993 were issued charging documents as of December 12, 2022.[4] Of the total number of individuals who did not check in with ICE, 102 were removed as of December 8.[5]

[2] ERO provides the number of Charging Documents Issued (CDIs) so that NTA mail-outs and administrative arrests are included. Simple arrest data would not include the number of noncitizens placed into removal proceedings via a mail-out NTA pursuant to Operation Horizon. An arrest list would also exclude administrative arrests such as noncitizens who are issued charging documents in person; booked into detention after being issued a charging document; or criminally arrested by local law enforcement but transferred to an ERO office and placed into proceeding via issuance of a charging document.

[3] As of December 8, 2022; timeframe of releases (March 21, 2021 - December 8, 2022). Check-in and Charging Document data as of December 12, 2022. Field Office Appointment Scheduler (FOAS) data as of December 12, 2022. ATD data provided by BI Incorporated as of December 12, 2022. DOJ EOIR data as of December 12, 2022. A check-in is defined when a noncitizen has an appointment record created in the FOAS or ENFORCE Alien Removal Module (EARM) Appointment Scheduler.

[4] ERO provides the number of CDIs so that NTA mail-outs and administrative arrests are included. Simple arrest data would not include the number of noncitizens placed into removal proceedings via a mail-out NTA pursuant to Operation Horizon. An arrest list would also exclude administrative arrests such as noncitizens who are issued charging documents in person; booked into detention after being issued a charging document; or criminally arrested by local law enforcement but transferred to an ERO office and placed into proceeding via issuance of a charging document.

[5] As of December 8, 2022; timeframe of releases (March 21, 2021 - December 8, 2022). Check-in and Charging Document data as of December 12, 2022. FOAS data as of December 12, 2022. ATD data provided by BI Incorporated as of December 12, 2022. DOJ EOIR data as of December 12, 2022. A check-in is defined when a noncitizen has an appointment record created in the FOAS or EARM Appointment Scheduler.

Question#:	26
Topic:	NTA's Issued
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: How many migrants who were processed with a NTR or Parole/ATD have been issued a NTA? How many have not been issued a NTA? In answering this question, please provide a state-by-state breakdown of how many migrants processed through these pathways have received a NTA and how many have not received a NTA.

Response: Between March 21, 2021and December 15, 2022, 532,318 noncitizens were released by CBP with an NTR or Parole+ATD and without a charging document. 194,468 of those noncitizens were subsequently issued a charging document as of December 15, 2022. The work of issuing charging documents in person and by mail remains ongoing. The below table displays the number of noncitizens who have been issued a charging document and the corresponding noncitizen's residential state.[6]

Charging Documents Issued to Noncitizens Released with NTR or Parole+ATD by State

State	Number of Noncitizens Issued Charging Documents
Alabama	1,780
Alaska	35
Arizona	1,575
Arkansas	817
California	15,526
Colorado	3,900
Connecticut	2,933
Delaware	440
District Of Columbia	389
Florida	25,582
Georgia	4,326
Hawaii	26
Idaho	891

[6] Check-in and Charging Document data as of December 15, 2022. FOAS data as of December 19, 2022. ATD data provided by BI Incorporated as of December 19, 2022. DOJ EOIR data as of December 21, 2022. The noncitizen's residential state denoted in the table is based on the most recently updated address available for the noncitizen in the Enforcement Integrated Database. If an address was not available for a member of a family unit, then an available address from others within the family unit was used. If an address was still not available for the noncitizen or the address was outside of the United States, then the state of the docket control office where the charging document was issued was used.

Question#:	26
Topic:	NTA's Issued
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Illinois	3,586
Indiana	2,725
Iowa	804
Kansas	1,110
Kentucky	2,225
Louisiana	3,894
Maine	1,315
Maryland	3,884
Massachusetts	10,415
Michigan	1,257
Minnesota	1,718
Mississippi	654
Missouri	1,315
Montana	116
Nebraska	1,279
Nevada	1,181
New Hampshire	224
New Jersey	15,436
New Mexico	499
New York	16,952
North Carolina	4,551
North Dakota	119
Ohio	2,790
Oklahoma	1,578
Oregon	1,139
Pennsylvania	3,154
Puerto Rico	38
Rhode Island	464
South Carolina	3,049
South Dakota	370
Tennessee	5,273
Texas	28,655
Utah	4,638
Vermont	55
Virgin Islands	8
Virginia	5,676

Question#:	26
Topic:	NTA's Issued
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Washington	2,324
West Virginia	108
Wisconsin	1,592
Wyoming	78

Question#:	27
Topic:	Use of Force Policies
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: Since Jan. 20, 2021, has U.S. Customs and Border Protection changed, modified, or revised its policies, guidance, paperwork requirements, or information collection regarding use of force policies for the Office of Field Operations or U.S. Border Patrol? Please answer yes or no.

If yes, please share a copy of each policy memoranda, guidance document, email, or other written materials for each change, modification, or revision.

Response: The most up-to-date CBP Use of Force Policy was signed before January 20, 2021 and went into effect in April 2021. While CBP's Use of Force guidance has remained the same since that date, CBP has updated its Emergency Driving-Vehicular Pursuit Directive (ED-VP), which modified CBP's general policies on use of force during a law enforcement encounter. The updated ED-VP Directive is new guidance and includes the prohibition on Offensive Driving Techniques (the PIT maneuver), which is an action covered in the 2021 Use of Force Policy. This updated directive (and other local/field-level policy updates) do not constitute any significant change in CBP's overarching Use of Force Policy/guidance.

Question#:	28
Topic:	Border Patrol Agent Duties
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: For Border Patrol Sectors along the U.S./Mexico border, what percentage of Border Patrol agents perform administrative duties and what percentage are in the field? How is this allocation determined?

Response: To help return agents to the field to perform their essential law enforcement and national security mission, DHS has hired nearly one thousand Border Patrol Processing Coordinators (BPPC)and added 2,500 contractors and personnel from other government agencies to help perform administrative duties. The Department has also introduced technological innovations that have saved over 70,000 hours in data entry and processing work and reduced the amount of time it takes to complete passenger manifests for repatriation flights from an average of 5.5 hours to 15 minutes.

There will always be a need to have agents performing administrative duties such as serving immigration and legal documents, taking sworn statements, and signing immigration documents. Performance of certain administrative duties is required to be conducted by a sworn law enforcement officer. As noted above, the Department has taken numerous steps to reduce the amount of administrative work conducted by Border Patrol Agents, however, as has always been the case in the past, there will be a need to have a certain percentage of agents conducting these critical legal duties.

Question: Has this allocation changed since January 20, 2021? If yes, please provide monthly percentages from January 20, 2021, to the date of OMB's clearance of response to these questions.

Response: Given the dynamic nature of these jobs, DHS does not track precise breakdowns for individual Border Patrol agents, and the number of agents performing administrative duties fluctuates greatly over time. To help return agents to the field to perform their essential law enforcement and national security mission, DHS has hired nearly one thousand BPPCs and added 2,500 contractors and personnel from other government agencies to help perform administrative duties. The President's Budget for FY 2024 requests funding to hire 310 BPPCs to further enable agents to return to the field.

Question#:	29
Topic:	OPR Operations
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: Since December 7, 2021, has CBP changed, modified, or revised any policies, charters, operational guidance, information collections, strategic plans, reporting structure, or any other aspect of the Office of Professional Responsibility? If so, please share with the Committee all written materials regarding such changes, modifications, or revisions.

Response: Since December 7, 2021, the Office of Professional Responsibility (OPR) has modified investigative operations' reporting structure and operational guidance regarding the handling of critical incident response.

On February 2, 2022, OPR Assistant Commissioner (AC) Klein and USBP Chief Ortiz issued a joint memorandum, *Interim Critical Incident Response Guidance (https:/www.cbp.gov/sites/default/files/assets/documents/2022-Feb/Interim-Critical-Incident-Response-Guidance_%2822-40128%29.pdfhtmlfile/Shell/Open/Command)*, also attached, which reiterated the July 2015 CBP Directive 4510-038, *Response to Use of Force Incidents*. The memorandum stated clear command and control are required during responses to serious use of force incidents, CBP-involved deaths, and other critical incidents involving serious injuries or deaths. USBP Critical Incident Teams (CIT) personnel may respond to these incidents at the direct request of OPR personnel and under the guidance of the OPR incident commander.

On May 3, 2022, CBP Commissioner Magnus issued a memorandum, *Critical Incident Response Transition and Support (https:/www.cbp.gov/sites/default/files/assets/documents/2022-May/critical-incident-response-memo-0522.pdfhtmlfile/Shell/Open/Command)*, also attached, which directed OPR to assume full responsibility for the critical incident response function utilizing its own assigned personnel by October 1, 2022. This includes coordination with external investigative and prosecutive entities. As of the end of FY 2022, U.S. Border Patrol eliminated all CITs and personnel assigned to USBP no longer respond to critical incidents for scene processing or evidence collection.

Furthermore, on September 29, 2022, AC Klein issued a memorandum, *Implementation of CBP's Incident Notification, Reporting and Response Procedures*. This memorandum reiterated the May 3, 2022, memorandum from the Commissioner on CIT and provided guidance on how CBP must report incidents to OPR.

Question#:	30
Topic:	Labor Trafficking
Hearing:	Threats to the Homeland
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: In the wake of the legalization of marijuana, Oklahoma has seen an increase in labor trafficking. We've heard from HSI that because they lack Title 21 authority, they cannot continue a labor trafficking investigation if there is a drug nexus. DEA has said that this is not true and that HSI does not have to stop investigating a labor trafficking case if they come across a drug nexus.

Has HSI ever stopped investigating a labor trafficking case because it overlapped with a drug case?

Response: HSI has full investigative authority to pursue human trafficking investigations, including instances of sex trafficking and forced labor (involving both domestic and transnational organizations). Although HSI has not terminated a labor trafficking case because it overlapped with a drug investigation, HSI has had to pause and delay its investigative efforts in such situations in order to coordinate investigative activities with the Drug Enforcement Administration (DEA).

Question: If law enforcement has reason to believe that there are victims of labor trafficking working at a marijuana grow, does HSI have the authority to investigate?

Response: Yes, HSI has full investigative authority to pursue human trafficking investigations, including instances involving victims of forced labor while working at a marijuana grow or in any employment capacity.

Senator James Lankford
Post-Hearing Questions for the Record
Submitted to The Honorable Christopher Wray

Threats to the Homeland
November 17, 2022

On the termination of Title 42:

1) Have you seen the projections for what will occur when Title 42 ends?
2) What impact do you believe this will have on the transnational criminal organizations that smuggle goods and illegal immigrants across the border?
3) Do you believe that a mass migration event that will occur after Title 42 is terminated will strengthen the cartels?
4) What impact will it have on the security of our country?

On Afghanistan:

The DOD IG report on Afghan vetting notes that the government was aware of more than 50 Afghan evacuees who made it to the U.S and were later discovered to have had significant derogatory information after leaving government supervision at the military bases.

5) How many Afghan nationals have been discovered to have some sort of derogatory information after arriving to the United States and leaving government supervision at the military bases?
6) Your recent testimony before the Senate Judiciary Committee suggested that the FBI does not know the location of each Afghan with derogatory information. Does the FBI know the location of each Afghan with derogatory information? If not, what steps are being taken to locate these individuals?

On PRC "Police Stations" in the US:

Numerous media outlets have reported about PRC "police stations" throughout the United States and Canada that are being used to advance China's transnational harassment and intimidation of political dissidents abroad. The FBI has briefed me and the other Commissioners on the CECC on this topic.

7) What is the extent of the PRC intimidation operation in the United States?
8) How are you coordinating with local law enforcement to identify these individuals who are unregistered agents of the CCP and harassing Chinese individuals who are here legally?

On Illicit Marijuana Grows:

There are 7,500 marijuana grows in Oklahoma. We have good reason to believe that marijuana grown in Oklahoma is crossing state lines and being funneled to other states. We also have good

reason to believe that the marijuana industry in Oklahoma has ushered in other serious federal crimes like money laundering, human trafficking and organized crime. I'm concerned that the tension between federal and state laws has led to a lack of enforcement of behalf of our federal law enforcement partners.

9) What is the FBI's attitude towards crimes involving marijuana?
10) What is your assessment of the overlap between the marijuana industry and other crimes like human trafficking?
11) Can you share how the FBI addresses these threats given the federal government's less than robust attitude towards marijuana?

USDA reports that roughly 38 million acres of agricultural land in the United States is owned by foreign entities – which is roughly the size of Georgia. Oklahoma saw the largest increase in foreign-held agricultural acres last year.

12) How is the Bureau prioritizing the involvement of transnational criminal organizations in an otherwise legal industry of marijuana distribution?
13) How is the bureau coordinating with law enforcement in Mexico and other Latin American countries who are engaging in the marijuana industry?
14) Would you welcome additional CFIUS oversight of these land purchases in close proximity to military bases and critical infrastructure?

On Labor Trafficking:

In the wake of the legalization of marijuana, Oklahoma has seen an increase in labor trafficking. We've heard from the FBI that labor trafficking falls more into DHS-HSI's lane because it is closely related to human smuggling. The FBI also shared that FBI resources are focused more specifically on sex trafficking and crimes against children.

15) Does the FBI handle labor trafficking cases?
16) When the FBI comes across a potential labor trafficking case, do you investigate the case or do you refer it to DHS-HSI or another Federal law enforcement agency?
17) When labor trafficking overlaps with a domestic drug case, would the FBI consider that to be HSI jurisdiction or FBI jurisdiction?

On FBI Investigation of Parents:

Last October, Attorney General Garland issued a memo to you and all U.S. Attorneys directing the FBI to investigate "threats" against teachers and school boards. This was seen by many of us as political because there were several news stories at the time about parents who were pushing back against draconian Covid policies and outrageous curriculums in school. The Attorney General has never rescinded the memo and has not responded to the letter I sent him in March.

18) Does the FBI have any current open investigations into individuals who have made threats against teachers, administrators, or other school personnel?
19) Do you believe investigating parents is an appropriate use of the FBI's resources?

On Child Sexual Abuse Material.

20) In your testimony you brought attention to crimes against children, specifically the presence of child sexual abuse material on the internet. In your experience, have you found that social media companies are aggressive in finding and taking down this material from their platforms and cooperating with law enforcement?

Contraband Cell Phone and Micro-Jamming Pilots:

We've previously discussed the issue of contraband phones in both federal and state correctional facilities. Similar to issues this committee has raised in Georgia, Oklahoma facilities have had transnational criminal organizations orchestrating drug trafficking, money laundering, and murder hits behind prison walls using contraband phones. The problem is unfortunately not slowing down. I have supported the full funding for BOP to carry out contraband cell phone interdiction pilot programs using both micro-jammers and managed access technology. The past few years BOP has been testing interdiction technologies, including micro-jammers that are as safe as the average consumer cell phones and seeing great results. Micro jamming is an effective security technology that effectively blocks all contraband cell phone signals from reaching a cellular network and threatening the public safety.

As publicly reported, micro jamming projects are installed or being installed at the most secure prison in America. It is my understanding that 6 BOP facilities are currently undergoing or have already installed micro-jamming infrastructure. Including the Atlanta facility that has been subject to oversight by this committee. However, I received word that the NTIA, although it has reviewed and approved prior Senate Appropriations Committee reports for the past three years detailing the micro jamming initiative by BOP to combat contraband cell phones, has been sitting on Special Temporary Authority applications by the Federal Bureau of prisons since February 2002 and has not given authority to turn on this life saving technology.

21) What steps is the Department of Justice taking to secure and NTIA approval and effectuate the actual deployment of safe, effective micro jamming technology to increase institutional security, particularly at one of the most troubled United States Penitentiaries at Atlanta GA as well as America's most secure prison ADX Florence?
22) Will you commit to getting an approval timeline from DOJ and NTIA?

SLTT Pilot:

In August, this committee passed legislation reauthorizing authorities of DOJ and DHS to countering threats from unmanned aircrafts systems. Importantly, the bill authorized a pilot program for state and local law enforcement to mitigate UAS threats under their own authorities with federal oversight. It's my understanding that there are still concerns over the pilot program. However, I think there is value to giving state and local law enforcement the ability to mitigate the increasing UAS threats.

23) Do you believe that the number of requests received annually is a sustainable model to be largely held by your agencies?

BOP & Drones:

Since 2015, there have been over hundreds of drone sightings, a number of drones interdicted by BOP staff and several Federal indictments carrying dangerous contraband into Federal prisons including cell phones, synthetic drugs, and escape paraphernalia in violation of 18 USC 1791 which prohibits contraband in prison. It's my understanding that the BOP, as publicly reported, has initiated a program of deploying counter unmanned aircraft system detection technology at its highest security penitentiaries. I applaud that effort and exercise of the legal authorities this committee supported.

24) What support does this committee need to give DOJ to continue and expand deployment of counter UAS detection technology, not only to high security federal prisons but all federal prisons?
25) What resources does DOJ need to deploy mitigation capabilities for counter UAS at federal prisons?

Cyber-Incident Reporting and FBI/CISA Coordination:

Director Wray and Secretary Mayorkas, both of your testimonies speak to the growing threats of nation state actors and subsequent cyber threats. Following the passage of the Cyber Incident Reporting for Critical Infrastructure Act, CISA and FBI both play a critical role in receiving reports from critical operators after a major cyber incident. However, the FBI has the critical role to assist victims with any investigation and potential criminal activities. I'm ultimately concerned with that the victim knows who to contact following a cyber-attack and isn't left playing mother-may-I from the federal government.

26) Following the passage of the cyber incident reporting legislation, how has the FBI worked with CISA and other sector-risk-management-agencies to ensure that victims know which federal partner to contact?
27) As a member of the Cyber Incident Reporting Council, how are you working to ensure that federal law enforcement are appropriately intertwined in the various federal reporting structures?

On attacks on prolife pregnancy centers

Since the draft opinion in Dobbs v. Jackson Women's Health Organization was leaked in May, churches and pro-life nonprofits, including pregnancy centers that are trying to help women facing an unexpected pregnancy, have experienced a horrific spike in the threats and attacks to their facilities and staff. From estimates I have seen, at least 75 pregnancy centers have been attacked and vandalized.

28) Is the FBI engaging to ensure that prolife pregnancy centers and houses of worship are protected?
29) Has the FBI made any arrests in connection with attacks on pregnancy centers or houses of worship since May 2022?

On Justice for the Five

Earlier this year, DC police recovered the remains of five unborn children at a home in DC. The remains of the children indicate that it is possible that they were subject to partial birth abortions.

As I wrote in a letter to DOJ earlier this year and have raised before the Committee several times, I remain concerned by allegations brought forward that suggest preborn babies underwent partial birth abortions or even infanticide at the Washington Surgi-Clinic in Washington, D.C.

30) Are you committed to investigating and when appropriate, prosecuting violators of the Partial-Birth Abortion Ban Act of 2003? How many Partial Ban Abortion Act violations has the FBI opened since 2017?
31) Can you confirm whether or not the FBI has conducted any investigation into the allegations that partial birth abortions may have taken place at the Washington Surgi-Clinic in Washington, D.C.?

On the FACE Act

On September 27 and October 12, I joined many of my colleagues in writing to you to express concerns with the FBI's seemingly politicized implementation and misapplication of the Freedom of Access to Clinic Entrances (FACE) Act. This includes one instance where 35 FBI agents and 15 vehicles arrived at a family's home to arrest the father of 7 children for allegedly pushing an abortion-rights escort who invaded the personal space of his 12-year-old son. In another case, charges were announced against a Franciscan monk, for engaging in non-violent civil disobedience, for which local authorities previously sentenced him.

32) How many FACE Act investigations has the FBI opened this year? How many were opened in the last 5 years?
33) Of each investigation, how many involve (1) Abortion facilities? (2) Pregnancy centers? (3) Churches or houses of worship?
34) What criteria does the FBI use when determining whether to open a case under the FACE Act that was previously dismissed by state courts?

The witness failed to respond to these questions by the end of the Administration on January 20, 2025. If responses are received after time of printing, they will be on file with the Committee for public review.

Senator James Lankford
Post-Hearing Questions for the Record
Submitted to the Honorable Christine Abizaid

Threats to the Homeland
November 17, 2022

On the termination of Title 42:

1) What is the IC's assessment of the current situation at the border from a counterterrorism perspective?
2) What impact do you believe the mass migration event like the one that may occur when Title 42 is terminated will have on preventing those with connections to terrorist organizations from entering the United States?

On Afghanistan:

3) A little more than one year out, in light of the DHS and DOD IG's findings on the vetting of Afghan nationals, do you believe that the resettlement operations have made our country safer? Why or why not?
4) What is the IC's assessment of the Afghan resettlement efforts? Does the IC believe that the resettlement efforts have strengthened domestic-based terrorist groups? If so, how?

On Iran:

The Islamic Revolutionary Guard Corps is a designated Foreign Terrorist Organization and continues to be the largest state sponsor of terrorism with its sponsorship of Hezbollah, Hamas, the Houthis, and Palestinian Islamic Jihad. The IRGC is now providing drones to Russia for use in Ukraine.

5) How are these UAV sales to Russia boosting the IRGC's sponsorship of terrorism in the Middle East?
6) What is the IC's assessment of the IRGC's role in the suppression of dissent in Iran during the ongoing protests?

Two weeks ago, Saudi intelligence shared that an attack from Iran could be imminent in either Saudi Arabia or Iraq. Iran has publicly accused Saudi Arabia, the United States, and Israel of instigating the demonstrations in Iran.

7) Between the potential attack, Iran selling weapons and training the Russians how to use them in Ukraine, and Iran's brutal treatment against its citizens and protestors, would it be accurate to say that Iran has not improved its behavior in the last two years?
8) How does a deepened alliance between Iran and Russia change the landscape of global terrorism?
9) What is your assessment of Houthi terrorist activity against our Gulf allies since the expiration of the truce in Yemen in October?

On PRC Land Purchases:

USDA reports that roughly 38 million acres of agricultural land in the United States is owned by foreign entities – which is roughly the size of Georgia. Oklahoma saw the largest increase in foreign-held agricultural acres in USDA's most recent report. What analysis can you provide about the role of state actors in these land purchases – particularly non-market economies or countries on ODNI's threat list like China, Russia, and Iran?

10) What about non-state actors and transnational criminal organizations?
11) In particular, how are our marijuana legalization frameworks opening up these opportunities for unwelcome foreign investment?
12) To what extent is CFIUS prioritizing oversight of these purchases in close proximity to military bases and critical infrastructure?

On Tik-Tok:

Earlier this year, a senior executive at TikTok testified before this Committee that the company has never shared user data of Americans with the CCP, but she would not state that it had never shared with members of the CCP.

13) What is the IC's present assessment of TikTok and the security risks of CCP access to U.S. user data through the app, which is owned by Chinese company Bytedance?

On Counter-Terrorism:

14) . Iraqi Prime Minister Mohammed Shia al-Sudani successfully formed a new government in Baghdad in October. How does this impact our counter-terrorism interests there – including sustaining our success against ISIS and preventing Iran from growing its foothold?
15) AFRICOM carried out a strike against al-Shabaab fighters in Somalia in November. What is the state of al-Shabaab's presence in North Africa and how is it impacting American interests in the region?
16) What is the counter-terrorism picture in Afghanistan right now and how has the threat assessment changed since the US withdrawal last August?
17) Specifically, what is the FTO presence in Afghanistan?
18) To what extent are terrorist actors involved in the Taliban government in Afghanistan?
19) How has China's presence in Afghanistan changed since last August?

Director Abizaid's responses to these QFRs are classified and on file with the Office of Senate Security (OSS-2023-0371).

○