TESTIMONY OF

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

BEFORE

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

ON

"Threats to the Homeland"

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

Introduction

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

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

The Evolving Threat Environment Since 9/11 Attacks

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

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

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

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

Foreign Terrorist Organizations

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

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

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

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

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

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

DHS Strategic Framework for Countering Terrorism and Targeted Violence

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

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

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

Acts of "Domestic Terrorism" and Targeted Violence

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

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

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

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

Weapons of Mass Destruction and Health Security

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

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

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

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

Cyber Threats and Emerging Technologies

Cyber Threats

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

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

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

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

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

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

5G Technology

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

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

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

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

Released in 2018, the *National Cyber Strategy*, also reiterates the need to acquire U.S. technology and capture U.S. data, communications, and intelligence property to support its goal of collaboration being the world leader in technology development and strengthens the government's commitment to work in partnership with industry to combat cyber threats and secure our critical infrastructure. Together, the *National Cyber Strategy* and *DHS Cybersecurity Strategy* guide DHS's cybersecurity efforts to prioritize the development of secure and reliable advanced information technologyrisks posed by supply chain vulnerabilities and the adoption of 5G technologies. To manage and address the risks posed by 5G, the U.S. government is taking an interagency approach, led by the White House. National Security Council (NSC) Cybersecurity Directorate and the National Economic Council co-lead a regular 5G interagency Policy Coordination Committee (PCC) through the National Security Presidential Memoranda (NSPM) - 4 process. DHS participates in these meetings and they provide an excellent opportunity to discuss and come to decisions on key G5 issues.

Unmanned Aircraft Systems

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

Supporting Election Security

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

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

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

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

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

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

Counterintelligence

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

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

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

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

Illegal Immigration

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

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

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

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

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

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

Global Illicit Drug Trade

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

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

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

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

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

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

Migrant Smuggling and Human Trafficking

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

Transnational Crime Organizations

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

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

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

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

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

Conclusion

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

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

I look forward to your questions.