Department of Justice

STATEMENT OF

CHRISTOPHER RAIA
DEPUTY DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"WORLDWIDE THREATS TO THE HOMELAND"

PRESENTED
NOVEMBER 18, 2026

STATEMENT OF
CHRISTOPHER RAIA
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
HOMELAND SECURITY COMMITTEE
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"WORLDWIDE THREATS TO THE HOMELAND"

PRESENTED
NOVEMBER 18, 2026

Chairman Garbarino, Ranking Member Thompson, and Members of the Committee, thank you for inviting me to appear before you today to discuss the threats that our great Nation faces, and the role of the Federal Bureau of Investigation (FBI) in countering these threats. Each day, the men and women of the FBI are making a real impact in communities across the Nation, tackling some of the most complex national security and criminal threats we face with perseverance, professionalism, and integrity—sometimes at the greatest of costs.

Keeping Americans safe at home and abroad is a no-fail mission. Our work to combat terrorism, espionage, cyber threats, violent crime, gangs, cartels, fentanyl, fraud, and a myriad of other threats has never been more important. Under the leadership of President Trump, the FBI's priorities are to crush violent crime, defend the homeland, rebuild public trust, and ensure fierce organizational accountability.

Counterterrorism

For more than a century, the FBI has held a critical role in defending the homeland from threats of terrorism. Domestic terrorists motivated by a range of ideologies exploit a variety of popular social media platforms, smaller websites with targeted audiences, and encrypted chat applications. They leverage these platforms to recruit, plan, garner support, and disseminate materials encouraging radicalization and mobilization to violence. The greatest domestic violent extremism threats we currently face is from anti-government or anti-authority violent extremists (AGAAVE), nihilistic violent extremists (NVEs), and racially or ethnically motivated violent extremists (REMVE). NVEs, threat actors driven by hostility toward society and a desire to destabilize it through chaos and destruction, pose a growing threat—with about an 85% increase in cases just this year.

The FBI remains committed to protecting the public from domestic terrorism as reflected in the recent disruption of eight extremists who were plotting an attack on government officials and others at the UFC Freedom 250 event in Washington, DC; and the arraignment of the first minor charged under the Juvenile Delinquency Act (JDA) for child sexual exploitation and child sexual abuse material distribution in an NVE case.

In September 2025, President Trump signed National Security Presidential Memorandum-7 (NSPM-7), directing the FBI and our Joint Terrorism Task Forces (JTTFs) to coordinate a comprehensive national strategy to investigate, prosecute, and disrupt entities and individuals engaged in acts of political violence and intimidation designed to suppress lawful political activity or obstruct the rule of law. As a result, the FBI now oversees the recently created NSPM-7 Joint Mission Center (JMC), which is composed of personnel from 10 agencies possessing counterterrorism, criminal operations and analytic expertise. The JMC is actively working to counter domestic terrorism and organized political violence by integrating intelligence, operational support, and financial analysis to proactively identify networks and prosecute domestic terrorists and related criminal actors. In total, JMC efforts to date have resulted in over 200 total arrests and more than 250 indictments or judicial complaints. The FBI has also created the NVE Fusion Cell, a centralized, cross-programmatic entity where our experts in counterterrorism and violent crimes against children are co-located to tackle the growing threat, and work with foreign partners to disrupt and dismantle networks in the United States and abroad. So far under Director Patel's leadership, the FBI has over 1,474 pending nihilistic violent extremism cases.

International terrorists continue to pose one of the most immediate threats to the homeland. The greatest international terrorism threat we currently face is from homegrown violent extremists (HVE). HVEs inspired by violent extremist ideologies aspire to carry out attacks in the United States or travel overseas to participate in terrorist activity. Meanwhile, the Islamic State of Iraq and ash-Sham (ISIS) continues to seek direct confrontation with the United States and will exploit any opportunity to attack the homeland or our interests. Al-Qa'ida senior leadership and its affiliates continue to issue statements and publish media calling for attacks against the United States, some of which include guidance on how to acquire materials and ways to conduct attacks. Similarly, Al-Qa'ida in the Arabian Peninsula (AQAP) also threatens U.S. officials and encourage lone actor attacks. The FBI continues to monitor the Government of Iran's intent to pursue violent efforts within the United States. In recent years, we have disrupted multiple Iranian plots targeting U.S. officials and activists living in the United States. The FBI's Iran Threats Mission Center—a cross-programmatic effort between the FBI's Counterterrorism, Counterintelligence and Espionage, and Cyber Divisions—has been working to synchronize intelligence and operations to increase our understanding of the Iranian threat, in line with the President's direction in National Security Presidential Memorandum-2.

Our JTTFs continue to aggressively work to prevent terrorist attacks on the homeland; stationed in all 55 field offices and composed of Federal, state, and local law enforcement working together under one roof to combat the threats from a variety of groups, including Iranian proxies. The most significant demonstration of the FBI's dedication to protecting the homeland from international terrorism threats was through the four major disruptions accomplished all within December 2025 around the holiday season—the Turtle Island Liberation Front Attack in which the FBI arrested four members of a far-left, anti-capitalist, anti-government group who were organizing a New Year's Eve bombing plot targeting U.S. businesses across Southern California; the arrest and disruption of an ISIS sympathizer in Texas, who was intending to provide bombmaking material to a foreign terrorist organization; the disruption of an individual in North Carolina who allegedly wanted to be a soldier for ISIS and made plans to commit a violent, ISIS-inspired, mass casualty attack on New Year's Eve; and the arrest of an individual in

Pennsylvania who had been researching ISIS propaganda to use in an explosives attack campaign.

So far under President Trump and Director Patel's leadership, the FBI has made over 6,744 Foreign Terrorist Organization (FTO)-related arrests, dismantled 76 FTOs, and made over 1,290 arrests of counterterrorism subjects. In addition, we have seized more than 430 firearms, worked with the Department of Justice on 476 counterterrorism convictions, and conducted 1,312 disruptions. (*Note: FTO-related arrest stats include counterterrorism and transnational criminal organization FTOs.*)

Counterintelligence

Counterintelligence operations against Nation-state adversaries mitigate grievous risk to U.S. national security. U.S. adversaries, including Russia, the PRC, and Iran continue to undermine our core institutions, and they are becoming more aggressive and more capable. Our adversaries target U.S. national defense information, attempt to recruit former or current Federal employees and military members to obtain sensitive information, gain insight into decision making, create vectors for foreign malign influence, and undermine U.S. intelligence operations. Guarding against the intelligence services of hostile states is indispensable to national security. Russia, the PRC, and Iran are all working to erode our institutions, and each is growing bolder and more capable. It is also hard to overstate the economic-espionage threat from the PRC. We have open investigations in all 55 field offices, and we are making significant headway defending American breakthroughs in semiconductors, biotechnology, quantum computing, and Super Intelligence.

The FBI's National Counterintelligence Task Force (NCITF) and multiple FBI-led, field-based Counterintelligence Task Forces (CITFs) drive a whole-of-government approach to addressing counterintelligence matters, combining the authorities of the Intelligence Community (IC) with our Federal, state, local, Tribal, and territorial law enforcement partners. The FBI also continues to facilitate robust engagements with the private sector to aid us in understanding and mitigating risks to critical infrastructure and to protect our intellectual property from adversaries. Additionally, leading up to the recent midterm elections, the FBI has worked closely with our IC and state and local partners to address any credible threats to local, state, and Federal election officials and infrastructure across the country.

In fiscal year 2026, the FBI has made 101 counterintelligence-related arrests, a 26% increase over fiscal year 2025; and has removed 90 foreign intelligence actors from the United States, a 143% increase since fiscal year 2025. So far under President Trump and Director Patel's leadership, the FBI has made over 167 counterintelligence and espionage arrests, 75 People's Republic of China (PRC)-related arrests, 34 global arrests, 18 Iran related arrests, 40 Russia-related arrests, and close to 499 counterintelligence and espionage disruptions. Over the past year we also charged seven Chinese researchers with trying to smuggle biological material into the country, five of whom have since been deported.

The FBI remains aggressive in the counterintelligence space, which has been demonstrated through some of our recent successes. In October, the FBI arrested a U.S.

Government contractor for allegedly leaking classified national defense information to someone not authorized to receive it, who then posted the classified information to an online publication. In February, the FBI arrested a former U.S. Air Force pilot accused of supplying unauthorized defense information to Chinese military aviators—a betrayal that put both our service members and our national security at risk. In January, the FBI also secured its first Super Intelligence (SI)-related theft of trade secrets conviction, against a Google engineer who attempted to funnel trade-secret SI technology to China. The FBI had several different cases where we disrupted various individuals who were circumventing export control laws to sell advanced U.S. technology, research and military-grade weapons and ammunition to Russia and Iran, respectively.

Cyber

Cyber espionage, theft, and outright attack from both Nation-states and criminal groups continue to escalate against the United States. Increasingly, state actors make common cause with financially driven hackers, producing a blended threat that the FBI—uniquely holding both criminal and intelligence authorities—is built to counter. This is not just an abstract problem. Ordinary Americans feel it directly through identity theft, hijacked accounts, business email compromise, and cyberstalking. In 2025 alone, the FBI's Internet Crime Complaint Center (IC3) received over one million complaints and overall cybercrime losses of nearly $21 billion. IC3 reports by victims reflect almost $57 million in ransomware losses so far in 2026. The rise of cryptocurrencies enables these criminal actors to acquire tools, collaborate, and launder their proceeds in new and challenging ways that are outside the regulatory framework.

The PRC, and in particular the operators that grew out of the publicly tracked Salt Typhoon campaign, keep pressing to breach telecommunications infrastructure and other critical networks. Alongside CISA, NSA, and industry, the FBI has dismantled a number of persistent-access operations aimed at both government and private systems. Other adversaries—the Democratic People's Republic of Korea, Iran, and Russia—remain active in cyber espionage, in enabling ransomware, and in pre-positioning on U.S. critical infrastructure for use in a future crisis or conflict.

The FBI's Cyber Strategy is in full alignment with the Administration's Cyber Strategy for America, specifically focused on four of the six pillars: Shape Adversary Behavior, Secure Critical Infrastructure, Sustain Superiority in Critical and Emerging Technologies, and Build Talent and Capacity. Through this strategy, the FBI imposes costs on cyber adversaries through unique authorities, world-class capabilities, and enduring partnerships. Human and technical resources enable the FBI and our partners to defend networks, attribute malicious activity, sanction bad behavior, and attack adversaries overseas. The FBI has also elevated the leadership, engagement, and coordination assets of the FBI-led, multi-agency National Cyber Investigative Joint Task Force (NCIJTF), creating new mission centers based on key cyber threat areas.

In support of President Trump's Executive Order 14390, "Combating Cybercrime, Fraud, and Predatory Schemes Against the American People," and the National Cyber Strategy, Operation Riptide demonstrated the impact of sustained, coordinated action; participating with our partners in 13 joint sequenced operations, making over 200 arrests, freezing/seizing over $23 million in illicit cryptocurrency and other funds, and initiating the return of $31 million in virtual

assets stolen by North Korean cybercriminals. The FBI has also launched Operation Winter SHIELD, a first-of-its-kind 60-day campaign to drive measurable progress across industry, government, and critical infrastructure. All 55 field offices were engaged in the campaign and conducted over 600 engagements across 14 critical infrastructure sectors.

So far in 2026, the FBI has made 159 cyber arrests, which is a 4% increase, claimed 193 indictments had 93 convictions, disrupted 240 malicious cyber operations which is an 11% increase, 11 ransomware convictions, which is an 450% increase, 40 ransomware charges, which is a 111% increase, 375 ransomware cases, which is a 21% increase, and completed 15 dismantlement's of Business Email Compromised networks, criminal enterprises, and criminal marketplaces and forums; all of which are increases from the same time in 2025. Under President Trump and Director Patel's leadership so far, the FBI has made 368 cyber arrests, claimed 544 indictments, and disrupted 557 malicious cyber operations.

Violent Crime

The FBI's continued and dedicated focus on combatting violent crime has led to historic results. So far under President Trump and Director Patel's leadership, the FBI has captured 10 of its Top Ten most wanted fugitives, made over 71,650 violent crime arrests, arrested over 47,000 violent criminals and gang members, and seized over 4,616 kilograms of fentanyl, enough lethal doses to potentially kill over 350 million Americans. The FBI has had many successful violent crime initiatives so far this year, to include Operation New Dawn in Illinois, Operation Southern Star in Alabama, Operation Gangsta's Paradise in California, and Operation Spring Cleaning in Alabama and Missouri. Together, these initiatives have led to the arrest of nearly 200 violent offenders, and a significant number of seizures of firearms, drugs, and money. Most recently in October of 2026, the FBI began its newest nationwide violent crime initiative, Operation Cold Front. All 55 field offices will work with their local, state and Tribal partners on a united front against violent crime. Since President Trump returned to office, there has been a 30% decrease in the murder rate nationwide, and violent crime rates may have dropped to the lowest levels ever, but the FBI will maintain its course and continue to bring criminals to justice.

The FBI's partnerships are key force multipliers, with over 550 unique task forces and over 6,000 members to tackle violent crime threats. In cities where crime is higher than the national rate, the FBI is sending Violent Crime Rapid Deployment Teams consisting of agents and intelligence personnel nationwide to surge resources to cities that need them most, and since January of this year, these teams have arrested over 600 subjects and seized over 250 firearms. Specifically, Operation Summer Heat was a multi-agency effort to make our communities safer across the Nation. It resulted in 7,617 violent crime arrests, 725 arrests of predators committing violent crimes against children, 3,279 drug seizures- including 436 kg of fentanyl and 55,772 kg of cocaine, and 2,451 weapons recovered. Specifically, in Louisiana, we saw a 56% decrease in homicide rates in New Orleans and a 42% decrease in homicide rates in Baton Rouge. In Memphis under the Memphis Safe Task Force, FBI surged personnel who participated in over 2,800 arrests. In one year of FBI efforts, under Director Patel's tenure, Memphis has seen a 26% decrease in homicides, a 22% decrease in aggravated assault, a 31% decrease in robberies, and a 48% decrease in carjackings.

Safeguarding children sits at the very top of the Bureau's priorities. Violent crimes against children such as financially motivated sextortion, Sadistic Online Exploitation, and SI-generated content are ushering in a host of new actors spread globally, who are committed to exploiting children and thwarting the FBI's efforts to capture them. Thanks to the leadership of President Trump and Director Patel, the FBI has identified 7,228 child victims, located 5,801 child victims, and arrested over 6,000 child predators and human traffickers.

To specifically combat violent crimes against children, the FBI has over 90 Child Exploitation and Human Trafficking Task Forces, which hosts over 90 task force officers, including over 90 international TFOs from over 60 countries. The FBI has efforts like the Innocence Lost National Initiative to address the growing issue of children recruited into commercial sex trafficking by going after the resources of those criminal enterprises that are exploiting children. Additionally, the FBI's four dedicated surges this year—Operation Restore Justice, Operation Enduring Justice, Operation Relentless Justice, and Iron Pursuit—have led to the arrest of over 1,000 predators this year. In February 2026, under Director Patel's tenure, the FBI also joined Europol's EMPACT initiative, Operation Global Chain, as the first U.S. Agency to formally participate. In 2026, this annual weeklong global human trafficking interdiction event resulted in 1,024 arrests, including 334 human trafficking arrests, 2,070 victims and potential victims identified, 465 new investigations opened, and 80 cases of document fraud detected worldwide.

Under President Trump and Director Patel's leadership, the FBI has put unprecedented attention on combatting violent crime, gangs, and criminal enterprises that have exploited Tribal lands and communities. We have launched a series of initiatives and coordinated operations, such as Voices Not Forgotten, a new initiative intended to generate new public tips to help close unsolved Indian Country investigations; Operation Steadfast Promise, a sustained commitment to address violent crime and improve public safety in Indian country, resulting in 890 new opened cases, over 450 arrests, over 130 child victims identified or located, and over 1,300 weapons seized; Operation Not Forgotten, an initiative to surge investigative, intelligence, and victim services support to field offices working Indian Country investigations; Operation Ballistic Backlog, designed to develop actionable leads on unresolved cases by testing and processing the backlog of seized firearms; and Operation Trusted Trails, initiated to disrupt criminal organizations and gang networks that are flooding Indian Country with drugs and violence, spanning 14 states and 31 Indian reservations.

The FBI has over 4,400 open investigations and over 300 full-time employees dedicated to making Tribal communities safer. The FBI continues to strengthen partnerships with Tribal law enforcement and communities through our 30 Safe Trails Task Forces, two of which were established under Director Patel's tenure, spanning 16 FBI field offices where violent crime, drug trafficking, fraud, and public corruption in Indian Country are rampant. Since Director Patel's tenure, he has attended over 18 Tribal events, including unveiling the Billings Field Office in December 2025 to further strengthen Tribal partnerships in Montana's Indian Country.

Cartels

Pursuant to President Trump's Executive Order 14159, "Protecting the American People Against Invasion," the FBI joined the Department of Homeland Security (DHS) in co-leading 59 Homeland Security Task Forces (HSTFs) nationwide, with a combined roster of more than 9,000 Federal agents, Task Force Officers (TFOs), and analysts. The HSTFs bring together over 20 Federal agencies and 440 state, local, and international law enforcement partners in a whole-of-government model. The creation of the HSTF represents the partnership, combining Federal, state, and local resources and integrating IC and Department of War (DoW) information into a whole-of-government approach to dismantle the most prolific Transnational Organized Crime (TOC)-Foreign Terrorist Organizations (FTO) operating globally. The Administration's FTO designations are an example of how the government is more united than ever. The FBI – which has unique authorities and tools available to us to counter both violent crime and terrorism – is empowered to use counterterrorism tools to combat cartels and gangs, who are terrorizing our communities.

Since the establishment of the FTO designations of cartels, the FBI has over 2,200 ongoing investigations related to the 22 designated cartels and transnational gangs. To illustrate the power of the FTO designations and the HSTFs, from August 25 to October 7, 2025, HSTF participating agencies surged in a unified approach to combat TCOs in the United States and around the world. Those efforts resulted in 400 operations, 3,266 Federal arrests, 91 metric tons of drug seizures, 1,067 weapons seized, and over $3.2 million in seized U.S. currency.

Fraud and Scams

The FBI is aggressively working to address the fraud and scam activities impacting Americans, much of which is being conducted by actors virtually and overseas. The FBI is a key leader supporting Executive Order 14390, "Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens," which mandates a whole-of-government approach to prevent, disrupt, and dismantle Cyber-Enabled Fraud actors, scam compounds, and the TCOs operating them. The FBI is coordinating efforts to support the mission with personnel embedded in the HSTF National Coordination Center (NCC), HSTF investigative squads around the country, as well as forward-deployed Law Enforcement Attache Offices.

On June 4, 2026, the FBI created the Most Wanted Fraudsters list to publicly identify individuals charged with defrauding the American people. Within two months of launching the list, the FBI arrested four subjects across three continents and to date, six of the FBI's top Most Wanted Fraudsters have been arrested, responsible for almost $2 billion dollars in losses. Other efforts to combat fraud include Take a Beat to raise public awareness, our IC3 Recovery Asset Team who work directly with financial institutions to freeze fraudulent wire transfers, Operation Level Up which uses sophisticated techniques to identify victims who are actively being defrauded, increased foreign engagement to combat the global nature of modern fraud with over 60 countries, and fortifying relationships with private sector partners.

Additionally, FBI launched Operation Blackout, a global campaign to identify, disrupt, and dismantle large-scale international scam compounds and the criminal networks that operate them. This year the campaign resulted in more than $15 billion in seized illicit assets, arrests of

over 300 individuals, and significant disruption of criminal infrastructure, including the disabling of internet terminals used by scam syndicates across Southeast Asia and the Middle East. In April 2026, the FBI—working with partners in Dubai and China—executed the largest FBI-led scam compound takedown in history. Nine compounds were raided, over 300 individuals arrested, and thousands of devices were seized.

Reforms and Accountability

The FBI continues to anchor the national Counter-Unmanned Aircraft Systems (C-UAS) effort. Through our National Counter-UAS Training Center (NCUTC) in Huntsville, Alabama and consistent with our Joint Interim Final Rule on the SAFER SKIES Act, we have continued to certify hundreds of State, local, Tribal, and Territorial partners against a shared national standard and those certified officers worked roughly 80% of the operational hours across World Cup counter-drone missions. Over the course of the 2026 FIFA World Cup, FBI deployed 5,000 personnel, conducted over 300,000 background checks, seized over 700 drones, and supported 104 matches with approximately 6.8 million attendees. More than a year of preparation made that possible, and it positions the FBI well for what is ahead with the 2028 Summer Olympic and Paralympic Games in Los Angeles, California.

The FBI supports the reauthorization of FISA 702 as a critical national security tool that cannot be replaced by other legal authorities or open-source investigative tools and methods. The FBI has implemented approximately 56 reforms as required by Congress under RISAA. During Director Patel's tenure, we have improved our query standard compliance rate from 82% in 2020, to higher than 99% in 2025, implemented a continuous double audit – one by FBI's Office of Internal Audits and one by DOJ, cut user access to the FISA 702 database data by 50%, further restricted U.S. Person Queries approvals to attorneys only, and terminated employees who have intentionally misused the FISA 702 database. We remain committed to being transparent with Congress on our use of FISA Section 702.

In conclusion, 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. The members of this committee are important partners in our fight against every threat out there – and in our efforts to build trust and credibility.

Chairman Garbarino, Ranking Member Thompson, and Members of the Committee, thank you for the opportunity to testify.

TESTIMONY OF

Hon. Markwayne Mullin
Secretary
U.S. Department of Homeland Security

BEFORE

Committee on Homeland Security
U.S. House of Representatives

ON

2026 Worldwide Threats to the Homeland

November 18, 2026
10:00 am
Washington, DC

Chairman Garbarino, Ranking Member Thompson, and Members of the Committee: Thank you for the opportunity to appear before you today to discuss the evolving threats facing our nation and the U.S. Department of Homeland Security's ongoing efforts to protect the American people.

The Department of Homeland Security was established to protect the United States from the complex threats of the twenty-first century. Earlier this year, we commemorated the 25th anniversary of 9/11. The horrific terrorist attacks that occurred on September 11, 2001, showed the importance of consistent, unified, and ever-vigilant defense of the homeland against global threats. It also revealed to the world the strength of the American spirit: We will never forget the lives lost and the valiant first responders and heroes from that day.

The current threat environment includes various actors who focus on a wide range of targets and constantly adapt their tactics to evade law enforcement. Whether it is nation-state adversaries targeting critical infrastructure with cyberattacks, malicious actors weaponizing Unmanned Aircraft Systems (UAS), foreign terrorist groups attempting to smuggle jihadists across our borders, or illegal aliens committing crimes in our communities, the threats facing our homeland require extensive coordination across federal, state, and local levels of government.

Today, I will outline the Department's efforts across four central homeland security priorities: border security and enforcement of immigration law, public safety and counterterrorism, critical infrastructure security, and threats to U.S. economic security. These are overlapping threat categories, and defending against one type of threat helps defend against the others.

Border Security and Enforcement of Immigration Law

Illegal aliens who evade law enforcement within our country are a threat to national security and public safety. Under President Trump's leadership, we have the most secure border in history. Encounters at the U.S.–Mexico border in 2026 are at historic lows, with 18 straight months of zero releases. Illegal alien encounters also continue to decrease. The U.S. Border Patrol recorded 58 percent fewer apprehensions along the Southwest Border in Fiscal Year (FY) 2026 than the previous year. More significantly, the U.S. Border Patrol's apprehensions along the Southwest Border in October 2026 were 95 percent lower than the monthly average of the Biden Administration; 97 percent below the peak of the Biden Administration in December 2023.

Similarly, the U.S. Customs and Border Protection (CBP) and its partners at the border remain on the frontline against drug smuggling, seizing dangerous narcotics before they reach American communities, saving millions of American lives. In October 2026, CBP seized over 45,000 pounds of drugs nationwide, including seizures of deadly fentanyl, cocaine, methamphetamine, heroin, and marijuana. Drug overdose deaths from fentanyl in 2025 were 45 percent lower than the annual average of the Biden Administration; 50 percent below the peak of the Biden Administration in 2022. Drug overdose deaths continue to trend downward in 2026.

This historic success has been driven by President Trump's common-sense border-security policies, increased enforcement of immigration laws passed by Congress, and complementary enforcement operations of our regional partners'.[1] The mass invasion of illegal immigration that occurred under the prior Administration allowed criminals, gang members, and known or

suspected terrorists to cross our borders undetected and hide in American communities with impunity. Reversing the flow and harms of mass illegal immigration has required an all-of-law enforcement approach. The Department remains laser-focused on the mission to arrest and remove aliens who have no legal right to remain in the United States. Let this be a warning to anyone who even thinks of crossing our border illegally: You will not get in. And to anyone who entered illegally, leave voluntarily now or you will be deported and never permitted to return.

Transnational Criminal Organizations (TCOs) remain a persistent threat to our homeland. With the Trump Administration's designation of over a dozen cartels and transnational gangs as Foreign Terrorist Organizations (FTOs), DHS is leading a number of efforts to disrupt, intercept, prosecute, and dismantle TCO and FTO threats in collaboration with our Agency partners. Specifically, Mexican cartels engage in the atrocious businesses of human smuggling, drug production, weapons trafficking, and corruption. These entities use violence, coercion, and bribery to protect profits, outcompete rivals, and increasingly leverage technologies such as social media and UAS to further their criminal activities. Human smugglers continue to exploit social media and encrypted communications platforms to advertise their services, recruit prospective aliens to attempt to cross our border illegally, and coordinate illicit travel.[2,3] Seeking nothing other than to profit from their destruction, cartels remain heavily involved in other illicit activities such as sex trafficking, extortion, fuel theft, and illegal fishing and wildlife trading. Transnational terrorist gangs, including MS-13 and Tren de Aragua (TdA), target U.S. cities for smuggling, violent crime, and other profitable illicit activity.

Under President Trump's leadership, we're delivering measurable results at the border and in the interior. The U.S. Immigration and Customs Enforcement (ICE) removals resulting from interior arrests through FY26 increased by more than 550 percent over the Biden Administration monthly average. As of October, ICE's interviews of unaccompanied alien children encountered at the Southwest Border led to more than four thousand arrests of suspected smugglers and human traffickers since President Trump returned to office. We are sustaining these enforcement efforts to secure our borders, protect public safety, and enforce our immigration laws throughout the country.

Additionally, Mexican cartels continue to exploit commercially available UAS, with CBP detecting more than 30,000 suspicious drone flights in 2026 along the Southwest Border. These technologies are utilized to surveil U.S. law enforcement and attempt cross-border drug smuggling. Within Mexico, weaponized drones have been used against Mexican authorities and rival cartels. Advances in drone technology, including improved cameras, longer flight times, anti-jamming features, and larger payloads, are likely to increase TCO and FTO interest in these systems and put our law enforcement officials at risk.

TCOs continue to adapt their methods to sustain the flow of illicit drugs into the United States, shifting between maritime, land, and air routes to transport cocaine through Latin America, the Caribbean, and directly into our homeland, and to traffic Mexico-produced fentanyl and methamphetamine into our homeland. In response to President Trump's policies to combat cartels and hold the PRC accountable through sustained enforcement pressure, TCO trafficking patterns have shifted. While fentanyl seizures by weight at the U.S.–Mexico border dropped by nearly half in 2026 compared with 2024, this metric partly reflects a tactical shift by TCOs from

finished tablets to powder. Because powder carries significantly higher potency and potential dosage-unit yield per kilogram, these seizures have a disproportionate impact on disrupting the illicit drug supply, removing countless lethal doses from circulation and directly protecting public health from this deadly synthetic opioid. However, traffickers now are adjusting to enforcement pressures, seeking to smuggle fentanyl powder at a higher purity, indicating that the total fentanyl flow into the United States remains significant.[4,5]

The President's Executive Order establishing the Homeland Security Task Force (HSTF) created the largest, most integrated campaign in U.S. history against transnational organized crime, uniting law enforcement, intelligence, defense, financial, and diplomatic power under a single national framework. The HSTF, led by DHS and the Department of Justice (DOJ), leads a coordinated, whole-of-government effort to eliminate violent transnational criminal organizations, foreign gangs invading our country, terrorist cartels, and the evil human traffickers that treat people as commodities. In FY26, HSTF conducted over 14,200 arrests, disrupted[1] or dismantled[2] almost 500 fentanyl trafficking TCOs, and seized more than $15 billion in virtual currency.

Illicit finance remains central to TCO enterprises, using cryptocurrency, money mules, brokers, money service businesses, bulk cash smuggling, wire transfers, trade-based money laundering, and front companies to conceal illegal proceeds. They also collaborate with Chinese money launderers who use underground banking, bulk cash, informal value transfers, and cryptocurrency transactions to obscure large financial movements. In August, President Trump signed NSPM-15, enabling us to have more tools at our disposal to fight these cybercriminals and terrorists. DHS is working diligently to dismantle, disrupt, and destroy these terrorist networks by harnessing the power of vetted private industry partners to counter TCO threats and combat transnational cybercrime, fraud, and other predatory schemes against American citizens.

Thanks to our brave men and women throughout DHS, we will continue to track down, arrest, and remove every member or affiliate of a TCO and ensure that none of these dangerous criminals and terrorists are ever allowed to roam our communities again. Due to strong border security and enforcement measures, we saw a 45 percent decrease in drug overdose deaths from fentanyl last year compared to the average during the Biden Administration.

The sustained decline in illegal border crossings and apprehensions, at levels not seen in over three decades, shows the profound impact of robust enforcement policies. The border remains more secure than at any point in history.

Public Safety and Terrorism

[1] Disruption Definition: Through affirmative law enforcement actions, impeding the normal and effective operation of the targeted criminal organization as articulated by factors that most often include changes in the organizational leadership, geographic control, and/or changes in the methods of operation, for example, financing, trafficking patterns, means of communications, or changes to its primary illicit activity.

[2] Dismantlement Definition: Through concerted law enforcement efforts, effectively eliminating a targeted criminal organization's ability to continue to operate. Some examples include the inability to reconstitute effective leadership or critical capabilities, the inability to maintain its former scope of activity, the loss of substantial geographic control, and the overall inability to continue core illicit activities.

Terrorism and mass casualty violence remain serious threats to our homeland. Whether terrorists or violent extremists seek to conduct attacks on American soil, send operatives across our borders, or weaponize social media and propaganda for domestic radicalization, DHS will remain vigilant in the fight against terrorism. From January 21, 2025, to September 30, 2026, ICE arrested more than 2,600 known or suspected terrorists (KSTs) and has deported more than 2,700 KSTs. We won't rest until every KST has been removed from our homeland. In addition to narco-terrorists and transnational gangs, we also face threats from domestic violent extremists, including anarchists and anti-fascists, and legacy Islamist terrorists.

Domestic violent extremists with varying ideological motivations use violence or the threat of violence to advance political and social agendas, including opposition to law and immigration enforcement; extreme views in favor of mass migration and open borders; adherence to radical gender ideology; and anti-Semitism, anti-Americanism, anti-capitalism, or anti-Christianity. Domestic threat actors have targeted faith-based communities, high-profile individuals, and law enforcement personnel. This was clearly demonstrated by the devastating assassination of my friend Charlie Kirk in Utah – a tragedy that shook the nation's political landscape and underscored the lethal reality of ideologically motivated violence. In 2026, domestic terrorists conducted at least seven attacks and engaged in at least five unsuccessful plots. In June 2026, law enforcement disrupted a plot to attack President Trump and bystanders attending the UFC Freedom 250 event at the White House. The suspects allegedly planned to use explosive-laden UAS and firearms to target crowds and high-profile attendees to "jumpstart a revolution in the United States."[6] Over the next year, lone wolf offenders or small cells motivated by domestic or global events will likely remain a primary terrorism threat to the homeland.

The threat from Islamist terrorists, whether inspired by FTOs or acting on behalf of state sponsors such as Iran, remains elevated. This threat has been fueled in part by Middle East conflicts and terrorist propaganda. Although overseas counterterrorism pressure and enhanced U.S. border security complicate FTOs' ability to send operatives to the United States, some individuals still attempt entry to conduct attacks. In March 2026, U.S.-based individuals inspired by foreign terrorist groups or their violent ideologies carried out three attacks, including ISIS-inspired attacks at Gracie Mansion in New York City and Old Dominion University in Norfolk, Virginia. Additionally, law enforcement disrupted an ISIS-related plot involving individuals allegedly attempting to send weapons to ISIS after previous travel plans to join ISIS abroad were prevented.

Chemical, biological, radiological, and nuclear (CBRN) threats also remain a concern, though most deliberate CBRN threats are expected to remain aspirational or rudimentary. Reported chemical or biological incidents rose from 18 in 2024 to 80 in 2025. Of those 80 incidents, approximately five appeared politically or ideologically motivated, eight targeted law enforcement personnel, and the remainder were criminal in nature. Materials involved ranged from chemical mixtures to common substances such as bleach, acids, antifreeze, and pepper or bear spray.

Regardless of who the threat is from, where it is headed towards, or what it is motivated by, the U.S. Department of Homeland Security is committed to protecting all Americans. We take this

responsibility seriously and are committed to working with all our state, local, federal, and tribal partners to prevent terrorism on American soil.

It is crucial that Congress reauthorizes Section 702 for our national security. Allowing FISA 702 to remain lapsed benefits our adversaries and puts U.S. intelligence and law enforcement at a disadvantage. At risk is our ability to effectively protect our cybersecurity infrastructure, combat dangerous illicit drugs from being trafficked across our borders, and thwart foreign terrorist plots. I thank the House for its work earlier this year to attempt to reauthorize 702 and urge Congress to redouble efforts to ensure this critical national security tool comes back online without delay.

Critical Infrastructure Security

The United States faces complex threats to our critical infrastructure from various sources, including nation-states, cybercriminals, terrorists, criminals, and lone wolf actors. DHS is constantly working to help defend against cyber and physical attacks, to include the development of cybersecurity attacks from adversarial super intelligence (SI), on the critical infrastructure sectors that support daily life, including energy, transportation, healthcare, water, telecommunications, and financial services.

Cyber actors affiliated with America's near-peer adversaries retain the capabilities to pose a severe cyber threat to U.S. critical infrastructure. They seek disruptive attacks against energy, water, telecommunications, transportation, and other critical networks. Cyber espionage also remains a threat, as our adversaries have made efforts to steal call records, private communications, and law enforcement data.

Iranian government cyber actors and pro-Iran cybercriminals have targeted U.S. critical infrastructure networks since the conflict with Iran began earlier this year. Since February, Iranian activity has increasingly targeted the transportation, healthcare, water, energy, and financial services sectors. These operations historically have produced localized and minimally disruptive effects against poorly secured industrial control devices, but vulnerable systems and weak cyber hygiene in lifeline infrastructure could create disruptive consequences.

North Korean cyber actors also pose significant threats. North Korean cyber actors regularly conduct fraud, money laundering, and other cyber-enabled crimes to support North Korea's weapons of mass destruction programs. They also use cyber espionage tactics, including phishing, against government and research institutions.

Ideologically motivated cybercriminals remain persistent threats. These cybercriminals often conduct distributed denial-of-service attacks and website defacements in response to global events. Cybercriminals continue to adapt their tactics, increasingly using adversarial SI to scale attacks, prioritize data theft, and target third-party providers, creating the potential for widespread disruption and financial loss.

Physical threats to U.S. infrastructure continue to be of concern, particularly against government facilities and personnel. Terrorists and criminals target commercial sites, government offices and

personnel, transportation systems, energy infrastructure, and healthcare facilities. Lone wolf offenders using simple weapons against accessible targets remain among the most difficult threats to detect and prevent. Trusted insiders also pose a persistent risk.

Unauthorized drone activity over critical infrastructure remains a security challenge. The online spread of tactics for weaponizing drones in overseas conflicts lowers the barrier for adoption of similar methods in the homeland.

To address these threats, the Cybersecurity and Infrastructure Agency (CISA) has aligned with President Trump's Cyber Strategy for America, shifting from passively defending toward proactively identifying, mitigating, and reducing malicious access to critical infrastructure. Earlier this year, CISA launched CI Fortify, an allied initiative bolstering public health and safety, defense-related critical infrastructure, economic continuity, and national security. This initiative works with operators to prepare for sustained essential operations during a potential geopolitical conflict, business operations lapse, or any other potential cyber risks. CISA is also performing targeted assessments of critical infrastructure. Under the Trump Administration, CISA has released a series of resources to address and mitigate risks from nation-state threats. These resources, coordinated with partners, provide the guidance to limit operational impact, provide mitigation options, and strengthen defenses. This mission-critical information sharing network with private industry relies on the authorities provided by Congress in the Cybersecurity Information Sharing Act of 2015, and I look forward to its reauthorization soon.

Finally, election security is national security, and protecting our critical infrastructure remains a top priority for the Trump Administration. For the 2026 elections, DHS supported state and local election officials as they worked to protect election infrastructure and safeguard the political traditions of our American way of life. CISA's election security activities addressed threats to election technologies, processes, facilities, and personnel by information sharing and providing CISA's resources for election infrastructure stakeholders.

Threats to U.S. Economic Security

The U.S. economy faces persistent and evolving threats from adversarial nation-states seeking to undermine U.S. economic competitiveness, acquire sensitive technology and proprietary systems, evade sanctions and export controls, manipulate supply chains, and exploit opaque financial networks.

America's near-peer adversaries use espionage and nontraditional intelligence collection to acquire U.S. technology, often deploying individuals who disguise their true background and pose as scholars or businesspeople to acquire U.S. intellectual property and critical technology. These efforts rely on intelligence officers, government officials, employees of U.S. firms, students, researchers, and talent programs to collect valuable information. [7,8,9,10,11,12,13,14,15,16,17]

Hostile nation-states also target critical U.S. technologies to support military modernization, weapons programs, and broader strategic goals. Their efforts often focus on acquiring controlled end products rather than underlying intellectual property.[18,19,20,21,22]

Foreign adversaries use front companies and transshipment intermediaries to procure export-controlled advanced and dual-use technology from the United States. These activities target technologies such as advanced U.S. semiconductors, with the goal of gaining an advantage in global SI computing power. [23,24,25,26,27,28,29]

Finally, adversarial nation-states continue to seek access to U.S. technology and intellectual property through corporate mergers and acquisitions, greenfield investments, and venture capital transactions. The risk extends beyond published research: collaboration can provide access to nonpublic technical know-how, data, methods, early-stage findings, and professional networks that reduce the time and cost required to replicate or operationalize U.S. innovation. These threats are particularly acute in dual-use fields such as SI, semiconductors, quantum information science, biotechnology, aerospace, and advanced manufacturing.

DHS actively participates in the Treasury-led Committee on Foreign Investment in the United States (CFIUS) and the DOJ-chaired Team Telecom to identify, assess, and mitigate national-security risks associated with foreign investment and transactions, including those involving critical technologies, infrastructure, and sensitive data. Through these interagency processes, DHS helps protect U.S. innovation and technology from exploitation by foreign adversaries.

Conclusion

The threats facing our nation are persistent, interconnected, and evolving. Transnational criminal organizations and foreign terrorist organizations continue to move people, drugs, money, and weapons across borders while adopting new technologies and techniques. Hostile nation-states are aiding and utilizing these illicit organizations as force multipliers in their efforts to target U.S. infrastructure, supply chains, technology, economic competitiveness, and American citizens. Both domestic and foreign-inspired violent extremists pose an elevated threat through active plots and direct attacks targeting public venues, faith-based communities, and high-profile individuals. As unmanned aerial system capabilities by TCOs advance, the Department continues to innovate solutions to counter this threat. Cyber and physical threats to critical infrastructure remain significant.

These threats require sustained vigilance, strong intelligence sharing, close coordination with federal, state, local, tribal, territorial, and private-sector partners, and continued attention to emerging technologies that adversaries can exploit. Under President Trump's leadership, DHS will continue working with its partners to identify, assess, and disrupt threats to our homeland.

The Department of Homeland Security will continue to adapt and meet the demands of an evolving threat environment. It is an honor to represent and serve alongside the dedicated DHS workforce, whose expertise, professionalism, and steadfast commitment help keep the homeland safe.

[1] Pew Research Center, "Migrant encounters at the US-Mexico border are at their lowest level in more than 50 years," 2 February 2026.

[2] DHS Office of Homeland Security Statistics, Drug Seizure Data, August 2026.
[3] DHS Office of Homeland Security Statistics, Drug Seizure Data, August 2026.
[4] U.S. Department of Justice, "Five Men Arrested and Charged in Plot to Attack and Kill Government Officials and Others Attending the Ultimate Fighting Championship at White House," 16 June 2026.
[5] Financial Times, "Silicon Valley steps up staff screening over Chinese espionage threat," 19 June 2024.
[6] Wall Street Journal, "Scale of Chinese Spying Overwhelms Western Governments," 8 October 2025.
[7] Department of Justice, "Chinese Government Intelligence Officer Sentenced to 20 Years in Prison for Espionage Crimes, Attempting to Steal Trade Secrets From Cincinnati Company," 16 November 2024.
[8] Department of Justice, "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," 19 July 2021.
[9] Department of Justice, "Chinese National Residing in California Arrested for Theft of Artificial Intelligence-Related Trade Secrets from Google," 6 March 2024.
[12] Center for Security and Emerging Technology, "Chinese Talent Program Tracker," undated.
[13] Department of Justice, "Superseding Indictment Charges Chinese National in Relation to Alleged Plan to Steal Proprietary AI Technology," 4 February 2025.
[14] Washington Post, "Stanford is a case study in how Beijing infiltrate U.S. universities," 5 June 2025.
[15] The Stanford Review, "INVESTIGATION: Uncovering Chinese Academic Espionage at Stanford," 7 May 2025.
[16] Department of Justice, "Chinese Government Intelligence Officer Sentenced to 20 Years in Prison for Espionage Crimes, Attempting to Steal Trade Secrets From Cincinnati Company," 17 November 2022.
[17] Department of Justice, "Chinese National and Two U.S. Citizens Charged with Conspiring to Smuggle Artificial Intelligence Technology to China," 25 March 2026.
[18] Department of Justice, "Iranian Company and Two Iranian Nationals Charged with Conspiring to Provide Material Support to Islamic Revolutionary Guard Corps (IRGC) and for Scheme to Procure U.S. Technology for Iranian Attack Drones," 1 April 2025.
[19] Department of Justice, "Two North Korean Nationals and Three Facilitators Indicted for Multi-Year Fraudulent Remote Information Technology Worker Scheme that Generated Revenue for the Democratic People's Republic of Korea," 23 January 2025.
[20] Department of Justice, "Spanish National Pleads Guilty to Conspiring to Export U.S. Military-Grade Radios to Russian Government End Users," 17 June 2025.
[21] Department of Justice, "Chinese National Pleads Guilty to Acting at the Direction of North Korea to Export Firearms, Ammo, and Technology to North Korea," 9 June 2025.
[22] Guardian, "North Korean agents using AI to trick western firms into hiring them, Microsoft says," 6 March 2026.
[23] Center for a New American Security, "Countering AI Chip Smuggling Has Become a National Security Priority," 11 June 2025.
[24] Business Standard, "With smugglers and front companies, China is skirting US AI bans," 4 August 2024.
[25] The Information, "Nvidia AI Chip Smuggling to China Becomes an Industry," 12 August 2025.
[26] Wirescreen, "PLA Has Been Acquiring America's Most Advanced AI Chips, Including Top Nvidia GPUs, Openly Through Its Own Procurement Channels for Years, WireScreen Report Finds," 1 June 2026.
[27] BBC, "Trio charged over alleged plot to smuggle Nvidia chips from US to China," 20 March 2026.
[28] Fortune, "Encrypted texts reveal how Nvidia chips and U.S. tech are being smuggled to China and Russia," 13 May 2026.
[29] Epoch AI, "Diversion and resale: estimating compute smuggling to China," 29 April 2026.