Michael Glasheen
Operations Director
Federal Bureau of Investigation

Statement Before the U.S. House Committee on Homeland Security
Washington, D.C.
December 11, 2025

Worldwide Threats to the Homeland

Statement for the Record

Good morning, Chairman Garbarino, Ranking Member Thompson, and members of the committee. I am Operations Director Michael Glasheen. I oversee the Bureau's national security divisions. I am honored to be here, representing the people of the Federal Bureau of Investigation ("FBI"), who tackle some of the most complex and most grave threats we face every day with perseverance, professionalism, and integrity. I am proud of their service and commitment to the FBI's mission and to ensuring the safety and security of communities throughout our nation.

Despite the many challenges our FBI workforce has faced, I am immensely proud of their dedication to protecting the American people and upholding the Constitution. Our country continues to face challenges, yet, through it all, the women and men of the FBI stand at the ready to tackle those challenges. The list of diverse threats we face underscores the complexity and breadth of the FBI's mission: to protect the American people and to uphold the Constitution of the United States. I am here to discuss with you what the FBI is doing to address these threats and what the FBI is doing to ensure our people adhere to the highest of standards while it conducts its mission.

Key Threats and Challenges

As an organization, we must be able to stay current with constantly evolving tactics and technologies. Our nation continues to face a multitude of serious and evolving threats ranging from international terrorists to hostile foreign intelligence services and operatives, from sophisticated cyber-based attacks to internet-facilitated sexual exploitation of children, from violent gangs and criminal organizations to public corruption and corporate fraud. Keeping pace with these threats is a significant challenge for the FBI. Our adversaries take advantage of modern technology, including the internet and social media and emerging technologies like artificial intelligence, to influence the American people, facilitate illegal activities, recruit followers, encourage terrorist attacks and other illicit actions, and disperse information on building improvised explosive devices and other means to attack the United States. The breadth of these threats and challenges are as complex as any time in our history. And the

consequences of not responding to and countering threats and challenges have never been greater.

The FBI is establishing strong capabilities and capacities to assess threats, share intelligence, and leverage key technologies. As a notable example, with the expansion of the Threat Screening Center's mission beyond terrorist watchlisting into transnational organized crime and foreign intelligence threat actors, the FBI, and government as a whole, are now well positioned to detect and mitigate threats before they reach our borders and ports, adding a critical layer of protection against the ever-growing list of dangers to the United States.

We continue to hire some of the best to serve as special agents, intelligence analysts, and professional staff. We have built, and are continuously enhancing, a workforce that possesses the skills and knowledge to deal with the complex threats and challenges we face today and tomorrow. We are building a leadership team that views change and transformation as a positive tool for keeping the FBI focused on the key threats facing our nation.

Today's FBI is a national security and law enforcement organization that uses, collects, and shares intelligence in everything we do. Each FBI employee understands that, to defeat the key threats facing our nation, we must constantly strive to be more efficient and more effective. Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of persistent terrorist, nation-state, and criminal threats to our national security, our economy, and indeed our communities.

The FBI intelligence program continues to enhance all aspects of the FBI's mission by building organizational capacity and providing operational teams, executives, and decision makers with real-time, actionable insights—enabling better, faster decisions and more accurate triage of future threats. The FBI's intelligence program transforms the valuable information the FBI collects into a shared asset that the Intelligence Community appreciates and relies upon for threat detection. We maintain a strategic capacity to detect and counter emerging and complex threats. Our outcome-driven culture ensures the FBI stays ahead of threats while upholding and protecting the Constitution of the United States.

National Security

Terrorism Threats

Over the past several years, the FBI has identified a particularly concerning uptick in the radicalization of our nation's young people. The FBI continues to work very hard to combat the increasing threat posed by domestic terrorists and those who may be motivated to commit violence and other criminal acts to further social or political objectives stemming from domestic influences.

Radicalization of domestic terrorists most often occurs through online self-radicalization. Social media and impenetrably encrypted communication applications have increased the stealth nature, speed and accessibility of violent extremist content, while also facilitating greater decentralized connectivity among extremist supporters. The FBI is refocusing its efforts at identifying lawful technical self-help capabilities to access such content in a timely fashion, but without provider assistance, such techniques frequently are contingent upon operational opportunities, tend to have limited lifespans, do not apply in some circumstances, and are exceptionally time and resource-intensive.

The FBI currently assesses international terrorists continue to pose one of the greatest, most immediate threats to the homeland. Some international terrorists are people located and radicalized to violence primarily in the United States, who are not receiving individualized direction from foreign terrorist organizations (“FTOs”) but are inspired by FTOs to commit violence. The lack of a direct connection with an FTO, ability to rapidly mobilize without detection, and use of encrypted communication platforms poses significant challenges to our ability to proactively identify and disrupt potential violent attacks. International terrorists who are inspired by FTOs such as ISIS and al-Qaida continue to aspire to carry out attacks in the U.S. or travel overseas to participate in terrorist activity.

The FBI continues to work closely with Intelligence Community partners to monitor for mobilization and radicalization indicators of the international terrorist threat and to leverage any human intelligence or online capabilities to disrupt threats posed by international terrorists.

Additionally, the Islamic State of Iraq and ash-Sham (“ISIS”) continues to pose a threat to U.S. interests, both domestically and abroad, through the group’s ability to direct, enable, and inspire attacks through their successful use of social media and messaging applications to attract individuals. ISIS seeks direct confrontation with the United States, and almost certainly would exploit any opportunity to attack the U.S. or Western interests. Like other FTOs, ISIS advocates for lone-offender attacks in the U.S. and Western countries via videos and other English-language propaganda that have specifically advocated for attacks against civilians, the military, law enforcement, and intelligence community personnel.

Iran continues to plot attacks against former government officials in retaliation for the for the January 2020 death of Islamic Revolutionary Guard Corps Qods Force (“IRGC-QF”) Commander Qassem Soleimani. They also have continued to provide support to their proxies and terrorist organizations throughout the world, such as Lebanese Hizballah.

In October 2024, we charged an asset of the IRGC who was tasked by the regime to direct a network of criminal associates to further Iran's assassination plots against its targets, including President Donald Trump. We have also charged and arrested two individuals who we allege were recruited as part of that network to silence and kill—on

U.S. soil—an American journalist who has been a prominent critic of the regime.

Iran has also conducted surveillance of Jewish and Israeli facilities and persons in the United States periodically over the past decade. It is possible the Israel-Hamas conflict and ensuing strikes between Iran and Israel will provoke increased Iranian surveillance of U.S.-based Jewish and Israeli persons.

The FBI continues to use intelligence to identify threats related to Iran's lethal capabilities targeting U.S. persons. We work closely with other U.S. government agencies and foreign partners to address the threat to U.S. interests from Iran and its proxies.

Cyber

The current state of the cyber threat landscape is one of interconnected and callous actors who have the tools to paralyze entire school systems, police departments, health care facilities, and other entities. China, Russia, Iran, North Korea, and criminal ransomware continue to be the top cyber threats facing the United States and, complicating this even more, there is no bright line where cybercriminal activity ends, and nation-state activity begins.

Cybercriminal syndicates, malicious hacktivist groups, and nation-states also continue to innovate, using unique techniques to compromise our networks and maximize the reach and impact of their operations. Those techniques include selling malware (including ransomware) as a service or targeting vendors to access scores of victims by hacking just one provider.

Critical infrastructure remains a highly attractive target for cybercriminals and nation-state actors due to the potential to cause widespread disruption, financial damage, and national security risks. The Salt Typhoon actors, for example, infiltrated the networks of multiple telecommunications companies and internet service providers. These Chinese cyber actors were able to steal customer call records data, compromise the private communications of a limited number of individuals, and copy certain sensitive information related to law enforcement. However, the FBI's unique cyber capabilities and highly skilled workforce allowed us to work with our partners to identify the Salt Typhoon campaign, collect and exploit forensic evidence, and quickly notify victims to mitigate the compromise. In 2024, the FBI received thousands of reports from critical infrastructure organizations that were affected by cyber incidents, with the most pervasive cybercriminal threat to critical infrastructure being ransomware. This threat is enormous in terms of the losses, the number of active variants, and the disruptive effects. The FBI's Internet Crime Complaint Center ("IC3") received over 3,100 reports of ransomware incidents in 2024. While this is nearly a 12% increase in overall ransomware complaints compared to 2023, the FBI has made an impact in this space—taking down threat actor infrastructure and obtaining and providing decryptor keys to

victims, which have saved hundreds of millions of dollars in ransom payments.

As one of the lead federal agencies for cyber threat response, the FBI works seamlessly with domestic and international partners to defend U.S. networks, attribute malicious activity, dismantle scam centers, sanction bad behavior, and take the fight to our adversaries overseas. Last year, these collaborations helped secure 176 convictions, 272 indictments, 289 arrests, and 342 disruptions of cybercriminals and their operations. The FBI's ability to receive details from victims to help take down cybercriminals is due in part to the Cybersecurity Information Sharing Act of 2015 ("CISA 2015"). CISA 2015 authorizes companies to monitor their networks for cybersecurity purposes, take defensive measures to stop a cyberattack, and share cyber threat indicators and defensive measures in real time with the government and with each other. If CISA 2015 is not reauthorized for the long term, the FBI will be left without one of its most critical statutory tools, and private sector companies and state and local government partners will be left with diminished support from the federal government when defending against nation-state cybercriminals We support a clean, 10-year reauthorization of CISA 2015 to ensure these vital information exchanges remain intact.

Foreign Intelligence Threats

Nations such as the People's Republic of China ("PRC"), Russia, and Iran are becoming more aggressive and more capable than ever before. These nations seek to undermine our core democratic, economic, academic, and scientific institutions, and they employ a growing range of tactics. Defending American institutions and values against these threats is a national security imperative and a priority for the FBI.

National Counterintelligence Task Force ("NCITF")

As the lead U.S. counterintelligence agency, the FBI is responsible for detecting and lawfully countering the actions of foreign intelligence services and organizations as they seek to adversely affect U.S. national interests. Recognizing the need to coordinate similar efforts across agencies, the FBI established the NCITF in 2019 to create a whole-of-government approach to counterintelligence. The FBI established this national-level task force in the National Capital Region to coordinate, facilitate, and focus a multi-agency counterintelligence effort to programmatically support local Counterintelligence Task Force ("CITF") operations. By combining the authorities and operational capabilities of the U.S. Intelligence Community, non-Title-50 departments and agencies, law enforcement agencies around the country, and local CITFs in each FBI field office, the NCITF coordinates and leads whole-of-government efforts to defeat hostile intelligence activities targeting the United States.

The Department of War ("DoW") has been a key partner in the NCITF since its founding. While the FBI has had long-term collaborative relationships with DoW entities such as the Air Force Office of Special Investigations, Naval Criminal Investigative

Service, and Army Counterintelligence, the NCITF has allowed us to enhance our collaboration for greater impact. This whole-of-government approach is a powerful formula to mitigate the modern counterintelligence threat.

Counterintelligence operations against nation-state adversaries mitigate grievous risk to U.S. national security. U.S. adversaries, including China, Russia, and Iran, continue to undermine our core institutions, and they are becoming more aggressive and more capable. The economic security threat posed by the PRC cannot be overstated. The PRC has deliberately created an environment that abuses global interconnectedness and encourages intellectual property acquisition, using human intelligence officers, corrupt corporate insiders, foreign direct investment, and reckless and indiscriminate cyber intrusions. We have active PRC counterintelligence investigations across all 56 FBI field offices. Russia continues to seek and to acquire U.S. technologies to help rebuild its defense industrial base, relying on complex procurement networks to evade US export controls and sanctions.

Iran Threats Mission Center ("ITMC")

The ITMC increases collaboration across all Iran threats—cyber, counterintelligence, and counterterrorism. The center synchronizes intelligence and operations on multiple joint initiatives and increases the FBI's understanding of the Iran threat, contributing to the President's National Security Presidential Memorandum ("NSPM-2"), "Imposing Maximum Pressure on the Government of the Islamic Republic of Iran" objectives.

Across all of our adversary threat streams, the FBI has made over 70 arrests protecting our country from nefarious foreign intelligence activity since January 20, 2025.

Technology

The FBI continues to enhance a workforce that possesses the skills and knowledge to deal with the complex threats and challenges we face today—and will face tomorrow. We are building a leadership cadre that views change and transformation as a positive tool for keeping the FBI focused on the key threats facing our nation. As criminal, terrorist, and foreign intelligence threats become more diverse and dangerous, the role of technology becomes increasingly important to our efforts; and keeping pace with technology remains a key concern for the future. The FBI Laboratory, operating out of state-of-the-art facilities in Quantico, Virginia, and Huntsville, Alabama, is one of the largest and most comprehensive forensic laboratories in the world. The FBI's laboratory facilities and personnel are helping to support investigations ranging from detecting deepfakes to identifying biological materials being smuggled into and out of the U.S. One example of the Lab's key services and programs is the Combined DNA Index System ("CODIS"), which allows over 200 law enforcement laboratories throughout the United States to compare over 25 million DNA profiles. Over one million DNA samples are added to CODIS every year and, as a result, over 125 investigations are aided each day. In the last 20 years, CODIS has aided over 722,000 investigations, while

maintaining its sterling reputation and the confidence of the American public.

Additionally, I would be remiss if I did not underscore an urgent legislative issue. On January 30, 2026, the authorities in 6 U.S.C. § 124n for the Departments of Homeland Security and Justice, including the FBI, to detect and mitigate malicious unmanned aircraft systems ("UAS") will expire. (HR 5371, Sec. 145.) Small UAS are inexpensive, widely available, and ready for surveillance out of the box. With minimal accessories, they can carry payloads, creating real risks to public safety and national security from criminals, foreign intelligence services, and terrorists. Without reauthorization or new and expanded authorization, the nation's highest-risk special events, like the 2026 FIFA World Cup and the 2028 Summer Olympics, and other covered missions will be unprotected against unsafe or malicious drones. Legislative action is essential. A measured expansion is also needed so trained and certified state, local, tribal, and territorial partners can act lawfully when a credible UAS threat emerges—in a manner that does not risk the safety and efficiency of lawful aviation operations, both manned and unmanned. The FBI's newly established and first-of-its-kind National Counter-UAS Training Center in Huntsville, Alabama, will serve as the nation's premier hub for preparing law enforcement and security professionals to detect, assess, and counter emerging UAS threats. The FBI also participated in the DoW's November 2025 Interagency Summit launching the DoW's Joint Interagency Task Force 401, which is aimed at countering small UAS threats and keeping the skies over America safe from dangerous drones.

In addition to addressing the extensive external threats facing our nation, the FBI will focus some of its resources to address the internal risk of non-compliance with all of the laws, rules, regulations and policy that apply to our work. We have been very clear that the FBI must create a culture of compliance that gives the American public the confidence that we will do our work objectively, impartially, and in strict adherence to the Constitution. Our broad mandate and sweeping authorities come with commensurate guardrails to protect U.S. citizens.

The FBI takes its responsibility of fiscal stewardship seriously and is looking at all available options to optimize existing resources and deliver more efficiently. Over the past few months, we commenced the process to reallocate hundreds of positions from the National Capital Region out to field offices across the country to enhance investigative capacity and provide better support to federal, state, local, Tribal, and territorial partners. This enhancement to field resources will increase the investigative capacity in 49 of our 56 field offices and will enable the FBI to focus these resources on addressing violent crime, gangs, drugs, counterintelligence, and terrorism threats.

Criminal Threats

The United States faces many criminal threats, including financial and health care fraud, transnational and regional organized criminal enterprises, crimes against children and human trafficking, violent threats against election personnel, and public corruption. Criminal organizations—domestic and international—and individual criminal activity represent a significant threat to security and safety in communities across the nation.

Violent Crime

Beginning on January 20, 2025, the President issued a national security executive order directing federal government agencies to pursue the total elimination of cartels and transnational criminal organizations (“TCOs”) in the United States. Additionally, in response to the February 20, 2025, U.S. State Department action designating six cartels and four transnational gangs as FTOs and Specially Designated Global Terrorists (“SDGTs”), the FBI developed the Counter Cartel Coordination Center (“C4”) to bring to bear all the FBI’s tools, resources, and skillsets to most effectively combat FTOs and SDGTs. C4 integrates the unique capabilities of Criminal Investigation Division and Counterterrorism Division, along with the U.S. Intelligence Community (USIC), DoW, and state, local, federal and foreign partners, to disrupt and dismantle persistent threats from the FTOs and SDGTs. Prioritizing criminal prosecutions to disrupt the threat, C4 leverages national security authorities and intelligence resources, which have yielded significant results.

For example, in March, working with our interagency partners, the FBI announced the expulsion of one of our “Ten Most Wanted” from Mexico—a key senior leader of the brutal MS-13 gang, Francisco Javier Roman-Bardales. This is the third fugitive the FBI arrested this year who is on the FBI’s most wanted list. Currently, FBI-led task forces are staffed with over 9,000 federal, state, local, Tribal, and territorial partners. Many of these task forces are focused on western hemisphere TCOs, cartels, violent crime, violent gangs, drug trafficking, child exploitation, and human trafficking across our nation's communities. Since January 20, 2025, the FBI participated in over 37,000 immigration-related operations, resulting in over 38,000 arrests, to include 230 arrests of Tren de Aragua members and 120 arrests of MS-13 members. Additionally, the FBI has seized over 230,000 kilograms of cocaine, 14,000 kilograms of methamphetamine, and 2,100 kilograms of fentanyl.

Over the last few months, personnel across the FBI's 56 field offices have participated in Operation Allied Corridor, a U.S. Immigration and Customs Enforcement (“ICE”) Homeland Security Investigations (“HSI”)-led operation to advance Title 8 enforcement priorities. The FBI, with support from ICE’s Enforcement and Removal Operations (“ERO”), HSI, the Drug Enforcement Administration (“DEA”), the Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”), and the United States Marshals Service (“USMS”), has targeted approximately 3,000 U.S.-based criminal aliens either associated with criminal organizations (TCOs and narcotics-smuggling networks) or re-entry violators with criminal histories who are eligible for deportation and removal from

the United States. We are starting to see incredible results because of task forces like these, and the country is safer as a result. The FBI partnerships do not stop at our borders. We are focused on collaborating with our international law enforcement partners as well.

Executive Order 14159, Protecting the American People Against Invasion, directed the establishment of Homeland Security Task Forces (HSTFs). The HSTF mission is to end the presence of criminal cartels and foreign gangs designated as FTOs, and TCOs across the United States. This task force construct is the first of its kind, employing a whole-of-government model to fight FTOs and TCOs by consolidating all of U.S. law enforcement, military, and intelligence efforts into a targeted effort in combatting these threats. The HSTF is co-led by the FBI and Homeland Security Investigations (HSI). Thirty regional CORE HSTFs and 29 Satellite Offices have been established and are fully operational, providing coverage across all 50 states, the District of Columbia, and U.S. territories. The HSTF National Coordination Center (NCC) serves as the primary federal coordinating entity to align law enforcement, defense, and intelligence efforts; reduce duplication; enhance officer safety; and optimize collaboration across all task forces, fusion centers, and partner entities combating cartels, FTOs, and TCOs.

HSTF has over 8,500 federal agents, task force officers, and analysts dedicated to the HSTF mission in addition to over 440 state and local agencies across the country, High Intensity Drug Trafficking Areas (HIDTA) partners, hundreds of U.S. Intelligence Community and Department of War analysts, and hundreds of legal attachés worldwide. The purpose of this structure is to coordinate HSTF efforts globally to achieve total elimination of these organizations' presence in the United States and their ability to threaten the territory, safety, and security of the United States through their extraterritorial command-and-control structures. For example, the HSTF NCC organized and led a surge in September 2025, during which HSTFs executed 400 multi-agency law enforcement operations resulting in over 3,000 arrests of FTO members, the seizure of over 1,000 firearms from dangerous criminals, the interception of over 92 metric tons of deadly narcotics that were prevented from flooding our nations streets, and over 100 watchlisted cartel and gang terrorists prevented from entering our borders.

An additional example of a strong collaborative initiative is the creation of the Scam Center Strike Force, combining the resources of the FBI with the U.S. Attorney's Office in the District of Columbia, the DOJ's Criminal Division, the U.S. Secret Service, the Department of State, Department of Treasury's Office of Foreign Assets Control ("OFAC"), and the Department of Commerce to disrupt scam compounds in Southeast Asia that are estimated to defraud Americans of nearly $10 billion a year. These scam centers are run by Chinese organized crime groups which exploit victims of human trafficking, who are held against their will, tortured, and sold to other criminal groups all while being forced to scam American citizens. It is the FBI's job to stop these criminals

from stealing Americans' money, disrupt their ability to perpetrate these heinous human rights abuses, and prevent them from further undermining the rule of law. We will continue to work diligently and aggressively with our partners to do so.

The FBI's Joint Terrorism Task Forces ("JTTFs"), located in each of the FBI's 56 field offices, support President Trump's executive orders and the Department of Justice's focus on immigration enforcement while working in partnership with Department of Homeland Security components to address terrorism-related subjects eligible for immigration enforcement action.

Additionally, the FBI is combatting evolving international terrorism threats as evidenced by the October 7, 2023, attack by Hamas in Israel and continued attempts of terrorist actors to infiltrate the United States as migrants. As a co-leader of the Department's Joint Task Force October 7 ("JTF 10-7"), created by the Attorney General on February 5, 2025, the FBI will continue to work tirelessly to seek justice for the victims of the October 7, 2023, terrorist attack and address the ongoing threat posed by Hamas and its affiliates. The continued sharing of information among our numerous partners through JTTFs, statewide and regional fusion centers, and law enforcement partners (or partner associations) across the country, and our legal attaché offices around the world, remains a critical component in identifying, preventing, and responding to terrorism threats.

We are starting to see incredible results because of effective cooperative initiatives like these, and the country is safer as a result.

Conclusion

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

Thank you for the opportunity to testify today. I am happy to answer your questions.