
TESTIMONY OF

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

BEFORE

Committee on Homeland Security
United States House of Representatives

ON

# "Worldwide Threats to the Homeland"

November 15, 2023
Washington, DC

Distinguished Members of this Committee:

I am proud to submit this testimony on behalf of the 260,000 people across our nation and around the world who make up the Department of Homeland Security (DHS). The people of DHS are our most important and vital resource. Serving alongside them is the greatest honor of my life and supporting them and their critical work has been my top priority since taking office.

In September, DHS published the 2024 Homeland Threat Assessment, which focuses on the most direct, pressing threats to our Homeland over the next year—public safety, border and immigration, critical infrastructure, and economic security. Together, we are enabling our workforce and our partners to effectively prevent, prepare for, and respond to the increasingly diverse and complex threats and challenges facing our country.

Already, in the weeks since the assessment publication, the world has changed after Hamas terrorists viciously attacked thousands of innocent men, women, and children in Israel on October 7, 2023, brutally murdering, wounding, and taking hostages of all ages. As the conflict continues, we have seen an increase in reports of threats against Jewish, Muslim, and Arab-American communities and institutions. Hate directed at Jewish students, communities, and institutions add to a preexisting increase in antisemitism in the United States and around the world.

Lone offenders, motivated by a range of violent ideologies, pose the most likely threat. We urge the public to stay vigilant and to promptly report suspicious activity to local law enforcement. The Department is closely monitoring unfolding events and will continue to engage in information sharing with our homeland security partners at home and abroad. We, along with our partners at all levels of government, will continue to help communities prepare for and respond to a range of public safety challenges and are working tirelessly on this mission, which has never been more important.

Again, I welcome this opportunity to discuss the overarching threats facing the Homeland as well as the tools necessary to address those challenges.

**Combating Terrorism and Targeted Violence**

Since this Department's inception, the threat landscape our Department is charged with confronting continues to evolve. Although the terrorism threat in the United States has remained heightened throughout 2023, Hamas's attack on Israel, along with other recent events, have sharpened the focus of potential attacks on targeted individuals and institutions perceived as symbolic of or tied to the conflict. These tensions, coupled with the widespread sharing of graphic and disturbing content related to this conflict, increase the prospects for violence in the United States. In 2024, we expect the threat of violence from violent extremists radicalized in the United States will remain high, marked by lone offenders or small group attacks that occur with little to no warning. DHS remains agile and vigilant in addressing all terrorism-related threats to the Homeland.

*Foreign Terrorist Threats*

Foreign terrorist groups like al-Qaeda and ISIS are rebuilding overseas, and they maintain worldwide networks of supporters that could target the Homeland. Among state actors, we expect Iran, the principal funder of Hezbollah and Hamas, to remain the primary state sponsor of terrorism and continue its efforts to advance plots against individuals in the United States. Foreign terrorists continue to engage with supporters online to solicit funds, create and share media, and encourage attacks in the United States and Europe while their affiliates in Africa, Asia, and the Middle East prioritize local goals. In Afghanistan, ISIS's regional branch, ISIS-Khorasan, continues to harbor intent to conduct external operations and maintains English-language media releases that aim to globalize the group's local grievances among Western audiences.

DHS works closely with our law enforcement, national security, and Intelligence Community (IC) partners to continually improve our ability to identify individuals who pose a national security or public safety threat and who seek to travel to the United States or receive an immigration benefit. DHS screens and vets every individual encountered at or between ports of entry, and if an individual is determined to pose a potential threat to national security or public safety, we either deny admission, detain, remove, or refer them to other federal agencies for further vetting and prosecution as appropriate. We continue to build partnerships with foreign governments that strengthen our vetting capabilities through increased information sharing. Under the International Biometric Information Sharing (IBIS) Program, DHS has partnered with the Department of State to build the capacity of partners in the Western Hemisphere to collect and screen biometric information—including against DHS holdings—to more effectively manage irregular migration. DHS has also added a new requirement to the Visa Waiver Program (VWP) to require participating countries to enter into an Enhanced Border Security Partnership (EBSP) by the end of 2026. Under EBSP, DHS will be able to send a biometric search to VWP partners to authenticate the identity of travelers and to detect whether individual travelers represent a possible threat to the security or welfare of the United States.

DHS's mission is to protect the country against all threats to homeland security regardless of origin, and the Office of Intelligence and Analysis (I&A) exists to provide intelligence supporting that mission, including through effective, appropriately tailored collection capabilities, including with respect to U.S. persons associated with or targeted by threats to homeland security. I&A uses these capabilities, analyzing and sharing information it receives through its collection from a variety of sources, including from voluntary interviews and publicly available sources, to inform intelligence and analysis, security decisions, policy development, and law enforcement. Specifically, I&A helps to ensure that state, local, Tribal, territorial, campus (SLTTC) and private sector entities can better protect themselves against threats by providing timely and accurate intelligence to the broadest audience at the lowest possible classification level. DHS, the IC, SLTTC, and private sector partners rely on I&A's contributions and unique authorities to share this information. DHS will continue to leverage our deployed intelligence professionals to ensure the timely sharing of information and intelligence with DHS components and SLTTC partners, in accordance with applicable law and privacy, civil rights, civil liberties, and intelligence oversight policies. These activities, as well as the information that I&A collects about the fentanyl trade, human smuggling, non-traditional

intelligence threat actors, and other serious threats to the Homeland, yield valuable insights to our DHS and IC partners with related missions.

*Violent Extremism and Targeted Violence*

Over the past year, domestic violent extremists (DVEs) and homegrown violent extremists (HVEs) inspired by foreign terrorist organizations have engaged in violence in reaction to sociopolitical events. These actors will continue to be inspired and motivated by a mix of conspiracy theories; personalized grievances; and racial, ethnic, religious, and anti-government ideologies, often shared online. The threat of a "lone wolf" actor attempting to exploit the conflict between Israel and Hamas and incited to violence by an ideology of hate is of particular concern. Foreign terrorist organization and lone offender reactions based on perceptions of U.S. support to Israel could further escalate the threat to Jewish, Muslim, and Arab-American communities in the United States and to U.S. government officials. As the conflict endures, graphic visuals will likely continue to circulate online and garner significant media attention, potentially acting as a catalyst for various violent actors who have shared and continue to share this kind of material.

Over the last year, DVEs and criminal actors with unclear or mixed motivations have increasingly called for carrying out physical attacks against critical infrastructure, particularly the energy sector. DVEs see such attacks as a means to advance their ideologies and achieve their sociopolitical goals. DVEs, particularly racially motivated violent extremists, have been promoting accelerationism—an ideology that seeks to destabilize society and trigger a race war. They have encouraged mobilization against critical functions, including attacks against the energy, communications, and public health sectors.

Notably, since 2022, there has been a dramatic spike in bomb threats, impacting over 30% of Historically Black Colleges and Universities (HBCUs), inciting fear and panic and resulting in campus evacuations and lockdowns across the nation. DHS has leveraged subject matter expertise and innovation from across the Department to respond and support our communities. For example, DHS created and delivered trainings, products, and resources specific to the threat. The Cybersecurity and Infrastructure Security Agency's (CISA) Office for Bombing Prevention (OBP) provided in-person on-campus training nationwide and hosted 27 virtual courses, ultimately training over 1,250 participants, and providing over 1,500 bomb threat planning and response products.

DHS is committed to providing resources to communities to prevent and respond to incidents of terrorism and targeted violence. We announced $2 billion in preparedness grant funding for this fiscal year, including $305 million for the Nonprofit Security Grant Program (NSGP) to support nonprofit organizations' preparedness activities and enhance broader state and local preparedness efforts. DHS also invested $70 million over the past four years in communities across the United States to help prevent acts of targeted violence and terrorism through the Targeted Violence and Terrorism Prevention (TVTP) Grant Program. Managed by the DHS Center for Prevention Programs and Partnerships (CP3) and the Federal Emergency Management Agency (FEMA), this program provides funding for SLTTC governments, nonprofits, and institutions of higher education to establish or enhance capabilities to prevent

targeted violence and terrorism. In September 2023, DHS announced 34 TVTP grant awards to entities in 22 states, totaling $20 million for Fiscal Year (FY) 2023. These awards fulfill the grant program's focus on prioritizing the prevention of domestic violent extremist acts, while respecting individuals' privacy, civil rights, and civil liberties.

**Nation-State Threats**

The United States faces evolving and increasingly complex threats from nation-state adversaries, including the People's Republic of China (PRC), Russia, Iran, and North Korea. In addition to traditional espionage and intelligence collection, nation-state adversaries likely will continue to conduct malign influence campaigns aimed at undermining trust in U.S. government institutions, social cohesion, and democratic processes. The proliferation and accessibility of emergent cyber and artificial intelligence (AI) tools will likely help these actors bolster their malign information campaigns by enabling the creation of higher quality low-cost, synthetic text, image, and audio-based content.

To augment many of their efforts in the public sphere, the PRC, Iran, and Russia likely will continue to pursue transnational repression activity in the Homeland, undermining U.S. laws, norms, and individuals' rights. Adversaries have targeted individuals in the United States whom they perceive as threats to their regimes, including ethnic and religious minorities, political dissidents, and journalists. Agents of these regimes have been known to use in other countries, and in some circumstances in the United States, physical assaults, threats, harassment, defamation, the manipulation of international law enforcement personnel and processes to suppress oppositional voices, and in limited circumstances, forced disappearances and even assassination. The PRC and Iran likely will remain the most aggressive actors within the United States.

**Cyber Threats**

Our interconnectedness and the technology that enables it—the cyber ecosystem—expose us to dynamic and evolving threats that are not contained by borders or limited to centralized actors, and that can impact governments, the private sector, civil society, and every individual. Hostile regimes like Russia, the PRC, Iran, and North Korea, as well as cybercriminals around the world, continually grow more sophisticated, steal our data and intellectual property, extort ransoms, and threaten our cyber systems. Accordingly, cyber threats from foreign governments and transnational criminals remain among the most prominent threats facing our nation. In recent years, ransomware incidents have become increasingly prevalent among U.S. state, local, Tribal, and territorial governments and critical infrastructure entities, disrupting services.

Malicious cyber activity targeting the United States has increased since Russia's full invasion of Ukraine, a trend we expect to continue throughout the duration of the conflict. Within the past three years, we have seen numerous cybersecurity incidents impacting organizations of all sizes and disrupting critical services, from the Russian government's compromise of the SolarWinds supply chain to the widespread vulnerabilities generated by open-source software like Log4j. We believe there is significant under-reporting of ransomware and other cybersecurity incidents, and we assess that ransomware attacks targeting U.S. networks

will increase in the near- and long-terms. Cybercriminals have developed effective business models to increase their financial gain, likelihood of success, and anonymity.

To respond to evolving cyber threats and increase our nation's cybersecurity and resilience, DHS has established several vehicles. The Joint Cyber Defense Collaborative (JCDC) leads the development and supports the execution of joint cyber defense plans with partners at all levels of government and the private sector to prevent and reduce the impacts of cyber intrusions and to ensure a unified response when they occur.

The Cyber Safety Review Board (CSRB) is a public-private advisory board dedicated to after-action reviews of significant cyber incidents. The Board released its second report in August 2023 on the activities associated with the Lapsus$ group focused on malicious targeting of cloud computing environments and approaches to strengthen identity management and authentication in the cloud. The Board is now initiating its third review of the Microsoft Exchange online intrusions.

Through the Cyber Incident Reporting Council (CIRC), DHS delivered several actionable recommendations to harmonize cyber incident reporting requirements, including establishing model definitions, timelines, and triggers for reportable cyber incidents. It also created a model cyber incident reporting form that federal agencies can adopt and streamlined the reporting and sharing of information about cyber incidents. The CIRC will work with agencies across the government to implement these recommendations.

The Department is committed to keeping Americans safe from the devastating effects of cybercrimes and protecting the nation's critical infrastructure from attacks is a core departmental mission.

**Border Security**

The Department continues to implement a border security strategy focused on enforcement, the expansion of lawful pathways, and agreements with regional partners. The plan has increased the number of law enforcement personnel along the border and expedited removals of noncitizens without a legal basis to remain in the United States thanks to enhanced enforcement processes and historic international agreements. Since May 12, 2023, we have removed or returned over 336,000 individuals, including more than 50,000 individual family unit members. This compares to 225,000 removals and enforcement returns during the same period in 2019, which was the comparable pre-pandemic and pre-Title 42 period. At the same time, we have implemented the largest expansion of lawful pathways in decades. Progress has been made, but more funding is required to manage the unprecedented flow of hemispheric migration and to increase our efforts to combat the Transnational Criminal Organizations (TCOs) ruthlessly trafficking fentanyl and other deadly illicit drugs.

Last month, the Department submitted a supplemental funding request to Congress for $8.7 billion that would fund: additional personnel and investigative capabilities to prevent cartels from moving fentanyl into the country; additional resources for Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and U.S. Citizenship and Immigration

Services (USCIS) to cover projected shortfalls, enhance enforcement and processing efficiencies, and hire additional personnel; and additional support for communities and non-profits receiving migrants through the Shelter and Services Program (SSP). The Department urges Congress to provide this supplemental funding to equip the men and women of DHS with the resources and support they need to achieve our safety and security mission.

*Transnational Criminal Organizations*

TCOs continue to pose a threat to the United States, particularly U.S. public health, as well as our economic and national security. Over the past ten years, they have grown in size, scale, sophistication, and their deadly impact. The increased supply of fentanyl and changes in its production during the last year have increased the lethality of an already deadly drug, a trend likely to persist in 2024. Drug traffickers in Mexico and the United States are using various additives and mixing fentanyl into counterfeit prescription pills, leading to overdoses. Given this trend, we expect fentanyl to remain the leading cause of narcotics-related deaths in the United States. The illegal narcotics trade also harms our communities by supporting violent criminal enterprises, money laundering, and corruption that undermines the rule of law.

TCOs that specialize in human smuggling increasingly exploit and financially benefit from the continued growth in global migration trends. In April 2022, DHS launched a first-of-its-kind effort, unprecedented in scale, to disrupt and dismantle human smuggling networks. To date, this campaign has resulted in the arrest of over 18,000 smugglers, more than 10,000 disruption actions, and more than $60 million seized. This has led to more than 2,000 indictments and more than 1,500 convictions in partnership with U.S. attorneys. U.S. Border Patrol (USBP) has also referred close to 10,000 individuals for prosecution.

*Counternarcotics*

DHS employs a multi-layered approach to mitigating and countering narcotics trafficking and threats of all types using our extensive liaison networks, domestic and foreign partnerships, personnel, and technology deployments such as Non-Intrusive Inspection (NII) capabilities. The increased production and trafficking of synthetic opioids from Mexico have prompted the interagency to implement a whole-of-government approach, including a number of DHS components and efforts, to combat these threats. These efforts have resulted in the seizure of more fentanyl in the past two years than in the prior five years combined: nearly 3.5 million pounds of fentanyl and methamphetamine precursor chemicals since FY 2021.

To further increase our counternarcotics efforts, DHS recently launched targeted enforcement campaigns to combat illicit narcotics, particularly fentanyl. Based on the success of Operation Blue Lotus earlier this year, which seized more than 4,700 pounds of fentanyl and yielded over 250 arrests by CBP and Homeland Security Investigations (HSI), DHS launched further campaigns focused on border and interior facilities to further disrupt and degrade the flow and supply chains that feed the production of fentanyl and other synthetic drugs through coordinated enforcement, investigative, interdiction, and scientific identification efforts. Under Operation Blue Lotus 2.0, CBP and HSI made 155 federal and state arrests, seized 1,680 pounds of fentanyl, 5,000 pounds of fentanyl precursors, and 10,194 pounds of other precursors between

June-July 2023. Operation Artemis efforts have led to well over 500 seizures, including more than 460 pill press related items; 13,000 pounds of fentanyl precursor chemicals; and more than 11,200 pounds of other narcotics between June-September 2023. In August 2023, HSI transitioned to a long-term counter-fentanyl posture, Operation Orion, which leverages HSI authorities and tools to target dark web vendors and other cyber-enabled actors that engage in fentanyl distribution via the internet and increase targeting in strategic field locations. HSI is also attacking the illicit supply chain beyond the border, launching over 135 investigations, leading to 110 criminal arrests and 229 seizures, including the arrests of six high level TCO members, and the disruption of five clandestine synthetic drug labs in Mexico.

The U.S. Coast Guard (USCG) leads maritime interdictions of narcotics in the Western Hemisphere, partnering with nations in South and Central America to combat the flow of narcotics before they reach U.S. shores. USCG intelligence personnel and Coast Guard Investigative Service Special Agents are fully integrated across the Department and at the Joint Interagency Task Force (JIATF) South, allowing for maximum counterdrug coordination across the hemisphere. In FY 2023, the USCG seized approximately 126 metric tons of cocaine, 51,000 pounds of marijuana, and 20 metric tons of other narcotics, including methamphetamines, heroin, and hashish.

**Human Trafficking and Child Sexual Exploitation**

Combating the abhorrent crimes of human trafficking and child sexual exploitation and abuse (CSEA) are top priorities for the Department. These crimes target the most vulnerable among us, offend our most basic values, and threaten our national security and public safety. According to the United Nations' International Labor Organization, human traffickers victimize an estimated 27.6 million people worldwide, with 77 percent subjected to forced labor and 23 percent in sex trafficking. The United States is no exception.

Almost every office and agency in the Department plays a role in our counter-human trafficking mission. The DHS Center for Countering Human Trafficking (CCHT), which was codified by the Countering Human Trafficking Act of 2021, integrates the counter-trafficking efforts of 16 DHS Component agencies and offices to advance counter human trafficking law enforcement operations, protect victims and enhance prevention efforts by aligning DHS's capabilities and expertise. DHS efforts encompass criminal investigations, victim assistance, identifying and reporting human trafficking, external outreach, intelligence, and training. By integrating these many functions, the CCHT enhances every aspect of DHS's counter human trafficking work. HSI leads criminal investigations into sex trafficking and forced labor, making 2,610 human trafficking-related arrests during FY 2023, including 1,045 indictments and leading to 518 convictions.

The Department is also redoubling efforts to combat online CSEA, which has increased dramatically in scope and severity in recent years. New forms of CSEA have also emerged and grown exponentially, including the live streaming of child sexual abuse, child sexual abuse material (CSAM) developed by AI, and sophisticated financial sextortion and grooming schemes.

In response, we are strengthening our HSI Cyber Crimes Center (C3), including the Child Exploitation Investigations Unit (CEIU), a global leader in counter-CSEA law enforcement operations. The CEIU Victim Identification Program (VIP) utilizes state-of-the-art technologies combined with traditional investigative techniques to identify and rescue child victims throughout the world. Since its establishment in 2011, the VIP has identified and/or rescued more than 11,000 child victims of sexual exploitation. CEIU's Operation Predator targets child sexual predators on both the open web and dark web, and in FY 2023 led to the arrest of 4,044 perpetrators for crimes involving child sexual abuse. During this same period, the CEIU Angel Watch Center issued 4,814 notifications regarding international travel by convicted child sex offenders, resulting in more than 1,050 denials of entry by foreign nations.

We also know that we must better educate Americans and work with partners around the world to spread awareness to prevent these crimes before they happen. In the coming months, DHS will launch Know2Protect, which will be the federal government's first national public awareness campaign to educate and empower children, teens, parents, trusted adults, and policymakers to prevent and combat online child sexual exploitation and abuses. The campaign will highlight the Department's existing programs, including HSI's iGuardian program and the U.S. Secret Service's Childhood Smart, in which agents work directly with communities to provide education sessions and resources to combat these crimes and prevent more American children from becoming victims.

**Extreme Weather Events and Climate Change Resilience**

The impacts of climate change pose an acute and systemic threat to the safety, security, and prosperity of the United States, and have already led to changes in the environment, such as rising ocean temperatures, shrinking sea ice, rising sea levels, and ocean acidification. Our changing climate acts as a force multiplier, turning more storms, floods, and fires into events that threaten the well-being of people across our nation. As our climate continues to warm, the United States will experience more climate-related disasters such as heat waves, droughts, wildfires, coastal storms, and inland flooding. Under the Biden-Harris Administration, DHS is engaged in climate change adaptation and mitigation efforts to make the Department and the nation more prepared, more secure, and more resilient.

In February of 2023, DHS became a member of the United States Global Change Research Program (USGCRP). As the first new member of the interagency USGCRP body in nearly two decades, DHS joined as its 14th member. USGCRP's membership consists of agencies that conduct global change research and use it to carry out their mission, creating opportunities for decision-makers to communicate information needs directly to scientists and for scientists to support informed decision-making.

On September 6, 2023, FEMA announced the first 483 Community Disaster Resilience Zones in all 50 states and the District of Columbia. FEMA used the National Risk Index and other tools to identify the census tracts across the country at the highest risk from natural hazards and those most in need. A Community Disaster Resilience Zone designation offers opportunities for public-private partnerships including governments, non-profits, philanthropy, insurance, and

private businesses to collaborate on innovative resilience investment strategies, leveraging the up to 13:1 return on investment for mitigation and resilience projects.

DHS has also made available more than $1.8 billion for the FY 2023 Building Resilient Infrastructure and Communities (BRIC) and Flood Mitigation Assistance (FMA) grant programs, which seek to help SLTT governments address high-level future risks to natural disasters such as extreme heat, wildfires, drought, hurricanes, earthquakes, and increased flooding to foster greater community resilience and reduce disaster suffering.

**Emerging Threats and Opportunities for Mission Advancement**

Advances in AI capabilities can offer tremendous benefits to our society. However, its misuse can also lead to real security challenges. We are committed to DHS leading in this space to both mitigate the harms and harness the benefits of AI. In the past year alone, DHS has shown the way in the responsible use of AI to secure the homeland and in defending against the malicious use of this transformational technology, but we have much more to do. As we move forward, we will ensure that our use of AI is rigorously tested to avoid bias and disparate impact and is clearly explainable to the people we serve.

Last month, the President issued an Executive Order (EO) to promote the safe, secure, and trustworthy development and use of AI. The EO directs DHS to take a lead role in ensuring the safe, secure, and responsible use and development of AI. DHS will manage AI in critical infrastructure and cyberspace, promote the adoption of AI safety standards globally, reduce the risks that AI can be used to create weapons of mass destruction, combat AI-related intellectual property theft, and help to attract and retain skilled talent. The EO follows DHS's innovative work deploying AI responsibly to advance its missions for the benefit of the American people.

DHS recently established the Department's first AI Task Force to drive the responsible use of AI in specific applications to advance our critical homeland security missions. The Task Force is working to enhance the integrity of our supply chains and the broader trade environment by deploying AI to more ably screen cargo, identify the importation of goods produced with forced labor, and manage risk. It is also charged with using AI to better detect fentanyl shipments, identify and interdict the flow of precursor chemicals around the world, and target for disruption key nodes in criminal networks.

I also tasked our Homeland Security Advisory Council to study the intersection of AI and homeland security. In September, the Council delivered findings that will help guide our use of AI and defense against its malicious deployment. The Council also delivered recommendations on keeping pace with technological advances while incentivizing responsible and impactful use of AI for the Department, to enhance and improve our ability to meet our mission in an ethical, informed, and responsible manner.

In September, DHS became the first Department to issue comprehensive face recognition guidance to ensure strong guardrails to protect American liberties. The guidance ensures that all uses of face recognition and face capture technologies will be thoroughly tested to ensure there is

no bias or disparate impact in accordance with national standards. DHS will review all existing uses of this technology and conduct periodic testing and evaluation of all systems to meet performance goals. Furthermore, the directive requires that U.S. citizens be afforded the right to opt-out of face recognition for specific, non-law enforcement uses, and it prohibits face recognition from being used as the sole basis of any law or civil enforcement related action while establishing a process for Department oversight offices, including the Privacy Office, the Office for Civil Rights and Civil Liberties (CRCL), and the Office of the Chief Information Officer, to review all new uses of face recognition and face capture technologies.

**Equipping the Department with the Necessary Tools**

*Countering Unmanned Aerial Systems*

Unmanned Aerial Systems (UASs), or drones, offer tremendous benefits to our economy and society, but their misuse poses real security challenges. DHS has successfully exercised its current counter-UAS (C-UAS) authority in protective operations at mass gatherings, Special Event Assessment Rating (SEAR) events, and National Special Security Events (NSSEs), including the 2022 World Series, the Indianapolis 500, the United Nations General Assembly, the Democratic and Republican National Conventions, the State of the Union address, the MLB All Star Game, the New York City Marathon, and the Boston Marathon. At all times, DHS engages in these activities consistent with applicable law and in a manner that protects individuals' privacy, civil rights, and civil liberties.

DHS's current C-UAS authority is set to expire on November 18, 2023. Ensuring that existing authorities do not lapse is vital to our mission, including protecting the President and Vice President, patrolling certain designated areas along the Southwest Border, securing certain federal facilities and assets, and safeguarding the public. Any lapse in DHS's current C-UAS authority would entail serious risks for our homeland security, as DHS would have to cease or curtail existing C-UAS operations. Congressional action is required for a long-term extension and expansion of C-UAS authority, and to prevent any lapse in C-UAS authority on November 18, 2023.

To ensure the Department can continue its C-UAS activities, including protecting the 2026 World Cup events, both the Department and the Administration remain committed to a multi-year extension as well as an expansion of existing authorities. The Department and Administration appreciate Congress considering and acting on S. 1631 and H.R. 4333, because both bills would address the need for long-term authority, while closing vulnerabilities by expansion of DHS's C-UAS authority. Specifically, the Department and the Administration look forward to working with Congress, including this Committee, to expand C-UAS authority to address critical gaps in the current law, such as insufficient protection for U.S. airports and the inability of DHS to partner on C-UAS activities with SLTT enforcement officials or critical infrastructure owners or operators. These two bills, S.1631 and H.R. 4333, if enacted, would provide the needed extension of C-UAS authority and close real gaps in our ability to protect the Homeland.

*Countering Weapons of Mass Destruction*

Although terrorist capabilities to conduct large-scale attacks have been degraded by U.S. counterterrorism operations and policies, terrorists remain interested in acquiring and using weapons of mass destruction (WMD) in attacks against U.S. interests and the Homeland. Congress established the DHS Countering Weapons of Mass Destruction Office (CWMD) in 2018 to elevate, consolidate, and streamline DHS efforts to protect the Homeland from WMD and chemical, biological, radiological, and nuclear (CBRN) threats. CWMD serves as the DHS nexus for WMD and CBRN coordination, which includes providing direct support to both our government and industry partners. Of significant concern is DHS's ability to continue the mission to counter WMDs after the authorization for CWMD terminates on December 21, 2023. DHS's tools to accomplish this mission are at risk.

The CWMD Office has primary authority and responsibility within DHS to protect the Homeland against CBRN threats by interpreting national strategies and developing departmental strategic guidance; monitoring and reporting on related threats; generating and distributing related risk assessments; and researching, developing, acquiring, and deploying operationally effective solutions, such as equipment, training, and exercises, in support of SLTT communities and Departmental Components. CWMD strengthens DHS-wide and federal interagency coordination and provides direct financial and operational support nationwide to SLTT partners who serve as first-responders. Additionally, as part of the President's EO on AI, CWMD was tasked with helping to evaluate and mitigate the potential for AI to be used to develop WMDs, such as through AI-enabled misuse of synthetic nucleic acids to create biological weapons. If CWMD authorization is allowed to expire, not only will DHS not be able to support these AI efforts, but over $130 million in annual grants will cease to support state and local first responders for full time biological detection, illicit nuclear material detection, training, and exercises. CWMD will also cease important CBRN research to improve security standards and equipment for SLTTs and DHS, including threat detection and prevention at large events.

*Chemical Facility Anti-Terrorism Standards*

Chemical Facility Anti-Terrorism Standards (CFATS) is the nation's first regulatory program focused specifically on security at high-risk chemical facilities. Managed by CISA, the CFATS program identifies and regulates high-risk facilities to ensure security measures are in place to reduce the risk that certain dangerous chemicals can be weaponized by terrorists. An attack on one of these U.S. sites could be as lethal as a nuclear blast. On July 28, 2023, DHS authorities to implement the CFATS expired, and the program ceased to operate. With the expiration of the program, DHS can no longer reassure the more than 3,200 communities surrounding chemical facilities at high risk of terrorist attack that everything is being done to ensure those chemicals are protected.

As of today, we have no longer been authorized to conduct over 450 inspections, when historically more than a third of inspections identify at least one gap in a facility's security. We have lost crucial visibility, with likely more than 100 facilities having newly acquired chemicals without reporting them, resulting in the inability of CISA to conduct risk assessments of these facilities. Cybersecurity and physical security measures at these sites are being allowed to lapse,

and government planners and first responders are forced to rely on out-of-date information about what civilian industry chemical stores exist in their areas of responsibility.

It is critical to the DHS mission and the safety of the Homeland that Congress reauthorize the Department's C-UAS authority, the CFATS program, and the CWMD Office without delay. These programs are vital to protecting our communities against drones, WMDs, and other related CBRN threats.

*Intelligence and Analysis Authorities*

It is also imperative that Congress protect two important intelligence collection authorities that are currently under debate. The first is Section 702 under the Foreign Intelligence Surveillance Act, which will expire unless Congress reauthorizes it by the end of this year. Section 702 allows our Intelligence Community to conduct the overseas electronic surveillance that produces much of our nation's most critical intelligence about our foreign adversaries and their plans and intentions. It would significantly diminish our national security if that authority were allowed to expire.

It is similarly important that Congress resist the proposed language in the Senate's version of the Intelligence Authorization Act that would curtail the authority of our Office of Intelligence & Analysis (I&A) to collect intelligence bearing on our homeland security. This provision would significantly limit the ability of our I&A collection professionals to generate the intelligence they use to warn our federal, state, local, territorial, Tribal and private sector partners about the threats facing them and the Homeland.

Both of these authorities are critical to our homeland security. While Congress should certainly consider any reasonable additions to the comprehensive regime of privacy and civil liberties safeguards under which they operate, it must keep both authorities in place and available to the Intelligence Community. These authorities have produced intelligence over the years that has been vital to our homeland security, and that intelligence is all the more vital now in light of the threat environment we are facing in the aftermath of the Hamas attacks in Israel.

**Conclusion**

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

# Department of Justice

**STATEMENT OF**

**CHRISTOPHER A. WRAY**
**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 15, 2023**

**STATEMENT OF**
**CHRISTOPHER A. WRAY**
**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 15, 2023**

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

Despite the many challenges our FBI workforce has faced, I am immensely proud of their dedication to protecting the American people and upholding the Constitution. Our country continues to face 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 prepared to discuss with you what the FBI is doing to address these threats and what the FBI is doing to ensure our people adhere to the highest of standards while it conducts its mission.

## Key Threats and Challenges

Our Nation continues to face a multitude of serious and evolving threats ranging from homegrown violent extremists ("HVEs") to hostile foreign intelligence services and operatives, from sophisticated cyber-based attacks to internet facilitated sexual exploitation of children, from violent gangs and criminal organizations to public corruption and corporate fraud. Keeping pace with these threats is a significant challenge for the FBI. As an organization, we must be able to stay current with constantly evolving technologies. Our adversaries take advantage of modern technology, including the internet and social media, to 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. We are hiring 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.

## National Security

### *Terrorism Threats*

As we saw earlier this month with the devastating attack in Israel, terrorist actors are still very intent on using violence and brutality to spread their ideologies. Protecting the American people from terrorism remains the FBI's number one priority. The threat from terrorism is as persistent and complex as ever. We are in an environment where the threats from international terrorism, domestic terrorism, and state-sponsored terrorism are all simultaneously elevated.

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

Domestic and Homegrown Violent Extremists are often motivated and inspired by a mix of social or political, ideological, and personal grievances against their targets, and more recently

have focused on accessible targets to include civilians, law enforcement and the military, symbols or members of the U.S. government, houses of worship, retail locations, and mass public gatherings. Lone actors present a particular challenge to law enforcement and intelligence agencies. These actors are difficult to identify, investigate, and disrupt before they take violent action, especially because of the insular nature of their radicalization and mobilization to violence and limited discussions with others regarding their plans.

The top domestic terrorism threat we face continues to be from DVEs we categorize as Racially or Ethnically Motivated Violent Extremists ("RMVEs") and Anti-Government or Anti-Authority Violent Extremists ("AGAAVEs"). The number of FBI domestic terrorism investigations has more than doubled since the spring of 2020. As of September 2023, the FBI was conducting approximately 2,700 investigations within the domestic terrorism program. As of September 2023, the FBI was also conducting approximately 4,000 investigations within its international terrorism program.

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

The FBI assesses HVEs as the greatest, most immediate international terrorism threat to the homeland. HVEs are people located and radicalized to violence primarily in the United States, who are not receiving individualized direction from FTOs but are inspired by FTOs, including the self-proclaimed Islamic State of Iraq and ash-Sham ("ISIS") and al-Qa'ida and their affiliates, to commit violence. An HVE's lack of a direct connection with an FTO, ability to rapidly mobilize without detection, and use of encrypted communications pose significant challenges to our ability to proactively identify and disrupt potential violent attacks.

While we work to assist our Israeli colleagues and understand the global implications of the ongoing conflict in Israel, we are paying heightened attention to how the events abroad could directly affect and inspire people to commit violence here in the Homeland. Terrorist organizations worldwide, as well as individuals attracted to violence, have praised HAMAS's horrific attack on Israeli civilians. We have seen violent extremists across ideologies seeking to target Jewish and Muslim people and institutions through physical assaults, bomb threats, and online calls for mass casualty attacks. Our top concern stems from lone offenders inspired by—or reacting to—the ongoing Israel-HAMAS conflict, as they pose the most likely threat to Americans, especially Jewish, Muslim, and Arab-American communities in the United States. We have seen an increase in reported threats to Jewish and Muslim people, institutions, and houses of worship here in the United States and are moving quickly to mitigate them.

As of right now, we have no information to indicate that HAMAS has the intent or capability to conduct operations inside the US, though we cannot, and do not, discount that possibility, but we are especially concerned about the possibility of HAMAS supporters engaging in violence on the group's behalf. As always, we are concerned with any foreign

terrorist organization who may exploit the attacks in Israel as a tool to mobilize their followers around the world. In recent years, there have been several events and incidents in the United States that were purportedly motivated, at least in part, by the conflict between Israel and HAMAS. These have included the targeting of individuals, houses of worship, and institutions associated with the Jewish and Muslim faiths with acts of physical assault, vandalism, or harassment. Anti-Semitism and anti-Islamic sentiment permeate many violent extremist ideologies and serves as a primary driver for attacks by a diverse set of violent extremists who pose a persistent threat to Jewish and Muslim communities and institutions in the United States and abroad. Foreign terrorist organizations have exploited previous conflicts between Israel and HAMAS via media outlets and online communications to call on their supporters located in the United States to conduct attacks. Some violent extremists have used times of heightened tensions to incite violence against religious minorities, targeting both Jewish and Muslim Americans.

The FBI remains concerned about the Taliban takeover of Afghanistan and that the intent of FTOs, such as ISIS and al-Qa'ida and their affiliates, is to carry out or inspire large-scale attacks in the United States.

Despite its loss of physical territory in Iraq and Syria, ISIS remains relentless in its campaign of violence against the United States and our partners—both here at home and overseas. ISIS and its supporters continue to aggressively promote its hate-fueled rhetoric and attract like-minded violent extremists with a willingness to conduct attacks against the United States and our interests abroad. ISIS's successful use of social media and messaging applications to attract individuals is of continued concern to us. Like other foreign terrorist groups, ISIS advocates for lone offender attacks in the United States and Western countries via videos and other English language propaganda that have specifically advocated for attacks against civilians, the military, law enforcement and intelligence community personnel.

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

Iran and its global proxies and partners, including Iraqi Shia militant groups, attack and plot against the United States and our allies throughout the Middle East. Iran's Islamic Revolutionary Guard Corps-Qods Force ("IRGC-QF") has too provided support to militant resistance groups and terrorist organizations. And Iran has supported Lebanese Hizballah and other terrorist groups. Hizballah has sent operatives to build terrorist infrastructures worldwide. The arrests of individuals in the United States allegedly linked to Hizballah's main overseas terrorist arm, and their intelligence-collection and -procurement efforts, demonstrate Hizballah's interest in long-term contingency planning activities here in the Homeland. Hizballah Secretary-General Hassan Nasrallah also has threatened retaliation for the death of IRGC-QF Commander

Qassem Soleimani. This willingness to seek retaliation against the United States was reflected in charges the Department brought in 2022 against a member of the IRGC, working on behalf of the Qods Force, who was plotting to murder a former national security advisor.

While the terrorism threat continues to evolve, the FBI's resolve to counter that threat remains constant. We continually adapt and rely heavily on the strength of our federal, state, local, tribal, territorial, and international partnerships to combat all terrorist threats to the United States and our interests. To that end, we use all available lawful investigative techniques and methods to combat these threats while continuing to collect, analyze, and share intelligence concerning the threats posed by violent extremists who desire to harm Americans and U.S. interests. We will continue to share information and encourage the sharing of information among our numerous partners via our Joint Terrorism Task Forces across the country, and our legal attaché offices around the world.

In addition to fighting terrorism, countering the proliferation of weapons-of-mass-destruction materials, technologies, and expertise, preventing their use by any actor, and securing nuclear and radioactive materials of concern are also top national security priority missions for the FBI. The FBI considers preventing, mitigating, investigating, and responding to weapons of mass destruction ("WMD") terrorism a "no-fail" mission because a WMD attack could result in substantial injuries, illness, or loss of lives, while yielding significant social, economic, political, and other national security consequences. In collaboration with federal, state, local, tribal, territorial, and other partners, the FBI integrates complementary efforts to counter WMD terrorism. An example of this collaboration is the FBI-led Weapons of Mass Destruction Strategic Group. This interagency crisis action team spans more than fifteen departments and agencies to coordinate the federal government's response to WMD threats and incidents. Alongside the FBI, the Department of Homeland Security maintains the largest footprint on the Strategic Group.

***Cyber***

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

These criminals and nation-states believe that they can compromise our networks, steal our property, extort us, and hold our critical infrastructure at risk without incurring any risk themselves. In the last few years, we have seen the People's Republic of China ("PRC"), the Democratic People's Republic of Korea ("DPRK"), and Russia use cyber operations to target U.S. research. We have seen the PRC working to obtain controlled dual-use technology, while developing an arsenal of advanced cyber capabilities that could be used against other countries in the event of a real-world conflict. And we have seen the disruptive impact a serious supply-chain compromise can have through the SolarWinds-related intrusions, conducted by the Russian Foreign Intelligence Service. As these adversaries become more sophisticated, we are

increasingly concerned about our ability to detect specific cyber operations against U.S. organizations. One of the most worrisome facets is their focus on compromising U.S. critical infrastructure, especially during a crisis.

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

So, as dangerous as nation-states are, we do not have the luxury of focusing on them alone. In the past year, we also have seen cybercriminals target hospitals, medical centers, educational institutions, and other critical infrastructure for theft or ransomware, causing massive disruption to our daily lives. Incidents affecting medical centers have led to the interruption of computer networks and systems that put patients' lives at an increased risk.

We have also seen the rise of an ecosystem of services dedicated to supporting cybercrime in exchange for cryptocurrency. Criminals now have new tools to engage in destructive behavior—for example, deploying ransomware to paralyze entire hospitals, police departments, and businesses—as well as new means to better conceal their tracks. It is not that individual malicious cyber actors have necessarily become much more sophisticated, but that they can now more easily rent sophisticated capabilities.

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

An example of this approach is the coordinated international operation announced in April 2023 against Genesis Market, a criminal online marketplace offering access to data stolen from over 1.5 million compromised computers around the world containing over 80 million account access credentials. Genesis Market was also a prolific initial access broker in the cybercrime world, providing criminals a user-friendly database to search for stolen credentials and more easily infiltrate victims' computers and accounts. As part of this operation, law enforcement seized 11 domain names used to support Genesis Market's infrastructure pursuant to a warrant authorized by the U.S. District Court for the Eastern District of Wisconsin. A total of 22 international agencies and 44 FBI field offices worked with the FBI Milwaukee Field Office investigating the case. And on April 5, the U.S. Department of the Treasury announced sanctions against Genesis Market.

In total, along with our colleagues at the Department of Justice ("DOJ"), we took over 1,000 actions against cyber adversaries in 2022, including arrests, criminal charges, convictions, dismantlements, and disruptions. We enabled many more actions through our dedicated partnerships with the private sector, with foreign partners, and with federal, state, and local entities. We also provided thousands of individualized threat warnings and disseminated 70 public threat advisories by way of Joint Cybersecurity Advisories, FBI Liaison Alert System ("FLASH") reports, Private Industry Notifications ("PINs"), and Public Service Announcements ("PSAs")—many of which were jointly authored with other U.S. agencies and international partners.

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

In summary, the FBI is engaged in myriad efforts to combat cyber threats, from improving threat identification and information sharing inside and outside of the government to developing and retaining new talent, to examining the way we operate to disrupt and defeat these threats. We take all potential threats to public and private sector systems seriously, and will continue to investigate and hold accountable those who pose a threat in cyberspace.

### *Foreign Intelligence Threats*

#### Top Threats

Nations such as the PRC, Russia, and Iran are becoming more aggressive and more capable than ever before. These nations seek to undermine our core democratic, economic, 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.

With that, the greatest long-term threat to our nation's ideas, innovation, and economic security is the foreign intelligence and economic espionage threat from the PRC. By extension, it is also a threat to our national security. . The PRC government aspires to reshape the international rules-based system to its benefit. Often, with little regard for international norms and laws.

When it comes to economic espionage, the PRC uses every means at its disposal, blending cyber, human intelligence, diplomacy, corporate transactions, and other pressure on U.S. companies operating in the PRC, to steal our companies' innovations. These efforts are consistent with the PRC government's expressed goals to become an international power, modernize its military, and create innovation-driven economic growth.

To pursue this goal, the PRC uses human intelligence officers, co-optees, and corrupt corporate insiders, as well as sophisticated cyber intrusions, pressure on U.S. companies in China, shell-game corporate transactions, and joint-venture "partnerships" that are anything but a true partnership. There is nothing traditional about the scale of their theft. It is unprecedented. American workers and companies are facing a greater, more complex danger than they have dealt with before. Stolen innovation means stolen jobs, stolen opportunities for American workers, and stolen national power.

**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 these multi-agency counterintelligence operations, and to programmatically support local Counterintelligence Task Force ("CITF") operations. Combining the authorities and operational capabilities of the U.S. Intelligence Community, 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 Defense ("DOD") has been a key partner in the NCITF since its founding. While the FBI has had long-term collaborative relationships with DOD entities such as the Air Force Office of Special Investigations, Naval Criminal Investigative Service, and Army Counterintelligence, the NCITF has allowed us to enhance our collaboration for greater impact. We plan to emphasize this whole-of-government approach as a powerful formula to mitigate the modern counterintelligence threat.

**Transnational Repression and Other Counterintelligence Threats**

In recent years, we have seen a rise in efforts by authoritarian regimes to interfere with freedom of expression and punish dissidents abroad. These acts of repression cross national borders, often reaching into the United States. Governments such as the PRC, the Russian Federation, and the Government of Iran stalk, intimidate, and harass ex-patriots or dissidents who speak against the regime from the United States.

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

In addition, our Nation is confronting multifaceted foreign threats seeking both to influence our national policies and public opinion and to harm our national dialogue and debate. The FBI and our interagency partners remain focused on foreign malign influence operations, including subversive, undeclared, coercive, and criminal actions used by foreign governments in their attempts to sway U.S. citizens' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic institutions and processes.

Foreign malign influence is not a new problem, but the interconnectedness of the modern world, combined with the anonymity of the internet, have changed the nature of the threat. The FBI is the lead Federal agency responsible for investigating foreign malign influence threats. Several years ago, we established the Foreign Influence Task Force ("FITF") to identify and counteract foreign malign influence operations targeting the United States. The FITF is led by our Counterintelligence Division, and comprises agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative divisions. It is specifically charged with identifying and combating foreign malign influence operations targeting democratic institutions inside the United States.

The domestic counterintelligence environment is more complex than ever. We face a persistent and pervasive national security threat from foreign adversaries, particularly the governments of China and Russia, and Iran, who conduct sophisticated intelligence operations using coercion, subversion, malign influence, cyber and economic espionage, traditional spying, and non-traditional human intelligence collection. Together, they pose a continuous threat to U.S. national security and our economy by targeting strategic technologies, industries, sectors, and critical infrastructure. Historically, these asymmetric national security threats involved foreign intelligence service officers seeking U.S. government and U.S. Intelligence Community information. Now, however, the FBI has observed foreign adversaries employing a wide range of nontraditional collection techniques, including the use of human collectors not affiliated with

intelligence services, foreign investment in critical U.S. sectors, and infiltration of U.S. supply chains. The FBI continues to adjust our counterintelligence priorities to address this evolution.

## 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*

Violent crimes and gang activities exact a high toll on individuals and communities. Many of today's gangs are sophisticated and well organized. They use violence to control neighborhoods and boost their illegal money-making activities, which include robbery, human trafficking, drug and gun trafficking, fraud, extortion, and prostitution rings. These gangs do not limit their illegal activities to single jurisdictions or communities. The FBI is vital to this fight in big cities and small towns throughout the Nation because we are able to cross jurisdictions and investigate wherever the evidence leads.

Every day, FBI special agents partner with federal, state, local, territorial, and tribal officers and deputies on joint task forces and on individual investigations. FBI joint task forces—Violent Crime Safe Streets, Violent Gang Safe Streets, and Safe Trails—focus on identifying and targeting major groups operating as criminal enterprises. Much of the FBI criminal intelligence is derived from our state, local, territorial, and tribal law enforcement partners, who know their communities inside and out. Joint task forces benefit from FBI surveillance assets, and our sources track these gangs to identify emerging trends. Through these multi-subject and multi-jurisdictional investigations, the FBI concentrates its efforts on high-level groups engaged in criminal conspiracies and patterns of racketeering. This investigative model enables us to target senior gang leadership and develop enterprise-based prosecutions.

By way of example, the FBI has dedicated tremendous resources to combat the threat of violence posed by MS-13. The atypical nature of this gang has required a multi-pronged approach. We work through our task forces here in the United States, while simultaneously gathering intelligence and aiding our international law enforcement partners. We do this through the FBI's Transnational Anti-Gang Task Forces. Established in El Salvador in 2007 through the FBI's National Gang Task Force, Legal Attaché San Salvador, and the United States Department of State, each Anti-Gang Task Force is responsible for the investigation of, primarily, MS-13 operations in the northern triangle of Central America and the United States. This program combines the expertise, resources, and jurisdiction of participating agencies to investigate and counter transnational criminal gang activity in Central America and the United States. There are now Transnational Anti-Gang Task Forces in El Salvador, Guatemala, and Honduras. Through

these combined efforts, the FBI has achieved substantial success in countering the MS-13 threat across Central America and the United States.

***Transnational Organized Crime ("TOC")***

More than a decade ago, organized crime was characterized by hierarchical organizations, or families, that exerted influence over criminal activities in neighborhoods, cities, or states. But organized crime has changed dramatically. Today, international criminal enterprises run multinational, multibillion-dollar schemes from start to finish. Modern-day criminal enterprises are flat, fluid networks with global reach. While still engaged in many of the "traditional" organized crime activities of loan-sharking, extortion, and murder, modern criminal enterprises are also involved in trafficking counterfeit prescription drugs containing fentanyl, targeting stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, illicit drug trafficking, identity theft, human trafficking, money laundering, alien smuggling, public corruption, weapons trafficking, kidnapping, and other illegal activities.

TOC networks exploit legitimate institutions for critical financial and business services that enable the storage or transfer of illicit proceeds. Preventing and combating transnational organized crime demands a concentrated effort by the FBI and federal, state, local, tribal, territorial, and international partners.

As part of our efforts to combat the TOC threat, the FBI is focused on the cartels trafficking narcotics across our border. The FBI has 328 pending investigations linked to cartel leadership and 78 of those investigations are along the southern border. Additionally, the FBI actively participates in 17 Organized Crime Drug Enforcement Task Forces ("OCDETF") across the United States, investigating major drug trafficking, money laundering, and other high priority transnational organized crime networks. On top of that, we are pursuing healthcare fraud investigations against medical professionals and pill mills through our prescription drug initiative, investigating the gangs and criminal groups responsible for distributing substances like fentanyl through our Safe Streets Task Forces, and disrupting and dismantling Darknet marketplaces that facilitate the sale of counterfeit prescription opioids and other illicit drugs through our Joint Criminal Opioid Darknet Enforcement team.

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

***Crimes Against Children and Human Trafficking***

Every year, thousands of children become victims of crimes, whether it is through kidnappings, violent attacks, sexual abuse, human trafficking, or online predators. The FBI is uniquely positioned to provide a rapid, proactive, and comprehensive response. We help identify, locate, and recover child victims. Our strong relationships with federal, state, local, territorial, tribal, and international law enforcement partners also help to identify, prioritize, investigate, and deter individuals and criminal networks from exploiting children.

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

Another growing area of concern involving the sexual exploitation of children is the explosion in incidents of children and teens being coerced into sending explicit images online and extorted for money. Known as financial sextortion, in 2022, law enforcement received over 13,000 reports of this type of crime, resulting in at least 12,600 victims here and abroad, and more than 20 suicides. A large percentage of these sextortion schemes originate outside the United States, primarily in West African countries such as Nigeria and Ivory Coast. The FBI continues to collaborate with other law enforcement partners and the National Center for Missing and Exploited Children to mitigate this criminal activity and provide the public with informational alerts and victim resources regarding these crimes.

The FBI has several programs in place to arrest child predators and to recover missing and endangered children. To this end, the FBI funds or participates in a variety of endeavors, including our Innocence Lost National Initiative, Innocent Images National Initiative, Operation Cross Country, Child Abduction Rapid Deployment Team, Victim Services, over 80 Child Exploitation and Human Trafficking Task Forces, over 74 International Violent Crimes Against Children Task Force officers, as well as numerous community outreach programs to educate parents and children about safety measures they can follow. Through improved communications, the FBI is able to collaborate with partners throughout the world quickly, playing an integral role in crime prevention.

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

The FBI also focuses efforts to stop human trafficking of both children and adults. The FBI works collaboratively with law enforcement partners to disrupt all forms of human trafficking through Human Trafficking Task Forces nationwide. One way the FBI combats this pernicious crime problem is through investigations such as Operation Cross Country. Over a

two-week period in 2023, the FBI, along with other federal, state, local, and tribal partners, executed approximately 350 operations to recover survivors of human trafficking and disrupt traffickers. These operations identified and located 59 minor victims of child sex trafficking, child sexual exploitation, or related state offenses and located 59 actively missing children. Furthermore, the FBI and its partners located 141 adults who were identified as potential victims of sexual exploitation, human trafficking, or related state offenses. In addition to identifying and recovering missing children and potential victims, the law enforcement activity conducted during Operation Cross Country led to the identification or arrest of 126 suspects implicated in potential child sexual exploitation, human trafficking, or related state or federal offenses.

Although many victims of human trafficking recovered by the FBI are adult U.S. citizens, the FBI and its partners recognize that foreign nationals, children, and other vulnerable populations are disproportionately harmed by both sex and labor trafficking. We take a victim-centered, trauma-informed approach to investigating these cases and strive to ensure the needs of victims are fully addressed at all stages. To accomplish this, the FBI works in conjunction with other law enforcement agencies and victim specialists on the federal, state, local, and tribal levels, as well as with a variety of vetted non-governmental organizations. Even after the arrest and conviction of human traffickers, the FBI often continues to work with partner agencies and organizations to assist victims and survivors in moving beyond their exploitation.

**Reauthorization of Section 702 of the Foreign Intelligence Surveillance Act**

Before closing, I would be remiss if I did not underscore an urgent legislative matter directly relevant to our discussion today. As the committee knows, at the end of December, Section 702 and other provisions of the Foreign Intelligence Surveillance Act (FISA) will expire unless renewed.

Loss of this vital provision, or its reauthorization in a narrowed form, would raise profound risks. For the FBI in particular, either outcome could mean substantially impairing, or in some cases entirely eliminating, our ability to find and disrupt many of the most serious security threats I described earlier in my statement.

I am especially concerned about one frequently discussed proposal, which would require the government to obtain a warrant or court order from a judge before personnel could conduct a "U.S. person query" of information previously obtained through use of Section 702. A warrant requirement would amount to a de facto ban, because query applications either would not meet the legal standard to win court approval; or because, when the standard could be met, it would be so only after the expenditure of scarce resources, the submission and review of a lengthy legal filing, and the passage of significant time—which, in the world of rapidly evolving threats, the government often does not have. That would be a significant blow to the FBI, which relies on this longstanding, lawful capability afforded by Section 702 to rapidly uncover previously hidden threats and connections, and to take swift steps to protect the homeland when needed.

To be sure, no one more deeply shares Members' concerns regarding past FBI compliance violations related to FISA, including the rules for querying Section 702 collection using U.S. person identifiers, than I do. These violations never should have happened and preventing recurrence is a matter of utmost priority. The FBI took these episodes seriously and responded rigorously, already yielding significant results in dramatically reducing the number of "U.S. person queries" by the FBI of the Section 702 database and in substantially improving its compliance rate. Moreover, as we publicly announced in June, the FBI is implementing further measures both to keep improving our compliance and to hold our personnel accountable for misuse of Section 702 and other FISA provisions, including through an escalating scheme for employee accountability, including discipline and culminating in possible dismissal.

Together with other leaders of the Intelligence Community and the Department of Justice, I remain committed to working with this committee and others in Congress, on potential reforms to Section 702 that would not diminish its critical intelligence value. There are many options for meaningfully enhancing privacy, oversight, and accountability, while fully preserving Section 702's efficacy. Doing that will be critical to fulfilling the FBI's continuing mission of identifying and stopping national security threats within the U.S. homeland.

## 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.

Chairman Green, Ranking Member Thompson, and Members of the Committee, thank you for the opportunity to testify today. I am happy to answer your questions.

**United States House Committee on Homeland Security**

**Annual Threat Assessment to the Homeland**

**Statement for the Record**

**Ms. Christine Abizaid**

**Director, National Counterterrorism Center**

**November 15, 2023**

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

I want to begin by addressing the recent attacks by HAMAS and the terrorism implications of the ongoing events, especially within the context of the threat to the Homeland. (U)

We continue to closely monitor, evaluate, and take appropriate actions with respect to potential threats to the United States in the wake of the 7 October HAMAS attacks against Israel and the resulting regional tensions. We are sharing relevant information with our federal state, local, and international law enforcement, intelligence, defense, and homeland security partners to ensure they are prepared for any threats. More broadly, we are monitoring the actions of a range of terrorist actors for key signs of terrorist escalation, including from Iran-aligned proxies in the region; al-Qa'ida and ISIS branches and affiliates from West Africa to Southeast Asia; and other terrorist organizations or lone actors who may seek to exploit the conflict. We are committed to analyzing, tracking, and enabling the disruption of threats targeting Americans abroad, and Jewish, Muslim, and Arab communities within the United States. Since 7 October, there have been increased threats to these communities worldwide, and some attacks and violent exploitation of protests, primarily driven by overall heightened tensions and individuals engaging in violent extremist attacks. My colleagues will address other threats by individuals mobilizing to violence driven at least in part by the current conflict. (U)

The cascading effects of HAMAS's brutal and highly complex attacks inside of Israel underscore the need for vigilance against a diverse array of terrorist actors who retain the capability and intent to conduct operations against the United States and our interests. Today's Middle East conflict and the potential implications thereof hits center-mass for a national CT effort that otherwise had been tracking an overall reduced threat emanating from ISIS and al-Qa'ida in the region and was adjusting to a more discrete, though geographically dispersed, terrorist threat. (U)

How this conflict unfolds in the coming days, weeks and months – and the degree to which it may help renew otherwise declining terrorist actors across the globe – will require careful monitoring. In the meantime, the United States must be careful to preserve the capabilities to address an inherently unpredictable range of terrorist adversaries and enable agile responses to emerging threats and crises, even as we confront a myriad of other national security challenges that play out both overseas and in the United States. (U)

**Terrorist Trends of Concern (U)**

NCTC's approach to evaluating the terrorist threat to the United States factors in the current capability and intent of various terrorist actors and the conditions under which they operate. These categories of terrorists and threat actors generally align as violent Sunni extremist groups such as ISIS and al-Qa'ida; Iran and Iranian-aligned terrorist groups such as Lebanese Hizballah, some militant groups in Iraq and Syria, the Yemen-based Huthis, HAMAS, and Palestinian Islamic Jihad (PIJ); and Homegrown Violent Extremists (HVEs) and other lone actors such as Racially or Ethnically Motivated Violent Extremists (RMVEs) with a foreign nexus. (U)

CT pressure by the United States and foreign partners during the last 15 years has been critical in degrading the capabilities of the most concerning threats, particularly by disrupting experienced leaders and operatives and exerting sustained pressure against key networks. Consistent with the last two years of testimony to this committee, we assess the most likely threat in the United States is from lone actors, whether inspired by violent Sunni extremist narratives, racially or ethnically motivated drivers to violence, or other politically motivated violence. This is not to say that the threat from organized

foreign terrorist groups is gone. Indeed, despite success at deterring sophisticated, hierarchically-directed terrorist attacks in the Homeland since 2001, as of 2022, terrorism threat reporting remained at roughly the same level as in 2010, when al-Qa`ida was at its relative peak, before the death of Usama bin Ladin and rise of ISIS. Today's current conflict will undoubtedly fuel even more threat reporting. (U)

As we evaluate that reporting beyond the dynamic of the Israel-HAMAS conflict, three key themes characterize our leading CT challenges: regional expansion of global terrorist networks despite degradation of their most externally focused elements; the growing danger from state involvement with terrorism; and, as mentioned above, the reality that lone actors are the most likely to succeed in carrying out terrorist attacks. (U)

### ***Regional Shifts by ISIS and Al-Qa'ida*** **(U)**

The United States is safer today because of the suppression of the most dangerous elements of ISIS and al-Qa`ida's global networks. Thanks in large part to American and regional partner CT operations, both organizations have suffered significant losses of key personnel and sustained CT pressure is constraining their efforts to rebuild in historical operating areas. Al-Qa'ida is at a low point in Afghanistan and Pakistan, where its revival is unlikely because it has lost target access, leadership talent, group cohesion, rank-and-file commitment, and an accommodating local environment. Meanwhile, since early 2022, ISIS has lost three overall leaders and more than a dozen other senior leaders in Iraq, Syria, and Somalia—including some who had been involved in planning attacks outside the region—as a result of pressure from the United States and international allies, regional governments, and local opposition forces. (U)

These terrorist losses have been partially offset by an increased external threat from ISIS-Khorasan in Afghanistan and the expansion of both ISIS and al-Qa'ida networks across Africa, although these remain largely regionally focused. Thus far ISIS-Khorasan has relied primarily on inexperienced operatives in Europe to try to advance attacks in its name and, in Afghanistan, Taliban operations have for now prevented the branch from seizing territory that it could use to draw in and train foreign recruits for more sophisticated plots. That said, given Afghanistan's history and the mix of terrorist and

insurgent groups that have long operated from its territory, a top CT priority remains protecting against threats emerging from that country. (U)

In North and West Africa, we are concerned that the erosion of democratic norms and the withdrawal of some traditional partners could further embolden terrorist groups who already pose a threat to U.S. interests in the Sahel. Al-Shabaab in East Africa has become al-Qa'ida's largest, wealthiest, and most lethal affiliate. The Somalia-based group has demonstrated the capability to carry out attacks across the region, including against U.S. personnel. (U)

In the Middle East, Al-Qa'ida in the Arabian Peninsula (AQAP) remains al-Qa'ida's most dedicated driver of external plotting despite its own losses of key personnel and resources. Remaining senior members of the Yemen-based group continue to produce media reinforcing the cohesion of al-Qa'ida's global network as well as calls for attacks against our interests globally. How AQAP, ISIS, or other regional groups may seek to capitalize on HAMAS' 7 October attack to recruit and rebuild anti-West attack capabilities will be critical to assess as tensions and violence rise as the conflict continues. (U)

### ***Iran as Quintessential State Sponsor of Terrorism*** **(U)**

Our CT enterprise remains focused on the Iranian Government's persistent global activity, including in the Homeland, targeting multiple populations over the past four years, such as Israeli or Jewish interests; Iranian dissidents; and U.S. officials in retaliation for the death of IRGC-QF Commander Qasem Soleimani in 2020. Lebanese Hizballah, a number of Iran-aligned militant groups in Iraq and Syria, the Huthis, PIJ, and HAMAS all have long-standing relationships with Iran and have received materiel, financial support, and training from Iran. These groups and surrogates pose an asymmetric threat to the United States and Israel, and the prospect of the Iranian Government's provision of more lethal and sophisticated capabilities to them remains a serious concern. (U)

More relevant to the Homeland, we are watching for signs that Iran could pursue additional operations here, though we assess they would be unlikely to do so given the consequences amidst the current conflict. Iran and its proxies do have a history of

external operations; Iranian state agents have pursued several dozen lethal plots and assassinated at least 20 opponents across four continents since 1979, while Lebanese Hizballah has conducted international terrorist attacks in Argentina, Saudi Arabia, and Bulgaria. Over the last several years, Iran has plotted against the United States, other Western interests, and Iranian dissidents more aggressively than they have at any time since the 1980s and become increasingly explicit in threats to carry out retaliatory attacks for the death of Iranian officials, especially against current and former U.S. officials whom it holds primarily responsible for Soleimani's death. (U)

As of mid-October, Iran is allowing its partners and proxies in the region to conduct attacks amidst the Israel-HAMAS conflict. For the United States, this has included Shia militant rocket and unmanned aircraft system (UAS) attacks against U.S. facilities in Syria and Iraq, leveraging a longstanding capability. Both Iran and Lebanese Hizballah are conducting or permitting dangerous actions that demonstrate their increased risk tolerance within the current crisis. So far, they appear to be avoiding dramatic actions that would immediately escalate the contours of the current conflict or open up a concerted second front with Israel. However, in the present regional context, their actions and those of their proxies carry great potential for miscalculation. (U)

### ***The Enduring Challenge of Violence by Lone Actors*** **(U)**

Violent extremists who are not members of terrorist groups will probably remain the most likely to carry out a successful attack in the United States over the next several years. The recent resurgence of such attacks in Europe, and the context of the ongoing HAMAS-Israel conflict reinforces our assessment. By their lack of affiliation, lone actors are difficult to detect and disrupt. While these violent extremists tend to leverage simple attack methods, they can have devastating and outsized consequences, as we have experienced in the Homeland with attacks in San Bernadino, CA; Orlando, FL; El Paso, TX; and in Buffalo, NY, to name a few. (U)

Since 2010, violent extremists influenced by or in contact with ISIS, al-Qa`ida, and other foreign terrorist organizations have conducted 40 attacks in the United States that have killed nearly 100 and injured more than 500 people. In 2022, there were two such attacks in the United States, which is a decline of about 70 percent compared to the

seven attacks in 2015—the height of ISIS's territorial control in Iraq and Syria and English-language messaging efforts. This averages out to a decline of almost 7 percent year-on-year during this period. The last Foreign Terrorist Organization-inspired lethal attack was in August 2021. However, we are on high alert for whether the current conflict in the Middle East may prove to be a catalyst for individuals to mobilize for attacks. (U)

Similarly concerning is the threat posed by the interconnected, transnational RMVE movement, particularly the foreign dimensions of this threat and its reach into the Homeland. NCTC continues to work closely with the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and our international partners to address this particular global phenomenon. (U)

The transnational nature of the threat is apparent from past RMVE attackers and plotters abroad, particularly the Norwegian attacker in 2011 and the Australian attacker in New Zealand in 2019. These previous foreign RMVEs have been particularly influential for likeminded individuals globally, with at least six subsequent RMVE attackers worldwide claiming inspiration from the writings of the Norwegian attacker and at least four citing the Australian attacker, including his use of social media to livestream his violence. Similarly instructive is the range of attacks by or disruptions of RMVEs globally in 2022, including in Slovakia, Brazil, the United States, the United Kingdom, France, and Germany. These attackers are part of an international ecosystem of individuals who share violent extremist messaging, mutual grievances, manifestos of successful attackers, and encouragement for lone actor RMVE violence. The transnational RMVE movement is largely fluid, fragmented, and lacking hierarchical structures. It is driven by individuals and networks that share racially and ethnically-based perceived grievances and messaging to incite violence, frequently framing actions around the concept of leaderless resistance. (U)

### ***International Terrorism Landscape Impacts Homeland*** **(U)**

Attacks abroad inspire more than just lone attackers and RMVEs in the Homeland, and we remain concerned about keeping our borders secure should individuals with links to transnational terrorist actors such as ISIS, al-Qa'ida, or Iranian state agents attempt to

enter the United States. Our efforts during the last two decades to build and enhance the screening and vetting system that guards against potential terrorist travel to the United States stands as one of our most valuable CT tools. Improving and sustaining our ability to identify, prevent, and disrupt such movement—whether by land, sea, or air—remains a critical priority in an era of increased global travel and migration. (U)

NCTC's support to the U.S. Government's screening and vetting enterprise plays a critical role in refugee and immigration processing by identifying any connections to international terrorism. We review about 30 million new travel and immigration applications annually—in addition to over 120 million continuous reviews—to enable DHS and the Department of State to prevent terrorist travel to the United States. (U)

We also work closely with our Intelligence Community colleagues to uncover, assess, and support actions to disrupt intersections between international terrorist and travel facilitation networks that could become potential threat vulnerabilities. While we have no credible or corroborated information to suggest that terrorist groups are currently trying to use such travel for operations, we know that terrorist actors have in the past considered or attempted different travel routes which reinforces our work to safeguard the United States. (U)

**Preserving NCTC's Critical Mission and Flexibility Within an Evolving National Security Environment (U)**

Over the past 20+ years, the U.S. Government has developed a highly integrated, innovative, and effective CT enterprise that continues to adapt to the changing threat. CT practitioners work behind the scenes every day to ensure that interconnected CT operations and programs are effectively used against the highest priority threats, employing a wide range of tools to do so, including identity intelligence, diplomatic security, sanctions, law enforcement investigations, direct-action operations, and partner capacity building efforts. (U)

As a critical part of that integrated community, NCTC fulfills its key missions, as directed by the Intelligence Reform and Terrorism Prevention Act of 2004. NCTC serves as the primary organization in the U.S. Government to analyze and integrate international

terrorism information; conduct strategic operational planning for counterterrorism activities and integrate all instruments of national power; ensure all agencies have access to and receive needed support to execute their counterterrorism plans; and serve as the central and shared knowledge bank on known and suspected international terrorists and international terrorist groups. (U)

NCTC sits at the intersection between foreign and domestic intelligence demands, and works to track threats across that divide in a way that is both effective against the threat and protects Americans' privacy and civil liberties. As an example of our critical intelligence fusion role, in 2007, NCTC established the Regional Representatives program to station analysts in the field charged with sharing timely and relevant intelligence, conducting training, providing finished intelligence products, and offering by-request support to the FBI, DHS, and their partners for CT operations. These Regional Representatives in select locations enable front-line support to DHS and FBI, as well as other federal, state, local, and private sector partners, and use the deep expertise, unique accesses, and connectivity of NCTC to serve as force multipliers against an array of international terrorist threats. (U)

NCTC is one part of the incredible confluence of capability housed in more than a dozen U.S. agencies that make up the CT enterprise. Our whole-of-government CT architecture must work across the spectrum of the threat landscape to quickly identify new threats and overcome enduring challenges that might allow space for terrorists to advance attacks. Our role in continuously evaluating and assessing the worldwide terrorist threat enables the CT community to focus its efforts on keeping the United States safe from the myriad terrorist threats we face. (U)

Vital to our CT efforts are intelligence collection tools, especially Section 702 of the Foreign Intelligence Surveillance Act, which provides key indications, warnings, and international terrorist disruptions to the entire CT enterprise, and has done so since its inception in 2008. We regularly leverage the essential authority of Section 702 to provide insight on foreign terrorists and their networks overseas. NCTC's Section 702 program focuses on reviewing communications by known and suspected terrorists, conducting international terrorist network development, and garnering insight into international terrorist operations. One of the most important questions for NCTC to determine is whether international terrorists could gain access to and pose a threat to

the Homeland. Section 702 is essential for our ability to do that, and without it, the United States and the world will be less safe. (U)

It is clear that the significant CT pressure brought to bear against terrorist groups over the last two decades, along with investment in effective CT defenses here at home, has resulted in a diminished threat to the United States Homeland. As evidenced by the events of the past month, however, our country must preserve CT fundamentals—such as collection, warning, analysis, disruption, information sharing, and key partnerships—to ensure constant vigilance. (U)

I would like to end with thanks to the professionals of the intelligence, diplomatic, military, and law enforcement communities, whose dedication to the CT mission has done so much to protect this country from persistent terrorist adversaries. It is a community the United States has relied upon time and again, and today is no exception. I am honored to be part of the CT enterprise and to work on behalf of the American people. (U)