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.