TESTIMONY OF

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

BEFORE

Committee on Homeland Security and Governmental Affairs
United States Senate

ON

"Threats to the Homeland: Evaluating the Landscape 20 Years After 9/11"

September 21, 2021
Washington, DC

Chairman Peters, Ranking Member Portman, and distinguished Members of the Committee,

Thank you for inviting me to join you today.

This month, we remember the 20th anniversary of the September 11th terrorist attacks that took thousands of American lives. Following that tragic day, Congress passed significant reforms to reorganize our government's national security agencies. The Department of Homeland Security (DHS) was created and charged with safeguarding the American people, our homeland, and our values.

Today, our country faces a threat landscape that has evolved significantly over the past 20 years. DHS confronts complex challenges, including international and domestic terrorism, a global pandemic, malicious cyber activity, transnational organized crime, and the catastrophic impacts of climate change, among others. Our Department is able to confront these challenges because of the extraordinary talent and dedication of the more than 250,000 individuals who comprise our workforce and serve our Nation.

Terrorism

In the years immediately following 9/11, we focused on foreign terrorists who sought to harm us within our borders and threaten our interests and assets abroad. In partnership with federal agencies spanning the law enforcement, counterterrorism, and intelligence communities, DHS built a multi-layered screening and vetting architecture to prevent certain individuals from traveling to or entering our country by air, land, or sea. We also issued a call for vigilance on the part of local communities and individuals alike.

The first major evolution of the terrorist threat emerged in the form of the homegrown violent extremist (HVE) – the individual in America who is radicalized by a foreign terrorist organization's ideology. HVEs became the most prominent terrorism-related threat to the homeland. In response, we partnered with law enforcement, first responders, social workers, mental health experts, and local communities to identify signs of radicalization and prevent violence before it occurred.

That threat has continued to evolve. Today, U.S.-based lone actors and small groups, including HVEs and domestic violent extremists (DVEs) who are inspired by a broad range of ideological motivations, pose the most significant and persistent terrorism-related threat to our country. DVEs are motivated by various factors, including racial bias, perceived government overreach, conspiracy theories promoting violence, and false narratives about unsubstantiated fraud in the 2020 presidential election. Among DVEs, racially or ethnically motivated violent extremists, including white supremacists (RMVE-WS), will likely remain the most lethal DVE movement in the Homeland. Since 2020, however, we have also seen a significant increase in anti-government and anti-authority violent extremism, particularly from militia violent extremists (MVEs), which typically target law enforcement, elected officials, and government personnel and facilities.

In June, the White House released the first-ever *National Strategy for Countering Domestic Terrorism* to improve federal response efforts. In executing this strategy, DHS will:

(1) focus on preventing terrorism and targeted violence, including through threat assessments, grants, and community-based prevention programs, as well as efforts to enhance public awareness;

(2) assess, evaluate, and mitigate the risk of violence inspired by violent extremist narratives, including those narratives shared via online platforms; and,

(3) establish partnerships with nongovernmental organizations (NGOs), including academia, and private sector entities, including technology and social media companies.

The National Strategy recognizes that online narratives espousing attacks on our fellow citizens, institutions, and critical infrastructure are a key factor in driving the radicalization and mobilization to violence by some recent lone offenders. DHS has shared analyses of this threat with our law enforcement partners at every level of government through formal information sharing channels, and with the American public through the National Terrorism Advisory System (NTAS). This year, I have issued three NTAS bulletins to contextualize the evolving threat landscape for the American people and provide information about how to stay safe.

Our Department is redoubling its efforts to provide timely and actionable intelligence and information to the broadest audience at the lowest classification level possible. As a result, DHS is augmenting its intelligence and information-sharing capabilities in collaboration with other government agencies; state, local, tribal, territorial, and campus law enforcement partners; and private sector partners. This includes publishing and disseminating intelligence bulletins that provide our partners with greater insight into evolving threats, and situational awareness notifications that inform public safety and security planning efforts to prevent terrorism and targeted violence.

We are also reviewing how we can better access and use publicly available information to inform our analysis. DHS's Office of Intelligence and Analysis (I&A) has enhanced its ability to analyze, produce, and disseminate products that address DVE threats, including violent extremist narratives shared via social media and other online platforms. This year, I&A also established a dedicated domestic terrorism branch that is leading our efforts to combat this threat.

Further, the newly formed DHS Center for Prevention Programs and Partnerships (CP3) is expanding our Department's ability to prevent terrorism and targeted violence through the development of local prevention frameworks. Through CP3, we are leveraging community-based partnerships and evidence-based tools to address early-risk factors and ensure individuals receive help before they radicalize to violence.

As it relates to our continued focus on combatting international terrorism, we are actively assessing the counterterrorism-related and other threats that could develop over the coming months and years, including those related to the fall of the Government of Afghanistan, and ensuring we have the resources and operational infrastructure required to protect the Homeland.

Al-Qa'ida, the Islamic State of Iraq and ash-Sham, and other terrorist groups continue operating worldwide, and the threat of these groups exploiting permissive environments to plan and launch attacks against the United States will continue posing challenges.

As I have said before, DHS is fundamentally a department of partnerships. Our ability to execute our mission depends on strong partnerships across every level of government, the private sector, and local communities. DHS works closely with Homeland Security Advisors in every state and territory to increase resiliency and preparedness across our communities. Additionally, through our partnership with the National Network of Fusion Centers, DHS deploys personnel to the field to share information on a broad range of threats, including counterterrorism, counterintelligence, and cybersecurity. DHS also partners with FBI-led Joint Terrorism Task Forces (JTTFs) to detect, disrupt and dismantle, and prosecute terrorists.

Further, this year, and for the first time, I designated combating domestic violent extremism as a "National Priority Area" for the Fiscal Year 2021 State Homeland Security Program (SHSP) and Urban Area Security Initiative (UASI) grant programs. Recipients of these grants will be required to spend at least 7.5 percent of their awards on combating DVE, meaning that states and local governments across our Nation will spend at least $77 million in grant funding on capabilities to detect and protect against these threats.

Economic Security

The United States continues to face counterintelligence and malign threats by nation-state adversaries intent on gaining military and economic dominance over our country. Of note, the People's Republic of China (PRC) represents a critical threat to U.S. economic competitiveness via its intellectual property theft, exploitation of vulnerable supply chains, engagement in illicit trade, and use of economic coercion. The PRC has mobilized vast resources to support its industrial development and defense goals and will continue exploiting U.S. academic institutions and our visa system to transfer valuable research and intellectual property that Beijing calculates will provide a military or economic advantage over the United States and other nations.

DHS is uniquely positioned to support federal government efforts to identify and counter these threats, from identifying instances of visa fraud to discovering and preventing the illicit transfer of user-collected data and/or proprietary research and technology. For example, DHS has targeted illicit PRC-based manufacturers who have exploited the COVID-19 pandemic by producing fraudulent or prohibited personal protective equipment (PPE) and medical supplies that especially endanger our front-line workers, prohibited the use of certain passenger and cargo screening equipment at airports from companies that pose a significant risk to the national security or foreign policy interests of the United States, leveraged technology to target and interdict deadly fentanyl and fentanyl-like substances originating in the PRC at our ports of entry, and prevented goods produced by forced labor from entering our markets. DHS also continues to work closely with the Department of State to prevent the exploitation of our academic system to further the PRC's military and economic goals.

Securing Cyberspace and Emerging Threats

Cyber threats from nation-states and state-sponsored and criminal actors remain one of the most prominent threats facing our Nation. We have recently seen numerous cybersecurity incidents impacting organizations of all sizes and disrupting critical services, from the SolarWinds supply chain compromise to the exploitation of vulnerabilities found in Microsoft Exchange Servers and Pulse Connect Secure devices, to ransomware affecting entities from Colonial Pipeline to JBS Foods to Kaseya. The assaults on these companies, not to mention interference in our elections, have reinforced the importance of cybersecurity and how we preserve and defend an open, interoperable, free, secure, and reliable Internet, and stable cyberspace.

Ransomware incidents continue to rise. Like most malicious cyber activities, ransomware exploits the weakest link. In 2020, nearly 2,400 state, local, tribal, and territorial governments, healthcare facilities, and schools across our country were victims of ransomware. That same year, victims paid an estimated $350 million in ransoms, a 311 percent increase over the prior year, with the average payment exceeding $300,000. The federal government and our private sector partners must be prepared to respond to and recover from a cyber incident, sustain critical functions even under degraded conditions, and, in some cases, quickly restart critical functionality after disruption.

This year, DHS has taken the following steps, among others, to increase our Nation's cybersecurity resilience:

- In February, I issued a call to action to tackle ransomware more effectively, including by increasing national adoption of the nine cybersecurity steps CISA recommends taking to protect against this threat. In July, together with the Department of Justice and other federal partners, DHS launched the first whole-of-government website that pools together federal resources to combat ransomware to help private and public organizations mitigate their related risk. This website, called StopRansomware.gov, is a one-stop hub to help individuals, businesses, and other organizations better protect their networks and know what to do if they become a victim of malicious cyber activities.

- As it relates to ongoing cybersecurity threats to our critical infrastructure, TSA issued two new security directives after soliciting industry feedback to strengthen the cybersecurity and resilience of our Nation's pipelines. The first security directive required owners and operators of critical pipelines to report confirmed and potential cybersecurity incidents to CISA, designate a cybersecurity coordinator to be available 24/7, review current practices, and identify any gaps and related remediation measures to address cyber-related risks and report the results to TSA and CISA within 30 days. The second security directive required implementation of specific mitigation measures to protect against ransomware attack, develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity review.

- In March, I announced a series of 60-day cybersecurity sprints to elevate existing work, remove roadblocks, and launch new initiatives. We are currently undertaking our fourth

sprint dedicated to the cybersecurity of transportation systems, building on lessons learned from the Colonial Pipeline ransomware attack and the TSA security directives to advance greater cybersecurity and resilience across transportation subsectors.

- In August, the Coast Guard released its new Cyber Strategic Outlook, the first update to this outlook since 2015. The strategy focuses on mitigating cyber risks to critical maritime systems essential to the nation's economy and security, defending the Coast Guard's networks, as well as leveraging the Coast Guard's capabilities to protect the maritime transportation system.

- Also in August, CISA announced the creation of the Joint Cyber Defense Collaborative (JCDC) to lead the development and execution of joint cyber defense planning with partners from all levels of government and the private sector to reduce risk before an incident and unify defensive actions when one occurs. This initiative underscores the whole-of-society approach needed to increase cybersecurity resilience.

- The U.S. Secret Service has continued expanding its cybercrime enforcement programs through the National Computer Forensics Institute (NCFI), the Nation's premiere federally funded training institute for state, local, tribal, and territorial law enforcement officers, prosecutors, and judges in cybercrime investigations. The NCFI provides hands-on training in ransomware response, digital evidence processing, and applicable law for high-tech criminal prosecution and adjudication.

- DHS also continues leveraging its authorities to deliver timely cyber threat-focused information to state, local, tribal, and territorial partners and the private sector at the lowest possible classification level. To scale these efforts, we are leveraging CISA, the U.S. Secret Service, and I&A to increase access to this information among our partners and stakeholders.

- Further, DHS increased the required minimum spend on cybersecurity via FEMA grant awards from 5 percent to 7.5 percent this year, representing an increase of $25 million. We are also optimizing existing grant programs to improve the cybersecurity capacity and capabilities of state, local, tribal, and territorial governments.

Election Security and Malign Foreign Influence

DHS continues working closely with state, local, tribal, and territorial partners to ensure their election systems are protected against interference. The Biden-Harris Administration has continually called out malign actors, such as the PRC, Russia, and Iran, that seek to interfere in our elections and threaten our democratic institutions.

Since 2016, Russia has continued to amplify mis- and disinformation about U.S. candidates for political office and the security of U.S. election systems, with the goal of sowing divisiveness and confusion, and weakening our democratic institutions. Iran continues to amplify narratives about perceived sociopolitical divisions to exacerbate domestic tensions. The PRC has consistently pushed conspiracy theories about the COVID-19 pandemic, including about its

origin. Russia, Iran, and PRC, as well as other malign influence actors, also continue to disseminate and amplify inaccurate information to international and U.S. audiences about topics such as racial justice, false claims about the 2020 presidential election, the efficacy of U.S. COVID-19 vaccines in comparison with Russian and Chinese vaccines, and our withdrawal from Afghanistan.

Further, Iran, the PRC, and other authoritarian regimes continue to target dissidents and human rights activists on U.S. soil. Known as "transnational repression," these governments are increasingly silencing exiles and members of diasporas – including activists, dissidents, defectors, journalists, and other critics – living outside their territorial borders. The Biden-Harris Administration is committed to addressing this challenge as part of our broader commitment to stem rising authoritarianism and prevent foreign influence and interference in our society.

Through CISA and I&A, DHS works with our federal partners, all 50 states, local jurisdictions, and election technology partners to ensure they have the resources they need to keep our elections secure and resilient. For example, CISA has provided more than 600 cybersecurity services to the election community, including cyber hygiene scans, risk and vulnerability assessments, phishing assessments, and other services. In the last year, CISA's informational products have reached over 3,500 election officials, offering scalable and customizable tools to improve infrastructure security and build awareness of CISA's resources and services. Further, CISA, through the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), has deployed intrusion detection devices to all 50 states and over 400 local jurisdictions and territories. All 50 states and over 3,000 local and territorial officials also receive threat alerts from the EI-ISAC.

Immigration and Border Security

The Biden-Harris Administration is committed to rebuilding a fair, orderly, and humane immigration system. DHS continues enforcing our immigration laws and responsibly managing our border, while restoring fairness and efficiency in our immigration system. We are safer when we take a more comprehensive and sustainable approach to border management and ensure that policies and procedures at our borders are consistent with our immigration laws and our values.

We currently face three linked and significant challenges along our southwest border. First, the surge of migrants, including unaccompanied children, encountered at and between ports of entry. Second, transnational criminal organizations (TCOs) seeking to profit from a range of illicit activity. Third, the ongoing impacts of COVID-19 on the DHS personnel responding to these challenges.

To address these challenges, DHS has leveraged FEMA's coordination capabilities, activated our volunteer workforce, and expanded processing capacity. We are also helping the Department of Health and Human Services increase its capacity to accept transfers and manage the care and custody of unaccompanied children efficiently and expeditiously, as required by the *Flores Settlement Agreement*, Homeland Security Act of 2002, and Trafficking Victims Protection Reauthorization Act of 2008. DHS also continues to enforce the Centers for Disease

Control and Prevention (CDC) Title 42 public health order. At the same time, the Department must continue to address increased levels of irregular migration, much of which has been exacerbated by TCOs activity. In consultation with the CDC, DHS has developed, implemented, and continuously evaluates a multi-layered approach for COVID-19 testing among noncitizens encountered along the southwest border where practical.

The Biden-Harris Administration is committed to stemming the flow of irregular migration and comprehensively addressing the long-standing challenges that drive this migration. Although there is no quick, easy, or single solution that will adequately address these challenges, we are taking the following steps:

- First, the most sustainable solution is to address the root causes that drive people to migrate in the first place. To this end, we are engaging with foreign governments and other partners to address the insecurity, violence, corruption, and systemic poverty that drive people from their homes.

- Second, we are working with foreign governments and international humanitarian organizations to provide potential migrants with meaningful opportunities to seek humanitarian protections as close to home as possible. These opportunities should include refugee resettlement and family reunification programs to the United States and other countries in the region, and regional relocation and integration programs. We must also expand seasonal and temporary employment-based non-immigrant visa programs to provide alternative pathways for those migrating primarily for economic reasons.

- Third, we are ensuring shared responsibility with other countries in the region by supporting their efforts to improve their asylum capacities.

- Fourth, we are seeking to dramatically improve our system for processing migrants at the border and adjudicating their asylum claims in a fair and timely way.

- Finally, we are marshaling our enforcement resources to deliver accountability in a fair and effective way.

While these efforts will dramatically improve migration management in the region and help restore safe and orderly processing at the border, they will take time. Addressing longstanding challenges cannot be accomplished overnight.

Transnational Criminal Organizations (TCOs)

TCOs and their smuggling operations present a clear and present threat to the homeland. These organizations – which profit from illicit activities that include fraud and large-scale theft, drug trafficking, wildlife and timber trafficking, extortion, sex trafficking, child exploitation, and human smuggling – are agile and adept at adjusting their operations. DHS continues making risk-based investments in our border security mission to combat TCOs and related threats.

For example, U.S. Immigration and Customs Enforcement (ICE) leverages its Border Enforcement Security Task Force to bring together officers from more than 100 different law enforcement agencies to combat TCOs. This Task Force employs a broad range of federal, state, local, tribal, and international law enforcement authorities and resources to identify, investigate, disrupt, and dismantle these organizations at every level. This model has closed the gap between international partners in multinational criminal investigations.

Further, in collaboration with federal and international partners, DHS announced Operational Sentinel, a counter-network targeting operation to hold accountable those with ties to TCO logistical operations. The Operation leverages law enforcement authorities to identify TCO targets and their foreign and domestic associates and assets, and it employs a series of targeted enforcement actions and sanctions against them. Such actions include, for example, denying access to travel through the revocation of travel documents, the suspension and debarment of trade entities, and the freezing of bank accounts and other financial assets tied to TCO logistical networks.

ICE also administers mobile, biometric data collection programs to disrupt and dismantle TCOs by strengthening international partners' law enforcement investigations, border security, and counterterrorism efforts. Further, ICE leads Transnational Criminal Investigative Units (TCIUs) in more than a dozen countries to facilitate rapid bilateral cooperation on investigations and prosecutions related to weapons trafficking and counter-proliferation, money laundering and bulk cash smuggling, human and narcotics trafficking, other customs-related fraud, child exploitation, and cybercrime.

Extreme Weather Events and Climate Change Resilience

DHS is committed to combatting the climate crisis and mitigating climate change-related risks, which impact our national and economic security. This year, we are once again facing an historic hurricane season while simultaneously fighting unprecedented wildfires. Hurricane Ida recently caused death and destruction from the Gulf Coast to the Northeast. At the same time, the Dixie and Caldor Fires, two of the largest wildfires in the history of the state, burned in California. So far, President Biden has declared major disasters in four states for Hurricane Ida and two major disasters in California for the fires, making much needed federal assistance available through FEMA and other federal agencies. FEMA is committed to working with affected states and communities to respond and rebuild in a resilient manner.

Sea-level rise, extreme weather events, drought, and other direct, indirect, and cumulative consequences of climate change will continue to threaten lives, essential functions, and infrastructure across the United States. Simply put, we are facing an existential climate crisis that poses a current and growing threat to our way of life. Under the Biden-Harris Administration, DHS is taking urgent action to address these increasing threats. The steps taken include the following:

- President Biden authorized $3.46 billion in Hazard Mitigation Grant Program funding, which states, tribes, and territories will utilize on mitigation projects to reduce the impacts of climate change.

- In April, DHS launched a Climate Change Action Group comprised of senior officials from across the Department to focus on promoting resilience and addressing multiple risks, including flooding, extreme heat, drought, and wildfires.

- DHS has leveraged the Building Resilient Infrastructure and Communities (BRIC) program – the funding for which President Biden doubled to $1 billion – to create incentives and funding to help our Nation address these threats. Our initial BRIC selections include wildfire resilience programs, flood control programs, small town coastal hazard mitigation plans, and more.

- We have upgraded our National Risk Index, which provides communities unprecedented clarity about the risks they face and thus helps equip them to act to reduce those risks.

- DHS has released new guidance on cost-effective methods for increasing local resilience.

- FEMA revised its policies governing individual assistance to overcome historic inequities adversely impacting minority, low-income, and other disenfranchised communities, to ensure a more equitable distribution of funds.

- FEMA also authorized the funding of mitigation measures through individual assistance to allow homeowners affected by disasters to repair their homes in a way that will protect against future damage.

Much more is on the way.

COVID-19 Response

On his first day in office, President Biden challenged FEMA to stand up 100 federally supported Community Vaccination Centers (CVCs) within 30 days. Before the end of February, FEMA was supporting over 400 CVCs. Today, there are almost 800 active sites, including almost 200 mobile sites still receiving federal support. President Biden also challenged DHS to deliver 100 million vaccinations nationwide in 100 days, a goal we surpassed. We are particularly focused on ensuring vaccine equity. To this end, FEMA worked with partners in 39 sites across the country to provide a supplemental allocation of vaccines above and beyond state, tribal, and territorial allocations and utilized mobile vaccination sites to increase access to COVID-19 vaccines among vulnerable and rural populations.

To protect the traveling public and transportation personnel, and pursuant to President Biden's Executive Order on Promoting COVID-19 Safety in Domestic and International Travel, TSA issued on February 2, 2021 a federal mask mandate at airports, on commercial aircraft, and in various modes of surface transportation, including passenger railroads and other public transportation. On September 9, 2021, TSA increased the range of civil penalties that can be imposed on individuals who violate this federal mask mandate,

to reinforce its importance to public health and safety.

Further, CISA developed voluntary guidance for the Essential Critical Infrastructure Workforce that has helped officials and organizations identify essential work functions during the COVID-19 pandemic.

ICE launched Operation Stolen Promise to protect American consumers and first responders by combatting COVID-19 related fraud and criminal activity. Through this operation, ICE and its partners have seized over $54 million in illicit proceeds, made 359 arrests, served 356 criminal search warrants, opened over 1,250 criminal investigations, and seized more than 2,200 mislabeled, fraudulent, unauthorized or prohibited COVID-19 vaccines, test kits, PPE, and other medical items. Further, the U.S. Secret Service – through its network of Cyber Fraud Task Forces and in partnership with law enforcement agencies across every level of government, state-employment agencies, and financial institutions – has prevented more than $3 billion of much-needed COVID-19 relief from fraudulently ending up in the pockets of criminals.

Conclusion

Twenty years after the tragic day of 9/11, the threats facing our country have significantly evolved and the global threat landscape is no less daunting. Those who wish to do us harm now have social media, encrypted apps, and other modern tools that enhance their ability to carry out attacks, sow discord, undermine our democracy and institutions, and erode our way of life.

At the same time, DHS continues to evolve to remain nimble enough to address the dynamism of not only the threat landscape confronting our Nation today, but also the threats, both seen and unseen, of tomorrow and of the next 20 years. We will do so with the commitment to protecting the security of both our homeland and our values. We will do so through the incredible dedication and talent of the public servants in the Department of Homeland Security.

Thank you and I look forward to answering your questions.