TESTIMONY OF

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

BEFORE

Committee on the Judiciary
United States Senate

ON

"Oversight of Department of Homeland Security"

March 28, 2023
Washington, DC

Introduction

Chair Durbin, Ranking Member Graham, and distinguished Members of this Committee:

Thank you for inviting me to join you today. This month marks the 20th anniversary of the Department of Homeland Security's (DHS or the Department) creation, which brought together many components of the federal government in a determined national effort to safeguard the United States against foreign terrorism in the wake of the devastation wrought on September 11, 2001. DHS remains the largest reorganization of the federal government's national security establishment since 1947, and a testament to the grave threat we faced as a nation from terrorism brought to our shores by foreign actors and foreign terrorist organizations (FTOs).

Thanks to extensive deliberation and collaboration across both sides of the aisle, Congress created a Department that significantly reduced the risk foreign terrorism poses to the homeland. We increased our capacity to prevent, prepare for, and respond to threats or acts of terrorism through greater collaboration across the national security enterprise, all levels of government, and the private sector.

Twenty years later, that vital mission remains, and the Department has evolved to meet new threats. Rapidly emerging technologies, evolving cyber capabilities of our adversaries, and increasing economic and political instability around the world combine to create a heightened threat environment at home. Collaboration with our partners and stakeholders remains central to our work to safeguard Americans.

We know that stopping foreign terrorism before it reaches our shores is not something we can do alone. We work increasingly with foreign governments to share information and vetting capabilities to ensure bad actors are denied entry to the homeland, whether it is at our borders or at their points of origin.

The threat of terrorism includes individuals who – fueled by violent extremist ideologies and personal grievances – seek to advance their political or social goals through violence. Countering this threat demands a collaborative, whole-of-society approach centered upon our communities. We work to build trust and partnerships across every level of government and with non-profit organizations, academia, the private sector, and the public to ensure communities, especially those that are vulnerable and underserved, have the resources and information they need to better prevent, prepare for, and respond to this threat.

Importantly, while combating all forms of violent extremism, DHS counterterrorism efforts must respect First Amendment freedoms, civil rights and liberties, and privacy protections. To that end, DHS policy prohibits profiling, targeting, or discriminating against any individual for exercising their First Amendment rights, and ensures all public-facing terrorism and targeted prevention resources and training materials respect Americans' privacy, civil rights, and civil liberties.

While these bedrock principles have not changed, our approaches and capabilities have. We are transforming the way we collaborate with the private sector and academia to stay ahead of the threats we face in cyberspace. After Russia's unprovoked and unjust invasion of Ukraine, we led the federal government's efforts to protect our homeland from adverse consequences. Our "Shields Up" initiative galvanized tens of thousands of businesses to implement urgent cybersecurity improvements. We continue to address cyber risks through the Cybersecurity and Infrastructure Security Agency (CISA)'s Joint Cyber Defense Collaborative (JCDC), which was recently expanded to include major energy and financial sector firms. Through the Cyber Safety Review Board (CSRB), experts from the public and private spheres analyze and disseminate best practices for responding to threats, and our Cybersecurity Performance Goals provide businesses and critical infrastructure owners a roadmap to protect themselves and the people they serve.

These initiatives are becoming best practices modeled around the world at a pivotal time. Hostile nations like the People's Republic of China (PRC) increasingly leverage sophisticated cyber capabilities to gain access to American intellectual property, data, and infrastructure and to carry out transnational repression through cyberspace. We have deepened and broadened our international cooperation in cybersecurity and combating cybercrime and are collaboratively working to harmonize requirements domestically and with international partners.

DHS is contending with conditions of violence, food insecurity, severe poverty, corruption, climate change, the COVID-19 pandemic, and dire economic circumstances that have contributed to a significant increase in irregular migration around the world. In our hemisphere alone, failing authoritarian regimes in Venezuela, Cuba, and Nicaragua, along with an ongoing humanitarian crisis in Haiti, have driven hundreds of thousands of people to migrate to the United States and other countries. These movements are often facilitated by numerous human-smuggling organizations that exploit migrants as part of a billion-dollar criminal enterprise. The depth of suffering that these migrants are willing to endure speaks to the desperation they feel about their prospects in their home countries.

Over the last several months, DHS has announced new processes for Cubans, Haitians, Nicaraguans, and Venezuelans and their immediate family members that combine an accessible, streamlined opportunity for eligible individuals to come to the United States via a lawful pathway, with consequences for those who do not avail themselves of this pathway and instead cross the Southwest border without authorization. Nationals of these countries who do not avail themselves of this process and attempt to enter the United States without authorization will generally be returned to Mexico.

There is universal agreement that the U.S. immigration system is broken, and we stand ready to work with Congress on solutions. In the meantime, DHS is responding with the legal tools available at its disposal, including surging resources and increasing efficiency, prioritizing smart border security solutions, making historic investments in technology, taking the fight to cartels and smugglers, doing more with our regional partners than ever before, and implementing innovative processes that couple legal pathways with consequences for those who do not avail themselves of those pathways.

We are also facing a new frontier of crimes of exploitation, as human trafficking and child sexual exploitation and abuse have grown rapidly in recent years. These crimes represent a direct attack on our values and personal and public safety, and threaten our physical and virtual borders, our immigration and customs systems, our prosperity, and our national security. The Department is accordingly redoubling its efforts to combat these abhorrent crimes, including by deploying cutting-edge forensic tools to locate and rescue victims and to identify and apprehend perpetrators.

Innovation and emerging technology are critical to combating human and narcotics smuggling. We are screening people, cargo, and vehicles at our ports of entry (POEs) more efficiently and effectively. Last year, we launched an unprecedented campaign with partners across the federal government and throughout the region that led to the arrest of more than 9,100 smugglers and the disruption of more than 9,000 human smuggling operations. In FY 2022, we seized nearly two million pounds of narcotics thanks to new technologies and partnerships with federal, state, tribal and local law enforcement agencies.

Emerging technology can directly impact public safety here in the homeland. Unmanned Aircraft Systems (UAS), commonly referred to as drones, can be used to conduct kinetic attacks and are increasingly violating FAA-established temporary flight restrictions that protect high-ranking officials, disrupting airport operations, surveilling outdoor mass gatherings, and conveying illegal narcotics across borders. It is vital that Congress act this year to extend and expand the Department's counter-UAS (C-UAS) authorities to protect against malicious drone activity.

Today, the non-partisan spirit of collaboration present at the Department's founding twenty years ago still drives and informs every aspect of our approach against the heightened threat environment. The threats of today demand a more coordinated response among our federal, state, and local governments, the private sector, first responders, nonprofits, academia, and – most importantly – our citizens. Our mission has never been more vital, our components have never collaborated more closely, and our nation has never been more prepared – but more can be done. The Department is eager to work with Congress to ensure the agency's mission is met and the homeland remains protected.

Combating Terrorism and Targeted Violence

Foreign Terrorist Threats

Since this Department's inception, the threat landscape has evolved dramatically, and DHS has remained agile and vigilant to address all terrorism-related threats to the homeland. In the years immediately following the September 11, 2001 terrorist attacks, the Department focused on foreign terrorists located overseas who sought to harm us within our borders and threaten our interests abroad. This focus evolved to include homegrown violent extremists (HVEs) —individuals in the United States whose ideologically motivated terrorist activities are primarily inspired by FTOs' political or social objectives.

Our assessments indicate that FTOs will maintain a highly visible presence online and prioritize messaging focused on inspiring HVEs to conduct attacks in the United States. Media branches of designated foreign terrorist organizations, including the Islamic State of Iraq and ash-Sham and al-Qa'ida, continue to target U.S. and Western-based audiences with their media releases. These releases address a variety of topics, including operational and communication security guidance, such as warning their supporters about the risks of engaging with associates online, as well as encouraging the use of violence by their supporters. ISIS and its supporters continue to call for attacks in the United States, and supporters often share tactics and techniques for reducing the likelihood of being detected online by law enforcement. Additionally, ISIS-Khorasan (ISIS-K) continues to hone its external operations capability and continues to represent a threat that requires close coordination and cooperation with our international allies to address.

We continue to see Iran, a state sponsor of terrorism, and its partner, Lebanese Hezbollah, pose an enduring threat to the homeland, evidenced by Iran's public statements threatening retaliation in the United States for Islamic Revolutionary Guard Corps Quds Force (IRGC-QF) Commander Qasem Soleimani's death and arrests of IRGC and Hezbollah members plotting operations in the United States. In the past several years, U.S. law enforcement has arrested numerous individuals for spying on Iranian dissidents in the United States and for acting as agents of influence for the Iranian Government. In August 2022, federal prosecutors unsealed charges against an IRGC member for plotting to assassinate a former U.S. official. In January 2023, prosecutors announced charges and a new arrest in connection with an assassination plot directed from Iran. Members of an Eastern European organized crime group are alleged to have plotted to murder a U.S. citizen of Iranian origin in New York City who has publicly opposed Iran's government. Given its capabilities, Iran could advance an attack plot targeted at the United States with little to no warning. DHS continues to work closely with other law enforcement agencies and the Intelligence Community (IC) to stay aware of ongoing threat streams and take preventative actions, as appropriate.

DHS works closely with our law enforcement, national security, and IC partners to continuously 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. In Fiscal Year (FY) 2022, the National Vetting Center (NVC), managed by DHS, expanded support to DHS and the Department of State (DOS) to support vetting for refugee applicants and all non-immigrant visa applicants worldwide. Through technology advancements, the NVC has increased efficiencies in vetting processes, improving our ability to identify potential threats.

We continue to build partnerships with foreign governments that increase our information sharing and vetting capabilities. DHS is constantly striving to increase our ability to engage in biometric comparison with our foreign partners, and most recently I added a new requirement to the Visa Waiver Program (VWP) to require participating countries to enter into an Enhanced Border Security Partnership (EBSP). Under EBSP, DHS will be able to conduct biometric checks against VWP member countries' biometric data to authenticate the identity of individuals seeking to travel under the VWP, and to receive information with regard to whether their citizens and nationals traveling to the United States represent a threat to the security and welfare of the United States and its citizens.

As a key part of the interagency approach to countering these threats, DHS provides timely and accurate intelligence to the broadest audience at the lowest classification level possible. DHS will continue to leverage our deployed intelligence professionals to ensure the timely sharing of information and intelligence with our state, local, tribal, territorial, and campus (SLTTC) partners, including the National Network of Fusion Centers, in accordance with applicable law and privacy, civil rights, civil liberties, and intelligence oversight policies.

Violent Extremism and Targeted Violence

The evolving threat to the homeland also includes those fueled by a wide range of violent extremist ideologies and grievances. DHS, along with the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center (NCTC), assess that the primary terrorist threat to the homeland stems from lone offenders or small groups motivated by a range of violent extremist ideologies. These can include individuals inspired by, but not acting directly on behalf of or in concert with, FTOs and individuals motivated by domestic grievances and ideologies, or "domestic violent extremists (DVEs)." DVEs are individuals operating primarily in the United States who seek to further political or social goals wholly or in part through unlawful acts of force or violence without direction or inspiration from an FTO or foreign power. These actors are motivated by various factors, including biases against racial and religious minorities, perceived government overreach, conspiracy theories promoting violence, and false or misleading narratives often spread online.

Amongst DVEs, the IC assesses that racially or ethnically motivated violent extremists (RMVEs) who advocate for the superiority of the white race and militia violent extremists (MVEs), a component of the anti-government or anti-authority violent extremism threat category, present the most lethal DVE threats to the homeland. In many cases, prior to their planned attacks, threat actors have spent inordinate amounts of time online viewing violent material and engaging with like-minded individuals. RMVEs often have the most persistent and concerning transnational connections because adherents to this ideology are present throughout the West. They frequently communicate with each other and, at times, have inspired attacks. Such connectivity with overseas violent extremists might lead to a greater risk of U.S.-based RMVEs mobilizing to violence. In June 2022, DHS, the FBI, and NCTC jointly assessed that the threat from DVEs fueled by various evolving ideological and sociopolitical grievances will continue to pose a sustained threat of violence to the American public, democratic institutions, and government and law enforcement officials. Events in the coming months, including continued perceptions of government overreach, immigration-related developments, or potential new legislation and court rulings, all present potential flashpoints that could inspire threat actors to commit violence.[1]

To prepare for this threat, the Department has embraced a community-based approach to preventing terrorism and targeted violence by building trust, partnerships, and collaboration across every level of government, the private sector, non-governmental organizations, and the communities we serve, while respecting First Amendment protections. We must make it harder to carry out an attack and reduce the potential for loss of life; one important way we do that is by helping to prevent mobilization to violence.

[1] DHS, NCTC, FBI, June 17, 2022 *(U) Wide-Ranging Domestic Violent Extremism Threat to Persist*.

DHS's Center for Prevention Programs and Partnerships (CP3) is at the forefront of the federal government's prevention efforts. Established in 2021, CP3 provides technical, financial, and educational assistance to help communities build or enhance local prevention capabilities. In addition to supporting state-level prevention strategies, CP3 supports local efforts to establish community support systems—bringing together mental health providers, educators, faith leaders, public health officials, social service providers, nonprofit organizations, law enforcement and public safety officials, and others—to create programs that connect individuals with the help they need. CP3 relies on the expertise of the professionals in DHS's Privacy Office and Office of Civil Rights and Civil Liberties to ensure all public-facing prevention resources and training materials respect Americans' privacy, civil rights, and civil liberties.

As part of this effort, DHS has invested more than $50 million over the past three 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 CP3 and the Federal Emergency Management Agency (FEMA), this program provides funding for state, local, tribal and territorial (SLTT) governments, nonprofits, and institutions of higher education to establish or enhance capabilities to prevent targeted violence and terrorism. Last September, DHS announced 43 TVTP grant awards to entities in 20 states, totaling $20 million, for FY 2022. These awards fulfill the grant program's focus on prioritizing the prevention of domestic violent extremist acts as well as efforts to counter mobilization to violence that occurs online, while respecting individuals' privacy, civil rights, and civil liberties.

DHS also provides security funding to support facility hardening and other operational and physical security enhancements for nonprofit organizations at risk of terrorist attacks through the Nonprofit Security Grant Program (NSGP). I am grateful that Congress supported this critically important program by providing $305 million in the FY 2023 Consolidated Omnibus Appropriations Act, an increase of $55 million from FY 2022 levels. The President's FY 2024 Budget proposes a further increase to $360 million. These funds are in addition to the resources provided by DHS to our state and local partners through the Homeland Security Grant Program (HSGP), in which DHS designated Combating Domestic Violent Extremism as a "National Priority Area" for both FY 2021 and FY 2022. As a result of this designation, between FY 2021 and FY 2022, states and local governments across our nation spent over $111 million in grant funding on capabilities to detect and protect against these threats.

CP3 is by no means the only part of the Department engaged in prevention work. Through the Presidential Threat Protection Act of 2000, Congress formally authorized the U.S. Secret Service (USSS) to establish the National Threat Assessment Center (NTAC) to conduct research, training, and consultation on threat assessment and the prevention of targeted violence. NTAC leads the field of targeted violence prevention by producing world-class research examining all forms of targeted violence, including domestic terrorism, mass casualty attacks, and attacks against K-12 schools.

NTAC's experts provide training and guidance for professionals from a wide range of agencies and institutions on establishing threat assessment frameworks and targeted violence prevention programs unique to their organization's missions and needs. In FY 2022, NTAC

delivered over 280 trainings and briefings to over 28,000 participants, including state and local law enforcement, government officials, educators, mental health professionals, faith-based leaders, and workplace security managers. The number of events and participants reached by NTAC in FY 2022 represent the highest totals in the Center's history.

On January 25, 2023, NTAC released its most comprehensive analysis of mass attacks to date, titled, *Mass Attacks in Public Spaces: 2016 – 2020*. This study analyzes 173 attacks perpetrated from 2016 through 2020 in public and semi-public locations in the United States, including businesses, restaurants, retail outlets, schools, houses of worship, open spaces, and other public locations. On the day of the release, NTAC hosted a virtual training event to highlight the report's findings. Over 21,000 public safety officials from across community sectors registered for the event, representing all 50 states and over 80 foreign countries.

The Department continues to see threats to federal employees and the targeting of federal facilities. The Federal Protective Service (FPS), a law enforcement agency within the Department, leads our efforts to provide integrated law enforcement and security services to protect more than 9,000 federal facilities across the Nation, and safeguards the more than 1.4 million federal employees and visitors to these facilities. FPS works closely with federal, state, and local law enforcement across the country to investigate these threats and respond to incidents at federal facilities.

Cyber Threats

Our interconnectedness and the technology that enables it—the cyber ecosystem—expose us to a dynamic and evolving threat environment, one that is not contained by borders or limited to centralized actors, and one that impacts governments, the private sector, civil society, and every individual. As a result, cyber threats from foreign governments and transnational criminals remain among the most prominent threats facing our nation. Hostile nations like Russia, China, Iran, and North Korea, as well as cybercriminals around the world, continually grow more sophisticated and create more adverse consequences.

Within the past three years, we have seen numerous cybersecurity incidents impacting organizations of all sizes and disrupting critical services, from the SolarWinds supply chain compromise to the widespread exploitation of vulnerabilities found in Microsoft Exchange Servers. Further, ransomware incidents—like those affecting JBS Foods, Kaseya, a major pipeline company and the CommonSpirit hospital system—continue to increase. As of February 2022, CISA, the FBI, and the National Security Agency observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, and victims paid an estimated $1.199 billion in ransoms in 2021, compared to $416 million in 2020. We continue to believe there is significant under-reporting of ransomware incidents.

Russia will likely remain a significant threat to U.S. networks, data, and critical infrastructure as it refines and employs sophisticated cyber espionage, influence, and attack capabilities, particularly in response to international pressure following its invasion of Ukraine. Russia has previously targeted critical infrastructure in the United States and allied countries to hone—and in some cases demonstrate— its ability to inflict damage during a crisis. In February

2022, just prior to their full-scale invasion, Russia conducted a cyberattack against commercial satellite communications, impacting families and businesses across Europe. Cyber operations, including attacks by pro-Russian cyber hackers, have been prolific throughout Russia's illegal war against Ukraine.

The PRC operates a multifaceted intelligence program globally, with perhaps the most prolific element of that being a highly advanced cyber program. They continue to leverage increasingly sophisticated, large-scale cyber espionage operations against a range of industries, organizations, and dissidents in the United States. The PRC uses cyber means to illicitly obtain U.S. intellectual property, personally identifiable information, and export-controlled information. The PRC launches cyber espionage operations against the United States via People's Liberation Army and Ministry of State Security cyber actors. PRC-backed hackers are among the most active groups targeting governments and critical infrastructure this year – including across Southeast Asia. They are the most active group targeting businesses around the globe. Just one PRC hacking group known as APT41 has stolen intellectual property from at least 30 multinational companies in the pharmaceutical, energy, and manufacturing sectors, resulting in hundreds of billions of dollars of lost revenue.

Iran has a robust cyber program that targets networks in nearly every sector, and conducts offensive cyber operations in the United States, Israel, Saudi Arabia, and via other regional adversaries. In July 2022, Iranian cyberattacks caused severe harm to government networks in Albania, limiting access to essential services. These attacks include disruptive and destructive cyber-attacks such as website defacements and data deletion. Iranian cyber espionage is a high frequency, widespread threat, and Iran may choose to leverage its cyber access for disruptive or destructive attacks. DHS is expanding the Abraham Accords into cybersecurity to improve our collective cyber resilience against common threats with our Middle Eastern partners. We are committed to focusing our work with Israel, the United Arab Emirates, Bahrain, and Morocco on network defense and cybersecurity collaboration to protect our critical infrastructure, including from shared threats from Iran and other nation states' targeting of critical infrastructure and widespread ransomware attacks.

In the last five years alone, North Korea has largely funded its weapons of mass destruction programs through cyber heists of cryptocurrencies totaling more than $1.2 billion.

We assess that ransomware attacks targeting U.S. networks will increase in the near and long term because cybercriminals have developed effective business models to increase their financial gain, likelihood of success, and anonymity. In recent years, ransomware incidents have become increasingly prevalent among U.S. SLTT government entities and critical infrastructure organizations, with ransom demands in 2020 exceeding $1.4 billion in the United States. The healthcare and public health sector remain popular targets for ransomware threat actors.

The Department is committed to keeping Americans safe from the devastating effects of cybercrimes. Cyber criminals' primary motivation is financial gain, and criminals show little regard for whom they target. Cybercrime investigators at the USSS and U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) are dedicated to seizing and returning stolen funds to the victims and arresting those responsible. Cybercrimes are often

transnational, with the criminal actors, their infrastructure, and their victims spread across the globe. The USSS was recognized by the Attorney General for its contributions to the recent dismantling of the Hive ransomware infrastructure used to communicate with other criminals, and disrupting the group's ability to attack victims. USSS and HSI continue to partner with federal and SLTT law enforcement and with international and foreign law enforcement in combating cybercrimes.

The Department plays an important role in helping to protect our nation's critical infrastructure from these attacks. The private sector, which owns and operates most of the nation's critical infrastructure, plays a vital role in working with CISA and Sector Risk Management Agencies (SRMAs) to ensure that we are aware of new campaigns and intrusions. That awareness in turn helps CISA advise other potential victims—increasing the nation's collective cyber defenses through our collaborative efforts.

In March 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) into law. CIRCIA marks an important milestone in improving America's cybersecurity. The increased number of incident reports that will be received from our private sector partners as a result of this new law will enable CISA, in partnership with other federal agencies such as the FBI, to build a common understanding of how our adversaries are targeting U.S. networks and critical infrastructure. This information will fill critical information gaps and allow us to rapidly deploy resources and render assistance to victims suffering cyberattacks, where appropriate, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims. We are grateful to Congress for passing this historic bipartisan legislation, marking a critical step forward in the collective cybersecurity of our nation.

Cyber Threat Mitigation and Resilience

To respond to evolving cyber threats and increase our nation's cybersecurity and resilience, DHS has taken several steps, including:

- In July 2021, with the Department of Justice (DOJ) and other federal partners, DHS launched StopRansomware.gov—the first whole-of-government website that pools federal resources to combat ransomware and helps private and public organizations of all sizes mitigate cyber risk and increase their resilience.
- In August 2021, CISA announced the creation of the Joint Cyber Defense Collaborative (JCDC) to develop and execute joint cyber defense planning 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.
- In February 2022, DHS launched the Cyber Safety Review Board (CSRB), a groundbreaking public-private partnership dedicated to after-action review of significant cyber threats. The CSRB published its first report last summer addressing the risk posed by vulnerabilities in the widely used "Log4j" open-source software library. Its second review of the recent attacks associated with Lapsus$, a global extortion-focused hacker group, is underway. We are asking Congress to strengthen the ability of DHS to carry

out comprehensive reviews of significant cyber incidents in ways that will allow us to learn from past experience and strengthen our response to future threats.

- In February 2022, recognizing the heightened risk of malicious cyber activity related to Russia's war against Ukraine, CISA launched a new campaign called "Shields Up" to amplify free cybersecurity resources and guidance for how organizations of every size and across every sector can increase their cybersecurity preparedness.
- In accordance with CIRCIA, DHS established the Cyber Incident Reporting Council (CIRC) this past summer. The CIRC, which includes many of our federal agency partners, is working to coordinate, deconflict, and harmonize federal cyber incident reporting requirements, including those issued through regulation. To facilitate this effort, DHS has been working to inventory all federal cyber incident reporting requirements.
- In September 2022, CISA and the FBI launched the Joint Ransomware Task Force (JRTF) to coordinate a whole-of-government effort to combat the threat of ransomware. One major objective of the JRTF is to coordinate efforts between federal agencies and private sector and SLTT partners to improve our nation's response to a ransomware incident, including efforts to increase our nation's cyber resiliency.
- In September 2022, the Department announced the State and Local Cybersecurity Grant Program (SLCGP) to help states, local governments, rural areas, and territories address cybersecurity risks and cybersecurity threats to information systems. In FY 2022, $183.5 million was made available under the SLCGP, with varying funding amounts allocated over four years from the Infrastructure Investment and Jobs Act.
- In October 2022, the Department released the Cybersecurity Performance Goals (CPGs), voluntary practices that outline the highest-priority baseline measures businesses and critical infrastructure owners of all sizes can take to protect themselves against cyber threats. By clearly outlining measurable goals based on easily understandable criteria such as cost, complexity, and impact, the CPGs are designed to be applicable to organizations of all sizes.
- The disruptive ransomware attack on a major pipeline company on May 7, 2021 revealed a continuing significant national security risk with critical vulnerabilities in the transportation sector that previous voluntary efforts did not sufficiently mitigate. Since the attack in 2021, the Transportation Security Administration (TSA) has issued security directives mandating that surface transportation owners and operators implement several critically important and urgently needed cybersecurity measures, such as designating a cybersecurity coordinator, reporting cybersecurity incidents, implementing a cybersecurity response plan, completing a cybersecurity vulnerability assessment, identifying cybersecurity gaps, and requiring certain measures such as network segmentation, access control, continuous monitoring and detection, and security updates and patching. As a result of feedback received by industry and stakeholders, TSA updated these directives to focus requirements on achieving security outcomes, rather than relying on prescriptive measures. On March 7, 2023, TSA issued an Emergency Amendment to certain TSA-regulated aircraft operators and airports, following the similar outcome-focused measures outlined above that TSA issues for surface transportation owners and operations. TSA took this emergency action because of persistent cybersecurity threats against the aviation sector. . DHS continues to consider what additional directive action might be necessary to address urgent cyber threats to

transportation and other critical infrastructure sectors and will continue to work closely with the Department of Transportation, the Department of Energy, and other SRMAs.

Emerging Technology Threats

Unmanned Aircraft System (UAS) Threats

UASs, or drones, offer tremendous benefits to our economy and society, but their misuse poses real security challenges. The rapid proliferation of drones and their expanded use by hobbyists, professionals, and threat actors have required DHS to shift its response efforts to mitigate smaller, more agile, and less attributable dangers across all its mission areas while still supporting the lawful use of these advanced technologies within our nation. Drones have conducted kinetic attacks with payloads of explosives or firearms, caused dangerous interference with manned aviation, disrupted airport operations (causing significant economic harm), and disrupted and damaged critical infrastructure. Nearly every day, transnational criminal organizations (TCOs) use drones to convey illicit narcotics, including fentanyl, and other contraband across our borders. TCOs also use drones to conduct hostile surveillance of law enforcement and guide human smuggling across the border.

I thank Congress for extending existing law that provides DHS's counter-UAS (C-UAS) authority through September 30, 2023. Ensuring that the existing authorities did not lapse was vital to our mission, including protecting the President and Vice President, patrolling the Southwest border where drones are being used to traffic fentanyl and other dangerous contraband, securing certain federal facilities and assets, and safeguarding the public. DHS has exercised its current C-UAS authority by successfully executing C-UAS 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, and the 2023 Super Bowl. 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.

To ensure that the Department can continue its C-UAS activities, both the Department and the Administration remain committed to a multi-year extension as well as an expansion of existing authorities. Any lapse in DHS's current C-UAS authority would entail serious risks for homeland security as DHS would have to cease or curtail existing C-UAS operations that protect the homeland. Additionally, 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 a lack of protection for U.S. airports from drone threats and the inability of DHS to partner on C-UAS activities with SLTT enforcement officials or critical infrastructure owners or operators to detect, identify, and—on a pilot basis under appropriate federal oversight, including privacy, civil rights, and civil liberties protections—mitigate drones posing a credible threat to their jurisdictions or at their facilities, respectively.

Congressional action is required, as DHS's authority to detect and counter drone threats will expire on September 30, 2023. A lapse in this authority and, failing to close known

vulnerabilities by expanding C-UAS authority, could have catastrophic implications for homeland security.

5G/6G

In the cyber ecosystem—which underpins the unprecedented interconnectedness we have achieved as a nation and across the globe—emerging technology and innovation can also expose us to a dynamic and evolving threat environment. For example, communications advancements in 5G and 6G technology continue to be a high security priority for the Department.

The PRC is using its technology to tilt the global playing field to its benefit, capitalizing on the worldwide demand for communications technology and luring customers with improved telecommunications networks at a low cost. However, Beijing often requires large PRC-based companies to share and store data from their networks in-country and to provide that data to the PRC government when requested by authorities. It is our belief that our essential telecommunications networks should not be owned or operated by companies that will either sell or provide information to a foreign government, and we are championing to international partners that cheap telecommunications technology is not worth the price of citizens' privacy, their national security, or their sovereignty.

For several years, DHS has worked closely with the interagency to secure 5G and to mitigate possible malicious use by PRC technology. At CISA, our 5G team provided supply chain risk analyses that significantly contributed to the federal government's response to this issue. However, today we are looking beyond 5G to the next frontier in 6G. The prevalent use of 6G is still approximately 8 to 10 years away, but the process to create the standards for 6G rollout is beginning today. This is a technology standardization process that has geopolitical implications, as Beijing is already positioning itself to dominate the standards process. We see this as a potential threat to our homeland and economic security and we are taking steps to educate our partners about the importance of this issue.

Cryptocurrency

While most cryptocurrency is used legitimately, cryptocurrency has attributes that have already been exploited by criminals, terrorists, and other adversaries to facilitate their operations. Most notably, as it has become easier to access and more widely used in general commerce, many transnational ransomware operations are using the cryptocurrency ecosystem to obfuscate illicit requests and to facilitate the receipt of ransoms.

Many components within DHS are focused on the rising illicit use of digital assets, developing and providing training, investigating, collaborating with interagency partners, and conducting research. Pursuant to the President's Executive Order 14067, *Ensuring Responsible Development of Digital Assets*, the Department contributed to the whole-of-government effort to address concerns with respect to digital assets.

For example, with domestic and international law enforcement partners, the USSS has achieved notable successes in combating cyber-enabled financial crimes, including dismantling

two centralized virtual currency providers that supported extensive criminal activity and the successful investigation of a Russia-based criminal scheme attempting to defraud cryptocurrency exchange customers of $16.8 million.

HSI has offices in over 50 countries and works to combat cybercrimes, including by providing training to international partners and analytical assistance in tracing digital assets. HSI investigations related to virtual assets have risen from one criminal investigation in 2011 to over 530 criminal investigations in FY 2022—seizing over $4 billion in virtual assets this last fiscal year. HSI has also trained law enforcement partners in more than 20 countries on dark web and cryptocurrency investigations, and regularly works with victims to remediate vulnerabilities before they are exploited.

Artificial Intelligence (AI)

AI encompasses several different technologies such as natural language processing, computer vision, generative AI, and more. It is imperative for DHS to take a proactive role in the use of AI systems and to contribute to the national conversation on the secure use of this transformative technology. Malicious actors are using increasingly advanced AI, powered by more data, increasingly accessible computing resources, and advancements in machine learning algorithms. Our own prudent and trustworthy use of AI can help us more effectively and efficiently accomplish our mission to secure the homeland. DHS has taken several steps, including:

- Responding to our statutory requirements from the 2023 National Defense Authorization Act (NDAA), DHS is working to create policies and procedures for AI acquisition and use and the consideration of risks and impacts associated with AI. This includes the full consideration of privacy, civil rights, and civil liberties impacts and misuse, degradation, and non-operability risks.
- We are taking a strategic approach to mitigate and counter adversarial AI efforts by tracking evolving adversary AI capabilities that could be used to exploit or overcome security measures at our physical borders, in cyberspace, in election systems, and beyond.
- We are working with other responsible partners—domestically and internationally—to share best practices and develop standards.

Quantum

The future development of quantum computers capable of breaking current cryptography presents a tremendous threat to the way we store and move sensitive government, critical infrastructure, financial, and personal data. DHS recognized this threat and established a productive partnership with the National Institute for Standards and Technology (NIST) within the Department of Commerce to produce actionable steps that our critical infrastructure and SLTTC partners can take to prepare themselves for the coming transition to new post-quantum cryptographic algorithms. DHS played a leading role in reflecting this work—and complementary efforts—in the whole-of-government and whole-of-society effort on quantum computing captured in the President's National Security Memorandum on quantum computing. DHS fully supports the requirements of the Quantum Cybersecurity Preparedness Act and is

actively engaging in outreach to industry and SLTTC partners to ensure a smooth and equitable transition to post-quantum algorithms.

Smart Cities and Connected Communities

The convergence of emerging technologies such as 5G, Internet of Things, AI, and cloud computing in our municipalities is creating exciting opportunities for efficient transportation, equitable delivery of government services, and energy efficiency in the form of "connected communities." At the same time, this issue presents a unique cybersecurity challenge for critical infrastructure, with the introduction of potentially tens of thousands of new Internet-connected devices. DHS has been working on this issue for over a year to ensure that our municipalities, large and small, can capitalize on this impressive technology in a safe and secure manner.

Border Security and Immigration

Over the last several months, DHS has announced and implemented new processes for Cubans, Haitians, Nicaraguans, and Venezuelans and their immediate family members that combine an accessible, streamlined opportunity for eligible individuals to come to the United States via a lawful pathway, with consequences for those who do not avail themselves of this lawful pathway and instead cross the Southwest border without authorization. Through a fully online process, individuals can seek advance authorization to travel to the United States and be considered, on a case-by-case basis, for a temporary grant of parole for up to two years, provided that they pass rigorous biometric and biographic national security and public safety screening and vetting; have a supporter in the United States who commits to providing financial and other support; and complete vaccinations and comply with other public health requirements. Nationals of these countries who do not avail themselves of this process and attempt to enter the United States without authorization will generally be returned to Mexico.

The coupling of these measures has led to a dramatic reduction in the numbers of Cubans, Nicaraguans, Haitians, and Venezuelans seeking to cross the Southwest border without authorization. Encounters of nationals from these four countries between POEs at the Southwest border declined from a seven-day average of 1,231 on the day this policy was announced on January 5, to a seven-day average of 46 on February 28—a drop of 96 percent. This reduction represents a decline of 99 percent in mid-February from the early December 2022 high of 3,546 daily encounters, and occurred even as encounters of other noncitizens began to rebound from their typical seasonal drop.

While encounters of Cubans, Haitians, Nicaraguans, and Venezuelans between POEs at the Southwest border have plummeted, thousands of nationals from these countries have successfully followed the process for lawful entry. As of March 1, more than 66,000 Cubans, Haitians, Nicaraguans, and Venezuelans have, after being thoroughly screened and vetted, received travel authorization. More than 45,000 individuals have lawfully arrived through commercial air travel at POEs to unite with supporters already in the United States, including more than 9,500 Cubans, more than 8,000 Haitians, more than 2,700 Nicaraguans, and more than 25,000 Venezuelans. The successful use of these parole processes and the significant decrease in illegal crossing attempts clearly demonstrates that noncitizens prefer to utilize a safe, lawful, and

orderly pathway to the United States if one is available, rather than putting their lives and livelihoods in the hands of ruthless smugglers. Combining accessible legal pathways with consequences for those who fail to use those pathways works.

Actions to Secure the Border

These measures build on our broader efforts to secure and manage our borders while building a safe, orderly, and humane immigration system. Last year, we announced six lines of effort within our current framework to continue building a sustainable immigration and border security program:

1. Surging resources, including personnel, transportation, medical support, and facilities to support border operations;
2. Increasing U.S. Customs and Border Protection's (CBP) processing efficiency and moving with deliberate speed to mitigate potential overcrowding at Border Patrol stations and alleviate the burden on the surrounding border communities;
3. Administering consequences for unlawful entry, including removal, detention, and prosecution;
4. Bolstering the capacity of non-governmental organizations (NGOs) to receive noncitizens after they have been processed by CBP and are awaiting the results of their immigration removal proceedings, and ensuring appropriate coordination with and support for state, local, and community leaders to help mitigate increased impacts to their communities;
5. Targeting and disrupting the TCOs and smugglers who take advantage of and profit from vulnerable migrants, and who seek to traffic drugs into our country; and
6. Deterring irregular migration south of our border, in partnership with the DOS, other federal agencies, and nations throughout the Western Hemisphere to ensure that we are sharing the responsibility throughout the region. This comprehensive plan leverages a whole-of-government approach to prepare for and manage increases in encounters of noncitizens at our Southwest border.

To meet the demands at the border, the FY 2024 President's Budget includes funding to increase personnel and enhance technological capabilities. I urge Congress to continue its support to properly resource the Department.

CBP has 24,000 agents and officers working along the Southwest border and the FY 2023 Consolidated Appropriations Act supported an additional 300 agents, as requested in the FY 2023 President's budget request. We have hired and contracted for over 1,000 Border Patrol Processing Coordinators to be able to continue to return agents to the field to perform their essential law enforcement mission. Through the Southwest Border Coordination Center, established in February 2022, we are coordinating a whole-of-government approach to prevent and respond humanely to increases in irregular migration by surging and coordinating our border security and law enforcement resources. Through the Emergency Food and Shelter Program administered by FEMA, we are also supporting local governments, NGOs, and faith-based organizations in border communities as well as interior cities who are responding to a surge in migration. FEMA is also working quickly to stand up the new Shelter and Services Program (as directed by the Bipartisan Year-End Omnibus bill on December 29, 2022), which will help to

relieve pressure on CBP's Border Patrol stations and provide humanitarian assistance. To avoid potential operational risks created by realigning funds from base budgets, as proposed in the FY 2024 Budget, CBP and ICE would use the Southwest Border Contingency Fund for emergent border management requirements associated with potential migrant surges. The fund will also allow FEMA to provide critical humanitarian resources and relief to local governments and non-profit organizations to help communities around the country better manage the costs of noncitizen arrivals in their communities.

We are prioritizing smart border security solutions, grounded in evidence rather than rhetoric, and making historic investments in technology. We are installing effective technology like linear ground detection systems and autonomous surveillance towers. We have also made historic investments in non-intrusive inspection technology at POEs to increase our interdiction of illicit drugs in all modes of transportation. We have made significant progress in digitizing stages of noncitizen processing across CBP, ICE, and U.S. Citizenship and Immigration Services (USCIS), to reduce the amount of time our agents and officers spend doing paperwork so that they can get back to the field. These innovations have already saved 70,000 hours of agent time. We are increasing processing efficiency, supporting decompression efforts, and strengthening overall process integrity and security.

Disrupting human smuggling is a top priority for our Department, and we have invested significant time and resources in the effort to disrupt and dismantle the TCOs that support human smuggling. Last year, we launched an unprecedented campaign with partners across the federal government and throughout the region that led to the arrest of more than 8,800 smugglers and the disruption of nearly 9,000 smuggling operations. This work includes raiding stash houses, impounding tractor-trailers that are used to smuggle migrants, and confiscating smugglers' communications technology. On the Southeast border and its maritime approaches, Homeland Security Task Force Southeast, a DHS-led task force supported by federal, state, and local law enforcement agencies, has surged air and surface assets and additional personnel to deter irregular maritime migration and reinforce safe and legal pathways to the United States.

We have also seized nearly two million pounds in narcotics, thanks to new technologies and partnerships with federal, state, and local law enforcement agencies. On October 16, 2022, I wrote to the United States Sentencing Commission urging that the guidelines for smuggling offenses be updated to address the seriousness of the offenses. According to the Sentencing Commission's own data, in FY 2021, the average sentence for smuggling human beings was just 15 months. These lower sentences impair prosecutors' ability to negotiate plea agreements and obtain the cooperation of co-conspirators; as a result, human-smuggling organizations survive and thrive, as key members are rarely severely penalized for their heinous crimes.

The United States cannot and should not do this work alone: hemispheric challenges require hemispheric solutions. We are strengthening our relationships with partners in Mexico and Central and South America to ensure a holistic response to this challenge, including the following actions:

- In October 2022, DHS announced joint actions with Mexico, reinforcing our coordinated enforcement operations to target human smuggling organizations and bring them to

justice. That campaign includes new migration checkpoints, additional resources and personnel, joint targeting of human smuggling organizations, and expanded information sharing related to transit nodes, hotels, stash houses, and staging locations.

- DHS officials have traveled throughout the region to strengthen partnerships with our counterparts. As Secretary, I have traveled to Mexico four times, including most recently with the President for the North American Leaders' Summit in January to discuss regional cooperation on migration, security, and other vital issues. I have visited Honduras, Guatemala, Panama, Ecuador, Colombia, and Costa Rica to advance our bilateral and regional partnerships and forge strengthened cooperation on migration management.
- We are also working with regional partners to implement the U.S. Strategy for Addressing the Root Causes of Migration and the hemispheric Los Angeles Declaration on Migration and Protection with historic U.S. Government investments, totaling nearly $1 billion in new assistance, according to the DOS. We have also concluded bilateral arrangements with Costa Rica and Panama, agreeing to humane border security measures and support with counter-smuggling as well as repatriation assistance. The United States is planning to offer additional assistance to support regional partners to address the migration challenges in the Darién Gap.

Actions to Enforce Our Immigration Laws

Under our immigration laws, individuals can request asylum and other humanitarian protection and, if they qualify, may be granted such protection. Individuals who are not eligible for protection or other lawful status generally are ordered removed. More individuals encountered at the border were removed or expelled in FY 2022 than in any previous year. In FY 2022, the United States expelled (under the Centers for Disease Control and Prevention's Title 42 public health Order) or removed (under Title 8 immigration authorities) over 1.4 million individuals. In September 2021, I issued guidance to focus ICE enforcement and removal on the greatest threats to the homeland, which yielded positive results. For example, while the guidance was in place and before it was vacated by a federal court, ICE arrested an average of 855 aggravated felons per month, compared to a monthly average of 687 during the four years of the prior Administration.

At the same time, we are implementing efficiencies in the asylum process while maintaining appropriate procedural safeguards and maintaining security. In May 2022, DHS began implementing a new rule that allows asylum officers, as opposed to only immigration judges, to consider in the first instance the asylum applications of noncitizens found to have a credible fear of persecution or torture. This rule aims to ensure that noncitizens who are eligible for asylum are granted relief quickly and provides DHS with the ability to promptly remove noncitizens who do not qualify for asylum or related protection. These reforms are especially important considering those seeking asylum under the current process often wait several years before receiving a decision. When the rule is fully implemented and resourced, the timeframe for hearing and deciding these asylum claims will shrink from several years to several months for most applicants. Already, initial cases placed through this process have concluded within a few months, demonstrating the potential of this new process.

As a complement to these efforts, and in response to the unprecedented surge in migration across the hemisphere and to reduce encounters at our border and in the maritime approaches to the U.S., DHS and DOJ issued a joint Notice of Proposed Rulemaking (NPRM) on February 21, 2023 to further incentivize the use of new and existing lawful processes and disincentivize dangerous border crossings between POEs by placing a new condition on asylum eligibility for those who fail to use the new lawful processes. Under the proposed rule, individuals who circumvent available, established pathways to lawful migration – including those new processes announced on January 5, 2023 as well as a newly available mechanism for migrants from any nationality to schedule a time and place to arrive at a POE – or fail to seek protection in a country through which they traveled on their way to the United States, would be subject to a rebuttable presumption of asylum ineligibility in the United States unless they meet specified exceptions. Individuals who cannot establish a valid claim to protection under the standards set out in the proposed rule will be subject to prompt expedited removal under Title 8 authorities, which carries a five-year bar to reentry. Consistent with America's history as a nation of laws and a nation of immigrants, this proposed rule ensures enforcement of U.S. immigration laws, lawful pathways, and access to asylum and other forms of humanitarian relief for those who need it. We have invited public comment on the proposed rule.

Actions to Build a Safe, Orderly, and Humane Immigration System

We are also building a safe, orderly, and humane immigration system. We are strengthening legal pathways and relief for noncitizens, including avenues to make protection claims where applicable, updating our enforcement policies, pursuing detention reforms, and ensuring just outcomes. When it comes to increasing legal pathways, we have, for example:

- Nearly doubled use of our H-2 temporary worker visa programs by nationals of the northern Central American countries of El Salvador, Guatemala, and Honduras to more than 19,000 in FY 2022 as compared to 9,796 in FY 2021. In doing this, we addressed acute needs that American businesses have for seasonal labor, while providing a significant avenue of lawful migration for those who sought work in the United States; it is notable that encounters of northern Central Americans fell by almost a quarter in this same period. In December 2022, DHS and the Department of Labor jointly published a rule authorizing an increase in the number of H-2B visas available by up to 64,716 for FY 2023, on top of the 66,000 H-2B visas that are normally available each fiscal year. Of these, an allocation of 20,000 visas are specifically reserved for workers from El Salvador, Guatemala, Haiti, and Honduras.
- Implemented a historic effort across the federal government to support vulnerable Afghans, including those who worked alongside us in Afghanistan for the past two decades, first through Operation Allies Welcome (OAW) and now continuing such support through Enduring Welcome. Over the past year and a half, DHS led and coordinated efforts to process nearly 89,000 Afghan allies and their families, including COVID-19 testing, isolation of COVID-positive individuals, vaccinations, additional medical services, and appropriate screening and vetting. Specifically, Afghan nationals paroled under OAW underwent an interagency screening and vetting process that began overseas and was supported by intelligence, law enforcement, and counterterrorism professionals from DHS, DOS, FBI, NCTC, and additional intelligence community

partners. Through Enduring Welcome, we continue to aid those who supported the U.S. Government and to facilitate family reunification for those already paroled into the United States through the U.S. Refugee Admissions Program. The federal government is leveraging every tool available to ensure that no individuals who pose a threat to public safety or national security are permitted to enter the United States. The continuous screening and vetting process is ongoing to ensure the continued protection of public safety and national security.

- Created a lawful and orderly process, Uniting for Ukraine (U4U), to issue two-year grants of parole to eligible Ukrainians and their immediate family members fleeing Russia's unprovoked war of aggression. U4U builds on the robust humanitarian assistance the U.S. Government is providing as we complement the generosity of European countries that are hosting millions of Ukrainian citizens and others who have been displaced. As of mid-March, over 150,000 Ukrainians have been authorized to travel to the United States through this process, which also includes interagency screening and vetting both prior to authorizing travel to the United States and upon arrival at a POE. Over 280,000 Ukrainians have arrived in the United States since the conflict began.

On January 4, 2023, USCIS, primarily a fee-funded agency, proposed revisions to its fee schedule that has been in place since 2016. USCIS is considering public comments on this proposal and intends to finalize a new fee schedule before the end of the year. Despite the challenges of operating under an outdated fee structure, USCIS ensured that all of the record number of available employment-based visas for FY 2022 were utilized, supported domestic processing of relocated Afghans, worked to rebuild refugee processing capacity, and stood up the new supporter-driven parole processes for certain Ukrainians, Cubans, Haitians, Nicaraguans, and Venezuelans.

We have also responded to humanitarian crises around the world and at the same time returned to the administration of our immigration laws in a manner keeping with our nation's values by:

- Providing Temporary Protected Status (TPS) benefits to nationals of 16 countries, including new designations and redesignations for: Afghanistan, Burma, Cameroon, Ethiopia, Haiti, Somalia, South Sudan, Sudan, Syria, Ukraine, Venezuela, and Yemen. Four additional countries (El Salvador, Honduras, Nepal, and Nicaragua) had TPS designations terminated by the last Administration but, due to pending litigation, those terminations have not taken effect and beneficiaries continue to receive TPS benefits. In addition, President Biden announced Deferred Enforced Departure (DED) for certain Liberian nationals and Hong Kong residents.
- Restoring the historical understanding of a "public charge" ground of inadmissibility that had been in place for decades, so as not to penalize individuals for using the health benefits and supplemental government services available to them.
- Preserving and fortifying the Deferred Action for Childhood Arrivals (DACA) policy through issuance of a final rule codifying the policy, working with DOJ to defend it against legal challenges, and effectively addressing significant processing backlogs inherited from the prior Administration. Despite our efforts, the program remains under

threat and hundreds of thousands of Dreamers continue to live their lives from one court decision to the next, under great uncertainty.

We have sought to ensure just outcomes through the Interagency Task Force on the Reunification of Families, which I proudly chair and which has reunited more than 600 children separated from their families at the Southwest Border under the Trump Administration's Zero Tolerance policy. We also initiated the Immigrant Military Members and Veterans Initiative, improving support for noncitizen military members, including returning to the United States previously removed veterans who honorably served our nation so they can return to their families and life here and access certain Veterans Affairs benefits to which they are entitled as a result of their service.

On his first day in office, the President delivered to Congress legislation that included critical reforms that would address root causes of migration; expand pathways for legal immigration; prioritize border technology and infrastructure; enhance the ability to prosecute the criminal organizations involved in smuggling and trafficking; and provide a roadmap to citizenship for those who have been contributing members of our communities for years. It is long past time for Congress to act on legislation to fix our broken and outdated immigration system, including by providing permanent protection to Dreamers who only know the United States as home.

Counternarcotics

DHS employs a multi-layered approach to mitigating and countering narcotics trafficking and threats of all types through the use of 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.

With the support of Congress, CBP continues to make significant investments and improvements in drug detection and interdiction technology to detect the presence of illicit drugs, including illicit opioids, in all operating environments, while CBP's National Targeting Center uses advanced analytics and targeting capabilities to identify critical logistics, financial, and communication nodes, and exploit areas of weakness in opioid trafficking networks. Leveraging these investments, CBP seized 11,200 pounds of fentanyl in FY 2021 and 14,700 pounds in FY 2022. This compares to 2,804 pounds in FY 2019.

CBP's extended border and foreign operations mission involves operating aircraft throughout North, Central, and South America, conducting counternarcotics missions to detect and interdict bulk quantities of illicit narcotics. Joint operations beyond the physical borders of the United States involves collaborating with U.S. and international partners to conduct joint maritime operations. The majority of these are maritime operations in the source, transit, and arrival zones of the Western Hemisphere and are accomplished in collaboration with Joint Interagency Task Force South (JIATF South) and host nation partners.

CBP seeks to prevent drug trafficking through POEs, which is where most synthetic drugs enter the United States. Recent DHS Office of Intelligence and Analysis reporting indicates that Mexico-based drug traffickers involved in both drug and human smuggling rarely exploit migrants to smuggle fentanyl into the United States. Analysts continue to assess that the vast majority of fentanyl that enters the United States moves through U.S. POEs, and CBP data indicates that U.S. citizens were responsible for transporting the fentanyl seized in 79 percent of seizures in FY 2022. Personal vehicles remain, by volume, the primary method of conveyance for illicit drugs entering the country over land, with notable increases within commercial truck conveyances for methamphetamine. The NII Systems Program provides technologies to inspect and screen cars, trucks, rail cars, sea containers, as well as personal luggage, packages, parcels, and flat mail through either X-ray or gamma-ray imaging systems. CBP officers use NII systems to effectively and efficiently detect and prevent contraband, including drugs, unreported currency, guns, ammunition, and other illegal merchandise, as well as inadmissible persons, from being smuggled into the United States, while having a minimal impact on the flow of legitimate travel and commerce.

CBP also robustly enforces the Synthetics Trafficking and Overdose Prevention (STOP) Act to prevent trafficking by mail. CBP operates within major international mail facilities to inspect international mail and parcels arriving from more than 180 countries. Additionally, CBP and the U.S. Postal Service are working to increase the amount of advance electronic data (AED) received on international mail. This advance information enables HSI and other agencies to identify networks of foreign suppliers and domestic importers that are responsible for smuggling fentanyl into the United States.

HSI also plays a critical role in countering narcotics trafficking by exchanging information, coordinating investigations, and facilitating enforcement actions with law enforcement partners abroad to deter the ability of TCOs to smuggle drugs, people, and contraband into and out of the United States. FY 2022 statistics reveal HSI conducted 11,535 narcotics-related criminal arrests and seized roughly 1.87 million pounds of narcotics, which included 20,981 pounds of fentanyl. Additionally, HSI agents seized more than $210 million in total currency and assets through their narcotics enforcement efforts.

One of HSI's most significant tools to combat TCOs engaged in fentanyl trafficking are the Border Enforcement Security Task Forces (BESTs). BESTs eliminate the barriers between federal and local investigations and close the gap with international partners in multinational criminal investigations. BESTs continue to be a primary vehicle used to carry out HSI's comprehensive, multi-layered strategy to address the national opioid epidemic.

Recognizing the unprecedented epidemic of deaths from illicit opioids, HSI recently developed and began the implementation of its *Strategy for Combating Illicit Opioids*. The strategy builds upon many of HSI's core investigative authorities and capabilities in combating TCOs and focuses efforts on four core goals, all of which align with the National Drug Control Strategy. They are: 1) reduce the international supply of illicit opioids; 2) reduce the domestic supply of illicit opioids; 3) attack the enablers of illicit finance, cybercrime, and weapons smuggling; and 4) conduct outreach with private industry. Through this strategy, HSI aims to make important strides in reducing the harm illicit opioids have on U.S. communities.

One of HSI's primary tactics in the fight against fentanyl is the Transnational Criminal Investigative Unit (TCIU) Program. The TCIU program was created to help facilitate the exchange of information between the United States and its foreign partners and to enhance the host country's ability to investigate and prosecute individuals involved in transnational criminal activities that threaten the stability and national security of the region and pose continuing threats to the homeland security of the United States. HSI TCIUs are comprised of foreign law enforcement officials, customs officers, immigration officers, and prosecutors who undergo a strict vetting process conducted by HSI to ensure that shared information and operational activities are not compromised. The units work to identify targets, collect evidence, share information, and facilitate the prosecution of transnational criminal organizations both in-country, among other foreign partner nations, and through the U.S. judicial system. HSI TCIUs prioritize criminal investigations related to weapons trafficking and counter-proliferation, money laundering and bulk cash smuggling, human smuggling, human trafficking, illegal drug trafficking, intellectual property rights violations and other customs fraud, child exploitation, cybercrime, and other violations of law within HSI's investigative purview. The current HSI TCIU footprint consists of over 500 personnel assigned to 12 TCIUs and two International Task Forces in 14 countries around the world. HSI anticipates expanding the program to additional countries in FY 2023. Colombia and Panama are the two largest international TCIUS, with nearly 70 vetted individuals.

HSI has also launched targeted campaigns. On March 13, 2023, CBP and HSI launched Operation Blue Lotus to facilitate and increase fentanyl interdictions at and between the POEs and develop criminal cases along the Southwest border. Starting at the ports of San Ysidro, CA, Otay Mesa, CA, and Nogales, AZ, Operation Blue Lotus aims to curtail the flow of illicit fentanyl smuggled into the U.S. from Mexico while simultaneously illuminating the Transnational Criminal Organizations (TCOs). In its first week, Operation Blue Lotus resulted in 18 seizures, 16 federal arrests, and 2 state arrests, stopping over 900 pounds of fentanyl, over 700 pounds of methamphetamines, and over 100 pounds of cocaine from entering the United States. The operation is expected to run through May 2023.

The U.S. Coast Guard (USCG) leads maritime interdictions of narcotics in the Western Hemisphere. The USCG disrupts illicit trafficking where it is most vulnerable: at sea in the transit zone, often far from U.S. shores, before bulk quantities reach the shore and are divided into small, hard-to-detect loads. The USCG is continuing to enhance cooperation with partner 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 JIATF South, allowing for maximum counterdrug coordination across the hemisphere. These efforts directly enable target identification and development that prioritize law enforcement investigations – perpetuating the interdiction continuum, the removal of multi-ton quantities of drugs from the supply chain and provide critical evidence for the prosecution of TCO members. In FY 2022, the USCG removed approximately 152 metric tons of cocaine, 60,000 pounds of marijuana, and 7.7 metric tons of other narcotics, including methamphetamines, heroin, and hashish. In addition to these drug removals, a USCG-led multi-agency effort in FY 2022 tied their maritime law enforcement

operations to the indictment and extradition of a consolidated priority organizational target to Puerto Rico for prosecution.

The Department appreciates Congress extending for two years the statutory authority to establish and operate Joint Task Forces (JTFs) in the FY 2023 NDAA. JTFs provide a direct operational coordination layer to enhance the multi-faceted challenges facing DHS. Today, JTF-East is responsible for ensuring Departmental unity of effort in the southern maritime approach to the United States and demonstrates the tangible, positive impacts that JTFs can have on enhancing DHS-coordinated operations.

Human Trafficking and Child Sexual Exploitation and Abuse

Combating the abhorrent crimes of human trafficking and child sexual exploitation and abuse (CSEA) is a top priority for the Department. These crimes target the most vulnerable among us, offend our most basic values, and threaten our national security and public safety.

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) coordinates the counter-trafficking efforts of 16 offices and component agencies, reflecting our commitment to combat this heinous crime from every angle: investigations and enforcement, intelligence, public education and prevention, policy innovation, victim protection and support, and more. HSI leads criminal investigations into sex trafficking and forced labor, making 3,655 human trafficking-related arrests during FY 2022, an increase of more than 50 percent over the previous fiscal year. Our human trafficking investigations led to 638 convictions, an increase of more than 80 percent over the previous year.

CBP is charged with rooting out forced labor-made goods from U.S. supply chains by preventing the importation of such illicit merchandise into the United States. CBP carries out this mission by investigating allegations of forced labor in supply chains and, where allegations are corroborated, issuing Withhold Release Orders (WROs) and forced labor findings. CBP issued six WROs, two findings, and one WRO modification in FY 2022. In June 2022, CBP also began enforcing the landmark Uyghur Forced Labor Prevention Act (UFLPA), enacted by Congress in December 2021.[2] Together with the DHS Office of Policy, which chairs the interagency Forced Labor Enforcement Task Force (FLETF), and other interagency members including the Departments of Labor, State, Justice, Treasury, Commerce, and the United States Trade Representative, CBP led the UFLPA's successful implementation and is committed to seeing it fully enforced to prevent the importation of goods produced, wholly or in part, with forced labor in the Xinjiang Uyghur Autonomous Region in the PRC.

DHS employs a victim-centered approach across all human trafficking programs and operations. This approach seeks to minimize additional trauma, mitigate undue penalization, and provide needed stability and support to victims. This approach is not only critical to helping

[2] UFLPA established a rebuttable presumption that the importation of any goods, wares, articles, and merchandise mined, produced, or manufactured wholly or in part in the Xinjiang Uyghur Autonomous Region of the People's Republic of China, or produced by certain entities, is prohibited by Section 307 of the Tariff Act of 1930 and that such goods, wares, articles, and merchandise are not entitled to entry to the United States.

survivors begin to repair their lives, it enables law enforcement to better detect, investigate, and prosecute perpetrators. For this reason, in FY 2022, DHS expanded the HSI Victim Assistance Program (VAP), increasing the number of victim assistance personnel, including victim assistance specialists (VASs) and forensic interview specialists (FISs), by 40 percent. In FY 2023, HSI will grow the program by another 60 percent. These investments have led to increases in the identification of victims of human trafficking, referrals for social services in local communities, and forensic interviews using trauma-informed, victim-centered methods to elicit accurate and complete information while minimizing distress. The VAP assisted 3,326 victims worldwide in FY 2022, including 1,138 victims of child exploitation and 765 human trafficking victims.

Public education is also a critical component of our counter-trafficking work. To name just a few of our achievements in this mission in FY 2022, the DHS Blue Campaign, the Department's national human trafficking public awareness initiative, trained more than 150,000 federal government, NGO, law enforcement, and public participants on how to recognize the indicators of human trafficking. And our Federal Law Enforcement Training Centers trained more than 3,300 law enforcement officers, representing over 90 federal law enforcement agencies, on how to recognize and respond to potential trafficking cases.

The Department is also redoubling efforts to combat online CSEA, which has increased dramatically in scope and severity in recent years. This scourge is nothing short of a global crisis. New forms of CSEA have also emerged and grown exponentially, including the live streaming of child sexual abuse and sophisticated sextortion and grooming schemes. The National Center for Missing and Exploited Children (NCMEC), the nation's clearinghouse for child sexual abuse material (CSAM), received over 32 million cyber tips in 2022, corresponding to more than 88 million images and videos of child sexual abuse—a roughly 75 percent increase in just five years. What is worse, these numbers represent only CSAM on the open web; they do not include the massive amount of child sexual abuse content produced and shared on the dark web.

In response, we are strengthening our 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 10,000 child victims of sexual exploitation, including more than 1,000 victims in FY 2022. The CEIU also detects and apprehends producers and distributors of CSAM and perpetrators of transnational child sexual abuse, employing the latest technology to collect evidence and track the activities of individuals and organized groups who sexually exploit children via websites, chat rooms, peer-to-peer trading, and other internet-based platforms. CEIU's Operation Predator targets child sexual predators on both the open web and dark web, and in FY 2022 led to the arrest of 4,459 perpetrators for crimes involving child sexual abuse. During this same period, the CEIU Angel Watch Center issued 4,527 notifications regarding international travel by convicted child sex offenders, resulting in more than 1,073 denials of entry by foreign nations. The DHS Science & Technology Directorate also develops and deploys leading-edge forensic tools and technologies that enable CEIU agents and other

national and international law enforcement partners to identify and locate child victims of online sexual exploitation. These tools include livestream capabilities, advanced facial recognition technologies, and speech and language technologies.

Our law enforcement agents will be the first to state, however, that we cannot investigate and arrest our way out of this epidemic. So, we are also expanding our policy, public education, and strategic engagement infrastructure to elevate and enhance the Department's counter-CSEA capabilities. DHS remains steadfast in advancing and leveraging our full breadth of authorities and resources to end these heinous crimes, and we urge you to support our efforts to expand this critical work to fight the rapidly escalating crisis of online child sexual exploitation and abuse.

Conclusion

The Department of Homeland Security was created in response to a singular threat. In the two decades since the September 11, 2001 terrorist attacks and as DHS enters its third decade, the Department has evolved to address multiple unforeseen and complex challenges. Through it all, our workforce has demonstrated exceptional skill and an unwavering commitment to keeping our country safe.

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. Thank you.