TESTIMONY OF

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

BEFORE

Committee Homeland Security and Governmental Affairs
United States Senate

ON

"Threats to the Homeland"

November 17, 2022
Washington, DC

Chairman Peters, Ranking Member Portman, and distinguished Members of this Committee:

Thank you for inviting me to join you today. Next week marks the 20th anniversary of the Homeland Security Act being signed into law, 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. It 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.

Thanks to extensive deliberation and cooperation from both sides of the aisle, Congress created a Department that significantly reduced the risk foreign terrorism poses to the homeland by increasing our capacity to prepare for and respond to those events. However, foreign terrorism remains a persistent threat that DHS combats every day. Foreign terrorist organizations remain committed to attacking the United States from within and beyond our borders. They use social media platforms to amplify messaging intended to inspire attacks in the homeland and have adapted to changing security environments, seeking new and innovative ways to target the United States. Foreign terrorists will continue to expand their networks, cross international borders, raise funds, and organize to improve their ability to target the homeland.

Rapidly emerging technologies, evolving cyber capabilities, and increasing economic and political instability around the world are contributing to a heightened threat environment at home. From cyber-attacks on our critical infrastructure and increasing destabilizing efforts by hostile nation states, to the rise of domestic violent extremism, the threats facing the homeland have never been greater or more complex.

Flouting internationally accepted norms of responsible behavior, transparency, and accountability in cyberspace, our adversaries—hostile nations and non-nation state cybercriminals—continue to advance in capability and sophistication. Their methods vary, but their goals of doing harm are the same. Hostile nations like Russia, the People's Republic of China (PRC), Iran, North Korea, and cybercriminals around the world continue to sharpen their tactics and create more adverse consequences. Their ransomware attacks target our financial institutions, hospitals, pipelines, electric grids, and water treatment plants to wreak havoc on our daily lives. They exploit the integrated global cyber ecosystem to sow discord, undermine liberal democracy, and erode trust in our institutions, public and private. These cyber operations threaten the economic and national security of every American, and many others around the world.

In particular, the PRC is using its technology to tilt the global playing field to its benefit. They leverage sophisticated cyber capabilities to gain access to the intellectual property, data, and infrastructure of American individuals and businesses. Russia's unprovoked invasion of Ukraine intensified the risk of a cyber-attack, impacting our critical infrastructure earlier this year. Nation state aggression is creating a heightened risk of chemical, biological, radiological, and nuclear-related threats to Americans as well.

Fast-emerging technologies like unmanned aerial systems, artificial intelligence, internet communications, and cryptocurrencies are helping societies be more productive, creative, and entrepreneurial. They also are introducing new risks. Transnational criminal organizations are deploying these technologies to commit a wide array of crimes as they continue to grow in size, scale, sophistication, and lethality.

The risk of targeted violence, perpetrated by actors abroad and at home, is substantial. Emerging technology platforms allow individuals and nation states to fan the flames of hate and personal grievances to large audiences and are encouraging people to commit violent acts. Those driven to violence are targeting critical infrastructure; soft targets such as sports venues, shopping malls, and other mass gatherings; faith-based institutions, such as churches, synagogues, and mosques; institutions of higher education; racial and religious minorities; government facilities and personnel, including law enforcement and the military; and perceived ideological opponents.

Addressing these threats requires a whole-of-society approach across federal, state, and local governments, the private sector, nonprofits, academia, and - most importantly - every citizen. Congress may not have predicted the extent of today's threat environment when our Department was created 20 years ago, but our mission has never been more vital, our components have never collaborated more closely, and our nation has never been more prepared. We must harness the same deliberative and bipartisan spirit in which this Department was created to combat the vast threats Americans face today.

Combating Terrorism and Targeted Violence

Foreign Terrorism Threats

Since the inception of this Department, the threat landscape has evolved dramatically, and DHS has remained vigilant against all terrorism-related threats to the homeland. In the years immediately following the September 11th 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 America whose ideologically motivated terrorist activities are primarily inspired by Foreign Terrorist Organization's (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 al-Qa'ida and the Islamic State of Iraq and ash-Sham (ISIS) have continued to celebrate perceived victories over the United States pointing to the September 11, 2001 terrorist attacks on their anniversaries and the U.S. military withdrawal from Afghanistan to encourage the use of violence by their supporters. ISIS media and its supporters have also sought to revitalize ISIS's image as a global enterprise and to portray the group as the true vanguard of resistance against the United States and its allies. ISIS and its supporters continue to call for attacks in the United States, and supporters often share online tactics and techniques for reducing the likelihood of being detected by law enforcement.

Some terrorist-associated individuals maintain a presence in the Western Hemisphere, and could be leveraged to support extremist activities, possibly involving the homeland. For example, al-Qa'ida-associated individuals in Brazil are involved in financial support through businesses they manage in the country, transferring funds in support of extremist-related activities, and involved in the printing and purchasing of counterfeit currencies in support of al-Qa'ida's global efforts.

We continue to see Iran 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 historical 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, federal prosecutors unsealed charges against an IRGC member for plotting to assassinate a former US official. 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 to stay aware of ongoing threat streams and take preventative actions as appropriate.

DHS works closely with our law enforcement, national security, and Intelligence Community partners to 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 FY 2022, the National Vetting Center (NVC), managed by DHS, enhanced its ability to support vetting for DHS and Department of State. 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, to include increasing our information sharing and vetting capabilities. DHS is increasing our ability to engage in biometric comparison with our foreign partners, and most recently amended requirements for the Visa Waiver Program (VWP) to require participation in the Enhanced Border Security Partnership (EBSP). Under EBSP, DHS will be able to conduct biometric checks against VWP member countries' biometric data to authenticate VWP travelers' identities to quickly receive immigration and criminal history information.

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, and territorial (SLTT) partners, including the National Network of Fusion Centers, in accordance with applicable law and DHS privacy, civil rights, civil liberties, and intelligence oversight policies.

Domestic Violent Extremism and Targeted Violence

The evolving terrorism threat to the homeland now also includes those fueled by a wide range of violent extremist ideologies and grievances, including domestic violent extremists (DVEs). DVEs are U.S.-based individuals who seek to further political or social goals wholly or in part through violence, without direction or inspiration from a foreign terrorist group 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. Today, these U.S.-based individuals, who are inspired by a broad range of violent ideologies, pose the most significant and persistent terrorism-related threat to the homeland.

The Intelligence Community 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/anti-authority violent extremism threat category, present the most lethal DVE threat in the homeland. In many cases, DVE actors have spent inordinate amounts of time online viewing extremist, violent materials and engaging with like-minded individuals. RMVEs are the DVE actors with the most persistent and concerning transnational connections, because individuals with similar ideological beliefs exist outside of the United States. These RMVEs communicate with and seek to influence each other. Such connectivity with overseas violent extremists might lead to a greater risk of U.S. RMVEs mobilizing to violence.

A June 2022 DVE assessment[1] by DHS, the Federal Bureau of Investigation (FBI), and the National Counterterrorism Center (NCTC) determined that the threat from DVEs is likely to persist for the coming months, with heightened tensions surrounding the 2022 elections, continued perceptions of government overreach, and immigration-related developments or potential new legislation and court rulings; all presenting potential flashpoints that could serve to encourage or inspire acts of violence.

To prepare for this threat, the Department has embraced a community-based approach to prevent 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 focus on reducing the threat of violence; we must make it harder to carry out an attack and reduce the potential for loss of life by preventing mobilization to violence.

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 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, nonprofits, public safety officials, and others—to create programs that connect individuals with the help they need. CP3 relies on the expertise of DHS's Privacy and Office for Civil Rights and Civil Liberties professionals to ensure all public-facing prevention resources, web content, and training materials are protective of Americans' privacy rights and 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. DHS recently

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

announced 43 TVTP grant awards to entities in 20 states, totaling $20 million, for Fiscal Year (FY) 2022. Managed by CP3 and the Federal Emergency Management Agency (FEMA), the TVTP Grant 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. This year's awards fulfill the grant program's focus on prioritizing the prevention of domestic violent extremism, as well as efforts to counter mobilization to violence that occurs online, while respecting privacy, civil rights, and civil liberties.

DHS 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 this critically important program has seen a funding increase this past fiscal year of $70 million from FY 2021 levels, for a total of $250 million. The FY 2023 President's Budget request proposes another 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 has designated "Combating Domestic Violent Extremism" as a "National Priority Area" for both FY2021 and FY2022. This means that between FY 2021 and FY 2022, states and local governments across our nation will spend over $111 million in grant funding on capabilities to detect and protect against these threats.

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.

DHS's Cybersecurity and Infrastructure Security Agency (CISA) works closely with public and private sector partners to build security capacity to mitigate cyber and physical risks, including threats posed by terrorism and targeted violence. Through trainings, tools, exercises, and best practices, CISA supports organizations in enhancing security holistically and in countering the most prevalent threats, including active shooters. Protective Security Advisors – a cadre of more than 140 security subject matter experts located across the country – provide direct and tangible support to facilities by conducting security assessments and advising on enhanced protective measures.

Gender Based Violence

Gender-based violence (GBV) is any harmful threat or act directed at an individual or group based on their actual or perceived biological sex, gender identity, gender expression, sexual orientation, or difference from social norms related to masculinity or femininity. Gender-based violence is rooted in structural gender inequalities and power imbalances. The DHS Council for Combatting Gender Based Violence (CCGBV) works to identify and build consensus and best practices around combatting GBV, including initiatives focused on domestic violence, forced marriage, female genital mutilation/cutting (FGM/C), online abuse and harassment, and trafficking in persons. The work of the CCGBV comes at an inflection point for the health, safety, and well-being of women and girls, as the COVID-19 pandemic has exacerbated a pre-existing "shadow pandemic" of gender-based violence, as well as economic, health, and caregiving crises that disproportionately impacted women and girls long before the pandemic struck.

Women and girls are particularly vulnerable and may be specifically targeted for acts of gender-based violence (GBV) as a part of terrorist activities, requiring specific protection measures. This includes safeguarding women's human rights during disaster and crisis situations, displacement, and other scenarios, in order to counter the effects of extremist violence. The USSS's NTAC has also identified the specific threat posed by misogynistic extremism, men who identify themselves as involuntary celibates or "incels" and target women for violence.

Cyber Threats

Our interconnectedness and the technology that enables it—the cyber ecosystem—exposes us to a dynamic and evolving threat environment, one that is not contained by borders or limited to centralized actors, 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, the PRC, Iran, and North Korea, as well as cybercriminals around the world, continually grow more sophisticated and create more adverse consequences.

Within the past two 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 a major pipeline company, JBS Foods, Kaseya, and 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 in the first half of 2021 paid an estimated $590 million in ransoms, compared to $416 million over all of 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. Last February, Russia conducted a cyber-attack against commercial satellite communications, impacting families and businesses across Europe.

The PRC poses a highly advanced cyber threat to the homeland. The PRC continues 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. Iranian cyber-attacks recently 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.

In the last two years alone, North Korea has largely funded its weapons of mass destruction programs through cyber heists of cryptocurrencies and hard currencies totaling more than $1 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 for 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 was also a popular target 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. DHS's investigative components, the USSS and Homeland Security Investigations (HSI), are dedicated to stopping criminal acts, identifying and arresting the criminals, and working to seize and return stolen funds to the victims. Cybercrimes are often transnational with the criminal actors, their infrastructure, and their victims, spread across the globe. The USSS and HSI partner with federal and SLTT law enforcement and with international and foreign law enforcement in combating cybercrimes.

It is the Department's responsibility to help 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 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 information received from our private sector partners' reports will enable CISA, along 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 attacks, 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 this summer addressing the risk posed by vulnerabilities in the widely used "Log4j" open-source software library.
- In February 2022, recognizing the heightened risk of malicious cyber activity related to the Russia-Ukraine conflict, 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 approximately 30 representatives from Sector Risk Management Agencies (SRMAs) and independent regulators, has convened several times to discuss opportunities to coordinate, deconflict, and harmonize federal cyber incident reporting requirements, including those issued through regulation. To facilitate this effort, DHS has inventoried all federal cyber incident reporting requirements and held one-on-one consultations with over 20 CIRC members.

- In September 2022, CISA and FBI launched the Joint Ransomware Task Force (JRTF) to coordinate a whole-of-government effort to combat the threat of ransomware. A major objective of the JRTF is to coordinate efforts among federal agencies and private sector and SLTT partners to improve our nation's response to ransomware incidents, 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 in May 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, and identifying cybersecurity gaps. TSA recently updated these directives to focus requirements on achieving security outcomes, rather than on prescriptive measures. Through security program amendments, TSA issued several similar requirements to larger airports and air carriers, with additional measures under consideration. DHS continues to consider what additional directive action might be necessary to address urgent cyber threats in transportation and other critical infrastructure sectors and will continue to work closely with the U.S. Department of Transportation (DOT), the U.S. Department of Energy, and other Sector Risk Management Agencies.

Emerging Technology Threats

Unmanned Aircraft System (UAS) Threats

The rapid proliferation of drones and their expanded utilization 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), disrupted and damaged critical infrastructure, and nearly every day, transnational organized criminal organizations (TCOs) use drones to convey illicit narcotics (including

fentanyl) and contraband across U.S. borders and conduct hostile surveillance of law enforcement.

Congress extended the law that provides DHS's current counter-UAS (C-UAS) authority through December 16, 2022, under the continuing resolution. Ensuring that the existing authority does not lapse, and the C-UAS activities currently being performed by DHS do not cease, are critically important to our missions protecting the President and Vice President, along the Southwest Border, securing sensitive federal facilities, and safeguarding the public. DHS has successfully executed C-UAS operations at mass gatherings and Special Security Assessment Rating (SEAR) and National Special Security Events (NSSEs), including the 2022 World Series, the Super Bowl, the Indianapolis 500, the UN General Assembly, the Democratic and Republican National Conventions, and the State of the Union address. At all times, DHS engages in these activities in a manner that protects individuals' privacy, civil rights, and civil liberties consistent with the requirements of the current law and DHS policy.

To ensure that the Department can continue its C-UAS activities, the Administration has requested that Congress pass a two-year, clean extension of existing C-UAS authorities in the NDAA or another legislative vehicle before these authorities expire. Any lapse in or narrowing of DHS's 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, including at the southern border where drones are being used to traffic fentanyl and other dangerous contraband. Rather, the authority should be expanded to address critical gaps in the current law, such as a lack of protection for U.S. airports from drones, the lack of authority for DHS to partner with state, local, tribal, and territorial law enforcement, enabling them to detect and mitigate threats themselves, and the inability of critical infrastructure owners and operators to detect drones operating near their facilities or request federal mitigation assistance.

Congressional action is urgently required, as DHS's authority to detect and counter drone threats will expire on December 16, 2022. A lapse in this authority could have catastrophic implications for homeland security.

5G/6G

In the cyber ecosystem—which underpins the unprecedented interconnectedness we've 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 government when requested by authorities. It is our belief that our essential telecommunications networks should not be owned or operated by companies who 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 efforts to secure 5G and to mitigate possible malicious use by PRC technology. At CISA, our 5G team provided supply chain risk analyses that were a significant contribution to the federal government's response to this issue. However, today we are looking beyond 5G to the next frontier in 6G. 6G is still around 8-10 years away but the process to create the standards for 6G roll out 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 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 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 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, *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 U.S. Secret Service has achieved notable successes in combatting cyber-enabled financial crimes, including dismantling two centralized virtual currency providers that supported extensive criminal activity and successfully investigating a Russia-based criminal scheme attempting to defraud cryptocurrency exchange customers of $16.8 million.

U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) has offices in over 50 countries and works to combat cybercrimes, including through 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, notably 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 use of AI can help us more effectively and efficiently accomplish our mission to secure the homeland.

- Over the past several years, DHS has been engaged in AI conversations across the federal government on AI ethics, governance, and use policies.
- We are taking a strategic approach to mitigate and counter adversary 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—on sharing best practices and developing 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 state, local, tribal, and territorial (SLTT) 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 recent National Security Memorandum on quantum computing.

Smart Cities and Connected Communities

The convergence of a number 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." 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 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.

Transnational Criminal Organizations

Transnational Criminal Organizations (TCOs) continue to pose a threat to the United States, particularly U.S. public health, as well as our economic and national security. Over recent years, they have grown in size, scale, sophistication, and lethality. According to a 2018 estimate, the U.S. Treasury Department estimated drug related crime alone generated over $100 billion in proceeds in the United States. These profits also come with a high toll on human life; the opioid drugs these TCOs traffic were responsible for the majority of the over 100,000 U.S. overdose deaths between April 2020 and April 2021, according to CDC reporting. Mexico-based TCO criminal activity is not limited to drug trafficking; they engage in wide variety of other criminal activity. TCOs also facilitated and profited from smuggling migrants into the United States and their illicit trade activity led to the seizure of over $2.14 billion in Intellectual Property violations in FY21. TCOs are adept at changing their illicit drug supply chains, shifting human smuggling routes and tactics, and using various money laundering techniques to evade law enforcement.

TCOs operating in Mexico, specifically the Sinaloa Cartel and New Generation Jalisco Cartel, almost certainly will continue to dominate illegal drug trafficking—including trafficking of methamphetamine, fentanyl, cocaine, and heroin—into the United States.

Other TCOs, some working with Mexico-based TCOs, also pose a growing threat to the homeland. TCOs in the PRC launder money for or sell precursor chemicals to TCOs in Mexico, while Central American gangs, such as Mara Salvatrucha (MS-13) and the 18th Street Gang, largely serve as cross-border couriers, smuggling drugs and people for Mexico-based TCOs. Asia-, Africa-, and Balkans-based TCOs are involved in a range of criminal activities that affect the homeland, such as money laundering, financial fraud, human smuggling, and racketeering.

To confront TCOs and other threat networks, DHS has embraced an approach that leverages U.S. Customs and Border Protection (CBP)'s unique authorities, data holdings, Intelligence Enterprise, and interagency partnerships to illuminate, disrupt, degrade, and dismantle networks that pose a threat to the homeland and its interests. CBP's international collaboration and integration with the interagency optimizes the collective global effort, which identifies options for intelligence-driven, risk-mitigating responses. Our success at identifying, degrading, and disrupting transnational networks relies on CBP frontline agents, officers, trade, and intelligence professionals working hand in hand with the whole of government, as well as international partners. Developing these relationships and capabilities enables CBP to proactively identify and stop threats before they arrive at U.S. borders.

Counternarcotics

DHS employs a multi-layered approach to countering narcotics trafficking. The shift in the illicit drug market towards synthetic drugs, primarily fentanyl, its analogues, and other opioids, led CBP to develop and implement the CBP Strategy to Combat Opioids. 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. CBP's extended border and foreign operations mission involves collaborating with U.S. and international partners to conduct joint maritime operations in the source, transit, and arrival zones of the Western Hemisphere. In collaboration with Joint Interagency Task Force South (JIATF-S), CBP operates aircraft throughout North and Central America, conducting counter-narcotics missions to detect and interdict bulk quantities of illicit narcotics. 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 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.

CBP seeks to prevent drug trafficking through ports of entry, which is where most drugs enter the U.S. Personal vehicles remain the primary method of conveyance encountered for illicit drugs entering the country by volume over land, with notable increases within commercial truck conveyances for methamphetamine. The Non-Intrusive Inspection (NII) Systems Program deploys technologies to inspect and screen conveyances or cars, trucks, railcars, 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 help them 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 ICE 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. Preliminary FY 2022 statistics reveal HSI conducted 11,535 criminal arrests and seized roughly 1.87 million pounds of narcotics, which included 20,980 pounds of fentanyl, in FY 2022. Additionally, in FY 2022, 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.

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 zones, often far from U.S. shores before bulk quantities are divided for distribution. The Coast Guard is continuing to expand cooperation with partner nations in South and Central America to combat the flow of narcotics before they reach U.S. shores. In FY 2022, the USCG removed approximately 140 metric tons of cocaine, 60,000 pounds of marijuana and 8 metric tons of other narcotics, including methamphetamines, fentanyl, heroin, and hashish.

The Department welcomes Congress' support for extending the statutory authority to establish and operate Joint Task Forces (JTFs). 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 Smuggling

Migration is a hemispheric challenge, one not limited to the United States. Displacement and migration are higher than at any time since World War II. At our Southwest Border, we are experiencing historic levels of encounters. The demographics of the population have also

changed, with more than triple the number of Venezuelans, Cubans, and Nicaraguans than last year, as people flee repressive governments and lack of economic opportunity. In September 2022, Venezuelans, Cubans, and Nicaraguans accounted for almost half of unique encounters at the Southwest Border – triple their share from one year ago. Reporting from the U.S. Agency for International Development (USAID) suggests that nearly one in four Venezuelans have fled their home since 2014, approximately seven million people. At least one in three of those who have fled from Venezuela have settled in Colombia. Additionally, the Office of the United Nations High Commissioner for Refugees (UNHCR) has reported that Costa Rica is hosting more than 200,000 Nicaraguan migrants, equal to nearly four percent of their total population.

We assess that global food and water shortages, poor economic conditions, and other socio-political factors will continue to drive an increase in cross-border migration. TCOs that specialize in human smuggling increasingly exploit and financially benefit from the continued growth in global migration trends. TCOs in Mexico play an influential role in human smuggling, increasingly facilitating illicit migration to and across the border. These groups control large sections of territory just south of the U.S. border and have traditionally taxed human smugglers to move migrants through their areas of operation.

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. In April 2022, DHS launched a first-of-its-kind effort, unprecedented in scale, to disrupt and dismantle human smuggling networks. So far, this campaign has resulted in the arrest of over 6,400 smugglers and the disruption of over 6,750 smuggling operations. This work includes raiding stash houses, impounding tractor-trailers that are used to smuggle migrants, and confiscating smugglers' communications technology.

On October 16, 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 fiscal year 2021, the average sentence smuggling drugs (average 74 months) was almost 5 times longer than for smuggling human beings (average of just 15 months). These lower sentences negatively affect prosecutors' ability to negotiate plea agreements and obtain co-operation 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 do this work alone; hemispheric challenges require hemispheric solutions. We are strengthening our relationships with partners in Mexico and Central and South America and taking unprecedented actions as a result. In October 2022, DHS announced joint actions with the Government of 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.

We are matching the unprecedented migration challenge we face with unprecedented and innovative solutions to secure the border. We are surging resources and increasing efficiency,

prioritizing smart border security solutions, making historic investments in technology, taking the fight to cartels and smugglers, and doing more with our regional partners than ever before. CBP has 23,000 agents and officers working along the Southwest Border and is seeking another 300 agents in the FY 2023 budget request.

We have hired and contracted for over 1,000 Border Patrol Processing Coordinators to get agents back into 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 humanely prevent and respond to increases in irregular migration by surging and coordinating our border security and law enforcement resources. We are also supporting border communities as well as interior cities – both local governments and NGOs – that are responding to a surge in migration, including through the Emergency Food and Shelter Program.

We are prioritizing smart border security solutions, grounded in evidence rather than rhetoric, and making historic investments in technology. We have incorporated mobile intake and en route processing to begin processing non-citizens in the field; integrated digital case review saving over 70,000 hours of agent time; and advanced capacity by leveraging virtual processing capabilities.

In addition to our digitization efforts, we are also installing effective technology like linear ground detection systems and automated surveillance towers. We have also made historic investments in non-intrusive inspection technology to be deployed at ports of entry to increase our interdiction of illicit drugs, because we know that traffickers seek to smuggle drugs through the ports of entry in all modes of transportation.

Trade in Counterfeit Goods and Theft of Intellectual Property

The Department continues to facilitate legitimate trade by investigating TCOs that profit from the sale of counterfeit goods and the theft of Intellectual Property (IP). To this end, HSI's Intellectual Property Rights Coordination Center (IPR Center) brings together 30 federal and international agencies to combat IP theft. In FY22, HSI initiated more IP theft cases; affected more criminal arrests, indictments, and convictions; and seized a higher value of counterfeit goods, more than $1.1 billion worth, than in FY21.

HSI's Operation Chain Reaction targets counterfeit goods entering the U.S. government supply chain, including that of the Armed Services. As an example of HSI's impact, the agency recently indicted one of the largest importers of counterfeit network routers. These routers, worth more than $1 billion had they been genuine, were destined to sensitive end-users, including in the Department of Defense, the FBI, government aerospace contractors, and medical facilities. In another example, HSI recently secured a guilty plea from an importer of counterfeit military uniforms destined to be sold to the Department of Defense. These counterfeit uniforms failed fire-resistance testing and failed to hide the wearer's radiation levels, making them detectible to enemy optics. Had these counterfeit goods not been seized, they would have imperiled the safety of our warfighters and exposed our service members to harm.

Human Trafficking and Child Sexual Exploitation

Combatting the abhorrent crimes of human trafficking and child sexual exploitation and abuse is a top priority for the Department. These crimes target the most vulnerable among us, offend our most basic values, and threaten our personal and public safety. Nearly every component within DHS is involved in combating human trafficking. We employ a victim-centered approach across our policies and programs, striving to support and protect victims. We lead criminal investigations into sex trafficking and forced labor, with HSI initiating nearly 1,400 investigations in FY 2022 alone and helping achieve hundreds of federal and state-level convictions each year against traffickers. We develop leading-edge technologies to identify and locate victims and perpetrators. We shine a light on these dark crimes through the Blue Campaign, our signature public awareness and education effort. We train our personnel to recognize and respond to human trafficking in the course of their daily responsibilities, delivering 53 training and outreach events to 5,927 participants in FY22. These efforts are streamlined and strengthened through the DHS Center for Countering Human Trafficking, the first Department-wide operational coordination center for combating human trafficking and the importation of goods produced with forced labor.

Combating trade in illicit goods produced with forced labor is also a critical part of our counter-trafficking mission. Recent studies estimate that upwards of 27 million people around the world are trapped in forced labor bondage, many of whom are members of racial, religious, and ethnic minority groups. Working to end these horrific practices not only promotes respect for human rights and dignity, but also benefits U.S. national security and other interests overseas. CBP is charged with rooting out forced-labor-made goods from our supply chains by preventing the entry of these illegal goods into the U.S. market. 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.

This year, DHS led the interagency Forced Labor Enforcement Task Force (FLETF) in its successful implementation of the Uyghur Forced Labor Prevention Act (UFLPA), which was enacted by Congress and signed into law at the end of 2021. Going forward, CBP will continue to enforce the new law, and DHS, as FLETF Chair, will continue to lead the interagency in updating the UFLPA enforcement strategy, including the list of entities subject to the UFLPA's rebuttable presumption.

The scope and severity of online child sexual exploitation and abuse (CSEA) has increased dramatically in recent years. Reports of online child sexual abuse material (CSAM) to the National Center for Missing and Exploited Children, the nation's clearinghouse for CSAM, increased by more than 35 percent between 2020 and 2021 (to nearly 30 million reports), and 2022 year-to-date numbers foreshadow an even greater increase this year. Increasingly, the victims of these horrific crimes are infants and toddlers, and the abuse has become more violent. New forms of CSEA have also emerged and grown exponentially, including the live streaming of child sexual abuse and sophisticated sextortion and grooming schemes.

That is why I am redoubling the Department's efforts in this space. We are strengthening our Cyber Crimes Center (C3), including HSI's Child Exploitation Investigations Unit (CEIU), a

global leader in counter-CSEA law enforcement operations. Every day, the extraordinary men and women of C3 and HSI field offices around the country and the globe work tirelessly to locate and apprehend offenders, identify and rescue victims, and share information with our partners in this fight. In FY21, CEIU identified and/or rescued 1,177 child victims in child exploitation investigations. During this same period, CEIU arrested 3,776 individuals for crimes involving the sexual exploitation of children and helped to secure more than 1,500 convictions. In FY 2022, HSI Victim Assistance Specialists assisted 3,326 victims of crimes, of which 1,138 were child exploitation victims. HSI Forensic Interview Specialists conducted 1,836 trauma-informed forensic interviews, of which 1,238 were in support of bringing perpetrators of child exploitation crimes to justice.

We are also building policy, public-education, and strategic-engagement infrastructure to elevate and enhance the Department's counter-CSEA capabilities. DHS remains steadfast in advancing and leveraging its full breadth of authorities and resources to end these heinous crimes, and we urge you to support our efforts to expand our work to fight all forms of human trafficking and child sexual abuse.

Chemical, Biological, Radiological, Nuclear, and Explosives Threats

The overall chemical, biological, radiological, nuclear and explosives (CBRNE) related threat environment in the homeland will likely remain unpredictable over the next 12 months. Terrorists remain interested in acquiring and using WMD in attacks against U.S. interests and the U.S. homeland. Separately, factors including the spread of dual-use CBRNE related technologies, materials, environmental change, advances in computer and related technology that lower technical barriers, and global expansion in the number and sophistication of biological laboratories will likely continue to influence threat trends in the coming years, especially the proliferation of CBRNE threats by non-state actors.

The United States assesses that Russia maintains an offensive biological weapons program and that other potential state adversaries engage in activities that raise concerns regarding compliance with the Biological Weapons Convention. Having seen the human and economic devastation resulting from the COVID-19 pandemic, our adversaries are more aware of the significance of biological threats. Additionally, a global desire to mitigate the consequences of future pandemics is likely to expand global interest in leveraging and advancing biological technology capabilities, including technologies used for biosafety and biosecurity. The dual-use nature of these capabilities complicates the ability to discern civil medical research from malign biological weapons development and heightens the risks of accidental release of biological hazards due to lacking biosafety and biosecurity.

DHS continues to monitor chemical-related threats, including the development and use of chemical weapons and the potential for non-state actors, lone actors, and criminals to pursue a range of chemical substances to use domestically. The use of chemical agents by Russia and North Korea in targeted attacks outside their borders in recent years reaffirms our commitment to monitor for and defend against similar attempts in the homeland. Similarly, chemical accidents of varying severity remain common and of enduring concern. Over time, these trends could manifest as an increased domestic threat.

Traditional radiological and nuclear threats to the homeland remain low. Due to material security and other factors, the likelihood of a large-scale radiological attack in the homeland is very low. Nevertheless, we cannot rule out the risk of unsecured or vulnerable fissile and other source materials in the United States. While the United States has expressed concern with Russian nuclear saber-rattling, we do NOT anticipate that a nuclear detonation in Europe would have any direct health consequences on the homeland.

The Countering Weapons of Mass Destruction Office (CWMD) leads the Department's efforts to safeguard the United States against CBRNE threats by collecting and analyzing CBRNE threat data, conducting risk analysis, and enhancing and implementing capabilities to prevent, detect, prepare for, and respond to the range of CBRNE incidents. This includes collaborating with federal entities to monitor biological threats in cities across the country, providing radiological and nuclear detection equipment to SLTTC partners in urban areas, providing surge support to protect special events, and equipping DHS operational components with radiological and nuclear detection equipment to prevent smuggling at the border. Additionally, CWMD works closely with campus jurisdictions to enhance their capabilities to address these threats and ensure a coordinated, national response.

The Office of Health Security (OHS) promotes a unified approach through partnerships that protect the health of our workforce and the health security of the homeland. In the face of an ever-expanding and complex national health security mission, OHS enhances integration of federal and SLTTC public safety and health security partners, leads the Department's engagements related to medical countermeasures prioritization and policy development, and coordinates food, agriculture, and veterinary defense activities. Recent domestic and global threats such as pandemics, supply chain disruptions, resurgence of zoonotic and transboundary diseases, climate change impacts, and cybersecurity incidents all underscore the important nexus between agro-defense, food protection, and food security with the national security, national economic security, and national public health and safety of the United States.

Extreme Weather Events and Climate Change Resilience

The impacts of climate change pose an acute and systemic threat to the safety, security, and prosperity of the United States, and have already led to changes in the environment, such as rising ocean temperatures, shrinking sea ice, rising sea levels, and ocean acidification. As our climate continues to warm, the United States will experience more climate-related disasters such as heat waves, droughts, wildfires, coastal storms, and inland flooding. This year, we have already seen the devastating impacts from Hurricane Fiona in Puerto Rico and Hurricane Ian in Florida, and Typhoon Merbok in Alaska. Natural disasters occur both seasonally and without warning, subjecting affected communities to insecurity, disruption, and economic loss. Natural disasters include all types of severe weather that have the potential to pose a significant threat to human health and safety, property, and critical infrastructure.

Preparedness and Resilience

Under the Biden-Harris Administration, DHS is engaged in climate change adaptation and mitigation efforts to make the Department and the nation more prepared, more secure, and more resilient:

- In 2021, DHS established a Climate Change Action Group (CCAG) to coordinate DHS response to climate-related Executive Orders and track implementation of actions and progress towards DHS climate change priorities. During the first year, the group was critical in coordinating a Strategic Framework to Address Climate Change and hold the first Department-wide exercise on extreme heat.
- DHS is leading the charge among federal agencies to transition its fleet vehicles from internal combustion engines to zero-emission electric vehicles and is the first federal agency to upfit a battery electric vehicle for law enforcement use. As the Nation's third largest federal agency and largest law enforcement agency, DHS has an inventory of more than 50,000 vehicles, with law enforcement vehicles making up 60 percent of its fleet.
- DHS made available more than $3 billion for the FY 2022 Building Resilient Infrastructure and Communities (BRIC) and Flood Mitigation Assistance (FMA) grant programs which seek to help SLTT governments address high-level future risks to natural disasters such as extreme heat, wildfires, drought, hurricanes, earthquakes, and increased flooding to foster greater community resilience and reduce disaster suffering.
- FEMA continues to evolve mitigation grant programs to be more equitable, reduce complexity, and address climate resilience. FEMA is focused on reducing barriers to access funding faced by those who need it the most and building capacity and capability to deliver mitigation grant programs.
- FEMA announced the expansion of BRIC non-financial Direct Technical Assistance (DTA), increasing the number of communities receiving this community resilience planning and project development assistance from 20 in FY 2021 to 40 in FY 2022, to help communities design transformational projects that address multiple hazards and accelerate community resilience.
- FEMA has also developed a Nature-Based Solutions Guide to help communities identify and engage the staff and resources that can be used to implement nature-based solutions to build resilience to natural hazards, which may be exacerbated by climate change. Nature-based solutions can help reduce the loss of life and property resulting from some of our nation's most common natural hazards. These include flooding, storm surge, drought, and landslides. As future conditions, like climate change, intensify these hazards, nature-based solutions can help communities adapt and thrive.

Nation State Threats

The United States faces an evolving and increasingly complex threat from nation-state adversaries, including the PRC, Russia, Iran, and North Korea, each of which views the United States as a strategic adversary. These adversaries employ a combination of traditional and non-traditional intelligence tradecraft, predatory economic and cultural outreach, and cyber and traditional espionage to seek illicit access to U.S. critical infrastructure and steal sensitive information, technology, and industrial secrets. These governments—and a growing number of others who are learning from their tactics—conduct overt and covert influence campaigns

spreading misinformation and disinformation to sow and exploit divisions in our society, undermine confidence in our democratic institutions, and weaken our alliances. In some cases, they surveil, harass, and otherwise seek to suppress perceived dissidents and regime opponents overseas, including those now living in the United States.

The global availability of technologies with intelligence applications—such as biometric devices, unmanned systems, high resolution imagery, enhanced technical surveillance equipment, advanced encryption, and big data analytics—and the unauthorized disclosure of cyber tools have enabled a wider range of actors to obtain sophisticated intelligence capabilities. Threat actors are using these capabilities against an expanded set of targets and vulnerabilities. Foreign Intelligence Entities are targeting most U.S. government departments and agencies, to include DHS, as well as national laboratories, the financial sector, the U.S. industrial base, and other private sector and academic entities. These activities put at risk the homeland security enterprise, as well as state and local partners, and private sector critical infrastructure providers.

We assess that the PRC will continue to exploit professors, scholars, and students visiting the United States from the PRC as nontraditional collectors to steal sensitive information and technology. Some collectors are unwittingly providing information back to the PRC, while others are aware of their roles and have admitted to stealing research from U.S. institutions to support Chinese military ambitions. We expect the threat from these actors will increase as international students return to U.S. universities after a hiatus due to the COVID-19 pandemic.

Russia embeds intelligence officers in its diplomatic posts inside the United States. While in the U.S., Russia's intelligence officers try to establish front companies and recruit Russian emigres and American citizens to steal sensitive U.S. academic, government, and business information. Russia continues to circumvent U.S.-imposed sanctions to acquire sensitive/dual-use technology for use in military weapons and aviation industry.

We assess that for the foreseeable future, Iran probably will present an enduring counterintelligence threat to the homeland as it seeks to advance its goals in the Middle East. During 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.

Election Security

The security and resilience of our nation's election infrastructure is one of the highest priorities for DHS. As demonstrated in recent election cycles, we continue to face a wide range of threats targeting U.S. election infrastructure and voters by sophisticated, state-sponsored cyber threat actors, such as the PRC, Russia, and Iran. In many cases, the foreign threat actors who are attempting to breach our election systems are the very same ones who are conducting influence operations that seek to sow discord in our country. Their influence operations often utilize information obtained illicitly through cyber activity, or they make false or exaggerated claims of cybersecurity breaches. These foreign threat actors advance their own disinformation narratives about U.S. elections, as well as amplify existing domestic disinformation narratives. Protecting election infrastructure is a whole-of-government effort. DHS works closely with the

U.S. Election Assistance Commission (EAC), DOJ, the intelligence community, and other agencies to help accomplish this goal.

Throughout the 2022 primary and general elections, DHS has worked to ensure that election officials and their private sector partners have the necessary information and tools to successfully manage risk and build resilience into the nation's election infrastructure. DHS works to protect and safeguard elections by:

- Sharing Intelligence and Information: DHS shares timely and actionable intelligence and information with our federal, state, local, tribal, and territorial government and private sector partners about threats and risks to election infrastructure, including foreign disinformation efforts concerning elections.
- Providing Services and Resources: CISA maintains an Election Security Resource Library to equip state and local governments, election officials, and others with no-cost tools they can use to secure election-related assets, facilities, networks, and systems from cyber and physical risks. This includes Cybersecurity Advisors located throughout the country and more than 100 Protective Security Advisors in all 50 states who provide cybersecurity expertise, conduct physical security assessments, and share guidance and best practices. Through 2022, CISA facilitated multiple classified and unclassified threat briefings, engaged thousands of election officials and SLTT partners for cybersecurity and physical security services, assessments, trainings, and tabletop exercises, including CISA's 2022 Tabletop the Vote exercise, a three-day exercise that engaged over 1,000 stakeholders across 40 states. CISA also provides funding to the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), which now includes all 50 states and more than 3,400 local jurisdictions. This is the main mechanism for sharing alerts with the election's community. DHS also provides funding for enhancing election security through FEMA grants.
- Combating Disinformation Around Elections: State, local, tribal, and territorial officials are the most trusted sources of election information in communities across our nation: DHS partners with them to help ensure that voters receive accurate information. DHS assists with addressing disinformation by being transparent about identified foreign malign influence campaigns, amplifying facts shared by state, local, tribal, and territorial officials with the public, and encouraging individuals to maintain digital and media literacy to recognize and build resilience.

Conclusion

While DHS was created in response to a singular threat, in the two decades since 9/11 the Department has evolved to address multiple unforeseen 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 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.