



The Third Quadrennial Homeland Security Review

April 2023



Homeland
Security

This page intentionally left blank

Secretary

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

April 2023

The Quadrennial Homeland Security Review (QHSR) comes at a critical time as the U.S. Department of Homeland Security (DHS or the Department) enters its third decade. As President Biden noted in his 2022 *National Security Strategy*, the world is at an inflection point, and the United States must seize this decisive decade to advance America's interests and achieve a better future of a free, open, secure, and prosperous world.

The world today is more interconnected than at any time in our Department's 20-year history. Ubiquitous cutting-edge technologies and our globalized economy have enabled tremendous economic progress and advancements for Americans; they also increasingly bring threats and challenges directly into our communities—to our schools, hospitals, small businesses, local governments, and critical infrastructure. Those who wish to harm us exploit the openness that defines our modern world. They do so through economic and political instability, through illicit trade and investment flows, through the exploitation of rapidly evolving technologies that connect us, and through disinformation spread around the world by the click of a mouse. "Homeland Security" as we thought of it in the wake of 9/11—safeguarding the United States against foreign terrorism—today has new meaning. Our homeland security has converged with our broader national security in ways we did not predict 20 years ago.

The lessons learned in the aftermath of the devastating attacks of September 11, 2001, now help us safeguard the American people amidst a transformed threat environment. One of those lessons is the importance of partnership. Thanks to the work of this Department during the past two decades, the Federal Government is more coordinated than ever in the way we prepare for, prevent, mitigate, respond to, and recover from the many new threats we face. DHS facilitates the sharing of threat information and intelligence between and among our federal partners, our state, local, tribal, and territorial partners, law enforcement agencies, and the private sector. These efforts significantly reduce the risk of terrorist attacks against the homeland and are also helping us prevent and mitigate a range of evolving threats.

The Department has matured, unifying eight Operational Components and 15 Offices, streamlining and improving the execution of the myriad responsibilities across them and enabling effective joint operations such as Joint Task Force Alpha, Operation Allies Welcome, the Southwest Border Coordination Center, and more. DHS has led the way in innovation, including in public-private partnerships, such as with the Joint Cyber Defense Collaborative; in deploying new technologies, including biometric technology with privacy protections to ease

the travel experience; in protecting against the use of new technologies to cause harm, such as our leadership in countering unmanned aerial systems threats; and much more. DHS has also demonstrated it can evolve quickly to address emerging threats, as shown when we met the challenges of the COVID-19 pandemic with a national mass vaccination campaign and the establishment of the Office of Health Security.

This Report reaffirms the five enduring homeland security missions as articulated in the first two QHSR Reports issued in 2010 and 2014 and focuses on how the Department must adapt and evolve to accomplish them. It also introduces a new homeland security mission, *Combating Crimes of Exploitation and Protecting Victims*, reflecting the overriding urgency of supporting victims and stopping perpetrators of such heinous crimes as human trafficking, labor exploitation, and child exploitation, the importance of engaging the public, and the heroic work of the DHS workforce and our homeland security enterprise partners in this mission space. DHS investigates crimes of exploitation, supports victims, trains law enforcement partners, and enforces trade laws related to human trafficking, and we will continue to advocate for additional resources to execute on these lines of effort at an ever-increasing level. U.S. Immigration and Customs Enforcement initiated more than 6,000 child exploitation cases and U.S. Customs and Border Protection seized 3,605 shipments valued at \$816.5 million due to forced labor concerns in fiscal year 2022. By elevating this work as a new mission, we are laying the groundwork for further growth in our commitment and capabilities, including planning, increased budget requests, operational cohesion, and partnerships.

This maturation of the Department and its ability to work with our partners has made it more fit for purpose to address the most significant threats facing the homeland as they have evolved than at any point in our 20-year history. Today, the most significant terrorist threat stems from lone offenders and small groups of individuals, especially domestic violent extremists, while the threat of international terrorism remains as foreign terrorist organizations have proven adaptable and resilient over the past two decades and individuals inspired by their ideologies have continued to launch attacks in their names. The capabilities DHS brings to bear across its workforce to counter terrorist threats allows it to support law enforcement agencies and communities with a wide range of resources to prevent and protect against terrorism and targeted violence. In the cyber domain, DHS has acted with unprecedented unity of purpose to meet the proliferating threats to our nation's networks. Complex challenges further strain our immigration system, and we have enforced the nation's immigration laws while making reforms and improvements to build a safe, orderly, and humane immigration system. Crimes of exploitation, including human trafficking, labor exploitation, and child exploitation, are occurring at alarmingly high rates. Transnational criminal organizations continue to threaten the security of the homeland through human smuggling and trafficking, illicit narcotics smuggling, and other illegal activities. This is particularly true when it comes to fentanyl, the vast majority of which is smuggled through U.S. ports of entry. In fiscal year 2022, DHS seized more than 1.8 million pounds of narcotics and 14,700 pounds of fentanyl. In March

2023, Operation Blue Lotus, a new coordinated and surge operation targeting the smuggling of fentanyl, stopped more than 900 pounds of fentanyl from coming into the United States in its first week, and the President's Budget for fiscal year 2024 makes significant investments critical to detecting fentanyl at ports of entry.

We face more serious threats from nation states now than at any time in the Department's history. DHS is bringing together its authorities and capabilities across Operational Components to counter those threats, including enforcing U.S. trade laws banning the importation of goods made, wholly or in part, with forced labor, strengthening maritime governance, and increasing awareness of nation state threats with our federal, state, local, tribal, territorial, and private sector partners.

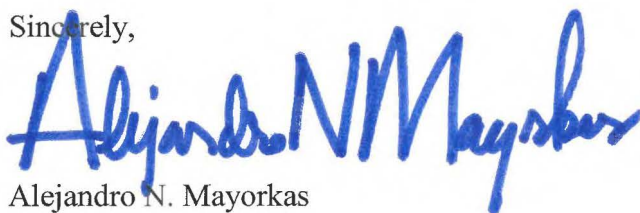
The nation also faces threats from the impacts of climate change causing more frequent and severe weather events, and from emerging infectious diseases. These threats disrupt the lives of millions of Americans as well as our economic prosperity, and DHS agencies like the Federal Emergency Management Agency—which, in 2022, helped more than 100,000 disaster survivors receive \$559 million in additional federal assistance—are on the front lines to prevent and respond to threats to the American people. Moreover, the types of challenges to which DHS responds have broadened, increasingly calling the varied and unique capabilities of our Operational Components into action. Personnel from across DHS sprang into action to lead these responses, including welcoming more than 88,000 vetted Afghan nationals to the United States, leading the preparation for potential risks to the homeland from Russia's unjust invasion of Ukraine, and coordinating various legal pathways for 270,000 displaced Ukrainian citizens to come to our country.

Our homeland security and national security are inextricably linked. We may not have envisioned the complexity and dynamism of today's threat environment when the Department was established 20 years ago, but it is clear we have never been more fit for the mission before us.

Addressing the threats of today and tomorrow requires all of us working together across federal, state, and local governments, the private sector, nonprofits, academia, and indeed, the involvement of every individual. The need for DHS's capabilities and tools will only continue to grow as we confront the threats of tomorrow.

This is the decisive decade. As we move forward in the ways described in this Review, we will accomplish the mission.

Sincerely,



Alejandro N. Mayorkas
Secretary

This page intentionally left blank

TABLE OF CONTENTS

The Purpose of the Third Quadrennial Homeland Security Review.....	1
Evolving Challenges for Homeland Security Missions.....	5
Dynamic Terrorist Threats.....	5
Increasing Complexity Further Straining the Immigration System.....	12
Crimes of Exploitation	20
Transnational Organized Crime.....	27
Proliferating Cyber Threats.....	30
Strategic Competition.....	38
Climate Change.....	43
Emerging Infectious Diseases.....	47
Complex and Interconnected Incidents.....	52
Strengthening the Enterprise.....	57
Emerging Technology.....	57
Building the Department’s Capacity.....	64
Conclusion.....	71
Appendix A: Legal Requirement for the Review and Report.....	73
Appendix B: Organizational Alignment of the Department with Homeland Security Strategic Priorities and Mission Areas.....	75
Appendix C: Process.....	81
Endnotes.....	83

The Purpose of the Third Quadrennial Homeland Security Review

*With honor and integrity, we will safeguard the American people,
our homeland, and our values.*

More than two decades after 9/11, countering terrorist threats to the American people remains an enduring U.S. Department of Homeland Security (DHS or the Department) mission; what's more, we are living in an increasingly dynamic and complex environment. As DHS enters its third decade of operation, the Department and the homeland security enterprise¹ must evolve to stay ahead of the challenges and threats of the next 20 years and beyond. What those will be, and how the Department will position itself to succeed in

carrying out its missions over the next four years, are the central subjects of this Report.

The first Quadrennial Homeland Security Review (QHSR) Report in 2010 defined the core homeland security missions and the nature of the homeland security enterprise. It connotes the collective efforts and shared responsibilities of federal, state, local, tribal, territorial, nongovernmental, and private-sector partners—as well as individuals, families, and communities—to maintain critical homeland



A New Homeland Security Mission

The 2010 QHSR identified the five homeland security missions that have endured and guided the Department's maturation and growth. These missions were reaffirmed in the 2014 QHSR and, with modifications to recognize the evolving threat environment, are reaffirmed again here in the Third QHSR. In addition, in light of the prevalence and severity of crimes of exploitation—including human trafficking, labor exploitation, and child exploitation—DHS has enhanced its efforts to combat these heinous crimes.² This prioritization is reflected in their inclusion in the Department's 2022 and 2023 priorities, Departmental budget requests for fiscal years 2023 and 2024, and now the Third QHSR where this work is recognized as a full mission of the Department. This is the first time the mission to *Combat Crimes of Exploitation and Protect Victims* has been included as a homeland security mission in the QHSR.

This step reflects the overriding importance of supporting victims and stopping perpetrators, as well as the heroic work of the DHS workforce and our partners in the homeland security enterprise. Every day they work to investigate, apprehend, and prosecute offenders, and to identify, protect, and support victims. DHS works to raise awareness of these threats and provides training to those who may encounter victims of human trafficking and other crimes of exploitation. This work will continue to grow and its identification as a full mission of the Department lays the groundwork for necessary enhancements, including planning, increased budget requests, operational cohesion, and partnerships.

security capabilities. These collective efforts remain at the heart of homeland security today. The second QHSR Report in 2014 applied analytic rigor to refine the five missions from the 2010 Report and identify five strategic priorities. This Report reaffirms the five enduring homeland security missions articulated in the first two QHSR Reports and focuses on how the Department must adapt and evolve to accomplish them in a changing environment. This Report also recognizes significant changes in the strategic environment by evolving the five enduring missions and by identifying a new mission for the first time since 2010 (Fig. 1). The Department has grown its

capabilities over many years to combat crimes of exploitation, including human trafficking, labor exploitation, and child exploitation. Now, for the first time, it is a core mission of the Department recognized in a QHSR. The new mission, *Combat Crimes of Exploitation and Protect Victims*, will provide the basis for the necessary enhancements to combat these pernicious crimes. Overall, this strategic guidance and updated mission framework will inform existing Departmental processes for translating priorities into resources, including the *DHS Strategic Plan* and the annual budget development process.

Threats to the homeland have become more complex and have arisen on new fronts. Challenges to securing the homeland are increasingly cross-cutting, often requiring more frequent coordination across the homeland security enterprise. The convergence of cyber-physical technologies and systems underpinning our critical functions—from manufacturing, to healthcare, to transportation—means that single events can have a cascading impact on multiple industries, sectors, and National Critical Functions.³

The Colonial Pipeline incident in May 2021, which started as a ransomware attack, quickly had cascading supply chain impacts—most notably to the distribution of gasoline and jet fuel to the Eastern United States—becoming a logistics problem more often experienced in



response to natural disasters. The migration surges at the Southwest Border during the COVID-19 pandemic presented both immigration and public health challenges that needed to be addressed through partnerships among multiple federal agencies, state and local governments, nongovernmental organizations (NGOs), and international organizations. The resettlement of tens of thousands of Afghan allies in the United States through Operation Allies Welcome (OAW), which DHS led for the nation, required combined capabilities across the Department and with our federal partners—including screening and vetting, health security, and resettlement—and challenged existing governmental structures. The February 2022 Russian cyberattack on Viasat, a satellite communications provider, had real-world reverberations across Europe, including impacting the functionality of wind turbines in Germany and critical infrastructure systems in numerous sectors and countries. Increasingly, these types of intersecting challenges will define the threat landscape the homeland security enterprise will face over the next 20 years, and it is these challenges to which the Department must adapt in the coming years.

The five enduring homeland security missions, together with the new sixth mission, are essential national missions and DHS and its homeland security enterprise partners are proud to work every day to achieve them. On any given day, this can include the

Partnerships

DHS is fundamentally a Department of partnerships. Our success depends on the strength of these partnerships as we cannot accomplish our missions alone. We pursue mutually beneficial partnerships across many sectors: foreign governments; international organizations; federal agencies; state, local, tribal, territorial, and campus officials and law enforcement organizations; private industry; academia; civic organizations; and NGOs and the communities they represent, including faith-based organizations. DHS interfaces with these entities daily, relying on their counsel and expertise, communicating departmental priorities and initiatives in real time, and accessing new technologies and ideas.

Since January 2021, DHS has created new partnerships to enhance the ability of the Department and the homeland security enterprise to tackle critical challenges. DHS launched the Joint Cyber Defense Collaborative (JCDC) to enable the Federal Government and major private sector information technology (IT) providers to share sensitive information in real time to secure critical networks. In September 2022, DHS, through CISA, kicked off the Joint Ransomware Task Force (JRTF) in partnership with the Federal Bureau of Investigation (FBI) to coordinate an ongoing nationwide campaign against ransomware attacks. DHS launched the “Hack DHS” bug bounty program in partnership with the independent cybersecurity researcher/ethical hacker community to increase the Department’s cybersecurity resilience. On the Southwest Border, DHS has partnered with state and local governments, law enforcement organizations, international NGOs, and non-profits to conduct border management, immigration processing, and resettlement operations. Under OAW, DHS worked with federal partners, including the Department of Defense, Department of State, and Department of Health and Human Services (HHS), as well as state and local governments, law enforcement, and resettlement organizations to carry out this unique effort (more information on OAW is included on page 53).

DHS developed these programs and initiatives in collaboration with our partners. We work to build trust through constant and forthright communication, both to receive input into policy development and to get feedback on policy implementation. When information is shared, it must be actionable and incorporate feedback loops to ensure all parties understand how recipients acted upon the information. With shared information and clarity of purpose, DHS will continue to build trusted and enduring collaborations with our partners.

DHS will develop and institutionalize best practices for partnering with outside organizations, taking advantage of existing federal guidance. We will develop a toolkit and training for staff across the Department on how to engage and build relationships with external organizations and identify opportunities to leverage external resources. DHS will remain focused on strengthening its partnerships across every level of government, the private sector, and the diverse communities we serve to secure the homeland while upholding our values.

Cybersecurity and Infrastructure Security Agency (CISA) partnering with Sector Risk Management Agencies (SRMAs) to enable the prevention or disruption of a ransomware attack against critical infrastructure and enhance the security and resilience of soft targets from terrorist threats, the Federal Emergency Management Agency (FEMA) delivering assistance to communities recovering from a devastating natural disaster or other incident, the U.S. Secret Service (USSS) partnering with state and local law enforcement to investigate cyber-enabled financial crimes, U.S. Immigration and Customs Enforcement (ICE) investigating cross-border crime to include human smuggling, U.S. Customs and Border Protection (CBP) screening people and cargo crossing our borders, U.S. Citizenship and Immigration Services (USCIS) removing obstacles to our nation's legal immigration pathways, the Transportation Security Administration (TSA) screening airline passengers to ensure their security, and the U.S. Coast Guard (USCG) rescuing individuals in distress from rough seas and protecting fisheries and waterways. These represent just a snapshot of the work that over 260,000 employees of DHS, together with our homeland security enterprise partners, do every day to keep the homeland safe and secure.

Continuing our essential work means looking into the future and preparing the Department and the homeland security enterprise for what lies ahead. Longstanding imperatives to counter terrorist threats, secure cyber networks,

administer the immigration system, and secure our borders have seen changes in the nature of the threats and challenges involved. We also live in an era of strategic competition, with nation states threatening the homeland in unprecedented ways. Infectious diseases, hardware and software vulnerabilities, supply chain insecurity, and climate change have all caused global disruptions, giving new impetus to building resilience to all hazards and developing new approaches to prepare, prevent, protect, mitigate, and respond if necessary. Rapidly developing emerging technologies also underpin the contemporary world in which we operate, further changing how we accomplish our missions and the nature of the threats we face.

Addressing this dynamic landscape will require a workforce that is strengthened; capabilities that are adaptable; technology and data systems that are interoperable; facilities that are secure and resilient; public-private partnerships that are empowered; and the data to operate with science, transparency, and accountability at the fore. The entire homeland security enterprise must work together in innovative ways to face new challenges as part of a coordinated and integrated approach to achieve critical homeland security objectives on behalf of the nation.

Figure 1: Homeland Security Missions and Objectives

Mission 1: Counter Terrorism and Prevent Threats
1.1 Collect, Analyze, and Share Actionable Intelligence and Information
1.2 Prevent and Disrupt Terrorist and Nation State Threats
1.3 Protect Leaders and Designated Individuals, Facilities, and Events
1.4 Identify and Counter Emerging and Chemical, Biological, Radiological, and Nuclear Threats
Mission 2: Secure and Manage Our Borders
2.1 Secure and Manage Air, Land, and Maritime Borders
2.2 Expedite Lawful Trade and Travel
2.3 Counter Transnational Criminal Organizations and Other Illicit Actors
Mission 3: Administer the Nation's Immigration System
3.1 Administer the Immigration System
3.2 Enforce U.S. Immigration Laws
Mission 4: Secure Cyberspace and Critical Infrastructure
4.1 Support the Cybersecurity of Federal Civilian Networks
4.2 Strengthen the Security and Resilience of Critical Infrastructure
4.3 Assess and Counter Evolving Cyber and Emerging Technology Risks
4.4 Combat Cybercrime
Mission 5: Build a Resilient Nation and Respond to Incidents
5.1 Coordinate Federal Response to Incidents
5.2 Strengthen National Resilience
5.3 Support Equitable Community Recovery
5.4 Enhance Training and Readiness of First Responders
Mission 6: Combat Crimes of Exploitation and Protect Victims
6.1 Enhance Prevention through Public Education and Training
6.2 Identify, Protect, and Support Victims
6.3 Detect, Apprehend, and Disrupt Perpetrators
Enable Mission Success by Strengthening the Enterprise
E.1 Mature Organizational Governance
E.2 Champion the Workforce
E.3 Harness Data and Technology to Advance Mission Delivery

Evolving Challenges for Homeland Security Missions

Founded in the aftermath of the September 11th attacks, DHS holds the enduring mission of countering terrorist threats to the homeland. In the twenty years since, terrorist threats have diversified, cyber threats have proliferated, and increasing complexities place the nation's outdated immigration system under greater strain. Crimes of exploitation, including human trafficking, labor exploitation, and child exploitation, occur at alarmingly high rates. We also now live in an era of strategic competition, as well as increasing impacts from climate change, risks from emerging infectious diseases, and the continuing threat of transnational organized crime. Threats and challenges to the security of the homeland continue to evolve in ways that require a refreshed understanding and, accordingly, shifts in approach to ensure the homeland security enterprise can continue accomplishing its enduring missions.

Dynamic Terrorist Threats

Despite significant progress and a diminished terrorist threat to the United States, the country continues to face a diversified and dynamic threat environment from a broad array of actors. We must remain vigilant against all forms of terrorism, both domestic and international. Today, the most significant domestic terrorist threat facing the homeland stems from lone offenders and small groups of individuals. They are motivated by a broad range of racial, ethnic, political, religious, anti-government, societal, or personal ideological beliefs and grievances—often exacerbated by conspiracy theories and false and misleading narratives spread online. 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.

Of these actors, domestic violent extremists (DVEs)—individuals who are based and operating primarily within the United States seeking to further political goals or address perceived grievances through unlawful acts of force or violence, without direction or inspiration from a foreign terrorist group or other foreign power—represent one of the most persistent and lethal threats facing our nation. DVEs are motivated by a range of ideologies and are galvanized by political and societal events in the

United States. As such, DHS, along with its partners, must continue to adapt and innovate to protect the American people and U.S. vital interests.

To counter domestic terrorist threats, DHS, working closely with interagency partners, will continue to align its mission to the core pillars of the first *National Strategy for Countering Domestic Terrorism*⁴: (1) understanding and sharing domestic terrorism-related information; (2) preventing domestic terrorist recruitment and mobilization to violence; (3) disrupting and deterring domestic terrorism activity; and (4) confronting long-term contributors to domestic terrorism. This begins with increasing our prevention efforts. DHS established the Center for Prevention Programs and Partnerships (CP3) in 2021 and is expanding the Department's

ability to prevent targeted violence and terrorism at the local level. CP3 works to build a safer America where communities come together to prevent targeted violence and terrorism by providing individuals and organizations with funding, training, increased public awareness, and the development of partnerships across every level of government, the private sector, and in local communities across our country. In fiscal year 2022, CP3 awarded \$20 million in grants to 43 organizations through its Targeted Violence and Terrorism Prevention (TVTP) Grant Program. Through CP3, our approach to targeted violence and terrorism prevention draws lessons from other forms of prevention, such as suicide prevention and domestic violence prevention, with the focus on health and well-being.

The DVE Threat

DHS assesses that racially or ethnically motivated violent extremists (RMVEs) and militia violent extremists (MVEs) present the greatest DVE threats, with RMVEs being the most persistent and lethal threats to conduct mass-casualty attacks against civilians, and MVEs typically targeting law enforcement and government personnel and facilities. We have also seen examples of both RMVEs and MVEs targeting critical infrastructure, including recently against the electric sector, among others.

RMVEs and MVEs are the primary DVE concern, given the lethality of the threat and incident data. While specific motives vary, many attackers share common behavioral characteristics and often connect with a grievance to justify their use of violence.

RMVEs and anti-authority/anti-government violent extremists are inspired by various violent extremist ideologies or perceived personal grievances, often cultivated through the consumption of online content or motivated by conspiracy theories. This results in many DVEs with hybrid ideological beliefs that do not fit into traditional categories.

DHS will implement additional prevention efforts, including through the USSS National Threat Assessment Center, which leads the field of threat assessment and targeted violence prevention, and through increasing capabilities to plan and implement security operations for National Special Security Events (NSSEs) and secure facilities and venues where our nation's leaders conduct business. These efforts are especially important given the DVE threat and an unprecedented number of NSSEs expected to occur between 2024 and 2028.

DHS will continue to enhance information sharing with partners, including state, local, tribal, and territorial (SLTT) officials, as well as civil society and the private sector. In 2021, DHS created a dedicated domestic terrorism unit within the Office of Intelligence and Analysis (I&A) to improve its capability to focus on and address threats posed by DVEs. The Department also will continue to collaborate with homeland security advisors in every state and territory, the national network of fusion centers, and other field-based information sharing partners to share timely and actionable information to enable our partners to keep their communities safe. Additionally, DHS will continue to identify opportunities to empower SLTT partners, the private sector, the public, and civil society to address this national threat effectively. Recent examples of our commitment to empower our partners include the DHS-supported Intelligence Summit to improve information sharing, as well as the

Secretary's designation, for the first time, of DVE as a National Priority Area within the Department's Homeland Security Grant Program and increasing the amount granted under the fiscal year 2021 TVTP Grant Program to \$20 million.

Since 2021, DHS has convened engagements regularly to inform our partners about the threat environment, including biweekly calls with state and local law enforcement and national-level calls with a broad group of stakeholders on emerging threats. These engagements have ranged from dozens to thousands of participants on national-level outreach efforts. DHS also has issued more than 100 intelligence products related to domestic violent extremism since 2021, including seven National Terrorism Advisory System bulletins, to inform the public about the latest terrorism-related threats to the homeland. The Department will continue to use this tool, among others, to raise public awareness, enhance security, and build resilience.

DHS also prioritizes the homeland security threats that disproportionately impact communities of color and communities of faith. Domestic violent extremism has long threatened communities of color and continues to do so, and those same communities are disproportionately targeted by foreign malign influence operations. The homeland security enterprise can work towards equitable



outcomes by prioritizing efforts to counter these threats—including the Nonprofit Security Grant Program that provides resources to protect nonprofits from threats of violence—with particular focus on how they impact these communities. Beginning in February 2022, the Department began efforts to build new and strengthen existing partnerships with campus law enforcement in response to the drastic increase in bomb threats at Historically Black Colleges and Universities and other institutions of higher learning. The Department has also convened the multi-denominational Faith-Based Security Advisory Council, comprised of faith leaders and other experts from across the country, to advise and work with the Department on strategies to prevent, respond to, and build resilience to violence borne of antisemitism and other ideologies of hate.

The threat of international terrorism to the homeland remains, as foreign terrorist organizations have proven adaptable and resilient over the past two decades and individuals inspired by their ideologies—homegrown violent extremists (HVEs)—have continued to launch attacks in their names. Within the United States, the threat from HVEs is likely to remain the most prominent form of international terrorism facing the homeland. However, emerging threats from foreign terrorist organizations are expected to evolve. While Al-Qa’ida and the Islamic State of Iraq and ash-Sham (ISIS) have been diminished by longstanding U.S. counterterrorism activities, their networks and affiliates have diffused and persisted, often in areas of or nearby enduring conflict or those lacking effective governance, such as Syria, Yemen, Somalia, Libya, other parts of Africa, Afghanistan, and Pakistan.

These groups and their supporters have also adeptly used online media and content generation to inspire attacks in the U.S. homeland and elsewhere. We must remain vigilant against the possible reemergence of terrorist safe havens abroad for training and plotting attacks and potential efforts by foreign terrorist organizations to exploit weak immigration laws in some countries in the Western Hemisphere. In the years since September 11, 2001, DHS has enhanced our nation's ability to identify and prevent individuals affiliated with these organizations from traveling to or entering the United States to conduct attacks. However, terrorists have and will continue to adapt to changing security environments and seek new and innovative ways to target the homeland.

The nation's success in protecting the homeland from international terrorism has been enabled, in part, by U.S. counterterrorism operations to detect, deter, and disrupt the terrorist threat as far away from U.S. borders as possible. DHS will utilize and expand its strong international partnerships to increase information sharing, including of criminal and terrorism-related information, both biometric and biographic, on all threat actors as well as providing critical training and equipment to bolster the counterterrorism capabilities of our allies and partners. DHS will continue to use and enhance its multi-layered screening and vetting architecture and enable identity technologies to prevent terrorists from traveling

to our country. DHS will also encourage interagency partners to work together to expand on the existing U.S. Government-wide screening and vetting architecture to tackle the threats facing our nation today and in the coming years. We will work with the Intelligence Community and law enforcement to prioritize collection that supports this mission.

Although terrorist capabilities to conduct large-scale attacks have been degraded by U.S. counterterrorism operations and policies, terrorists remain interested in acquiring and using weapons of mass destruction (WMD) in attacks against U.S. interests and the homeland. DHS will continue its efforts to secure the homeland from the enduring threat of terrorist use and proliferation of WMD which poses profound and, in some cases, existential dangers to the United States. This threat continues to evolve due to advances in science and technology and as dual-use knowledge, goods, materials, and technology applicable to WMD continue to proliferate. The Countering Weapons of Mass Destruction Office will continue to provide equipment, expertise, and training in close coordination with and in support of all Operating Components, Offices, and SLTT partners to prevent, detect, and mitigate the impacts of these devastating threats.

Increasing Complexity Further Straining the Immigration System

The United States is a nation of laws and a nation of immigrants. We have a longstanding commitment to welcoming refugees and asylum seekers. Our missions to secure our borders and administer our immigration system with integrity and compassion are complementary, and DHS will continue to work with our partners across the homeland security enterprise to accomplish these missions. DHS continues to confront increasing complexities placing the nation's broken and outdated immigration system under greater strain. DHS will make investments in policy, technology, human capital, and infrastructure to better position our Components to secure our borders, administer immigration processes, enforce our laws, and support matters of public safety and national security concern. These efforts will be designed to manage our borders in a safe, orderly, and humane manner, upholding civil rights, civil liberties, and privacy in ways that embody our nation's highest values.

The root causes that drive migration in Latin America and the Caribbean—including abuses perpetrated by authoritarian regimes in Venezuela, Nicaragua, and Cuba, and food insecurity, violence, corruption, lack of opportunities, and systemic poverty—are longstanding factors which we will continue to address with our interagency and international



partners. The effects of the COVID-19 pandemic and the ravages of climate change-induced natural disasters accelerate these factors and contribute to a surge in migration. Transnational criminal organizations and their affiliates are supporting human smuggling networks that exploit many who seek to make the dangerous journey to our Southwest Border. Many migrants transiting Central America and Mexico believe they have little to no choice but to incur a heavy financial burden to pass through territory controlled by these groups who pose a direct threat to their safety.

The use of technology by smugglers and migrants, including social media, contributes to increasingly dynamic and volatile migration patterns. Human smuggling organizations also leverage these technologies to entice people to make the journey north, often spreading misinformation and disinformation about U.S.

border and immigration policies and putting migrants in harm's way for profit.

Over the past decade, there has been a fundamental change in migratory patterns that has far-reaching impacts for DHS and the broader U.S. immigration system. Until 2013, more than 90 percent of individuals encountered at the border were single adults, and the vast majority were Mexican citizens. In 2014, the United States began experiencing a surge in migration of family units and unaccompanied children, which have accounted for more than half of all encounters since 2018. Unaccompanied children and family units present humanitarian concerns that make having them in custody and conducting initial processing more complex and resource-intensive than processing single adults. In

addition, CBP and ICE are both encountering more diverse demographic profiles than their infrastructure was designed to manage.

The composition of migrant encounters will continue to change, requiring the Department to maintain maximum flexibility in its operations and processing capabilities. Today, DHS is facing a surge in migration from non-traditional sending countries, including Brazilians fleeing the devastation wrought by COVID-19. There have also been surges in Haitians fleeing their home country due to instability, indiscriminate violence, and economic collapse, as well as surges from South American countries, where many have lived for years, due to economic recessions and changes in those countries' immigration policies. Repressive regimes in Cuba, Nicaragua, and Venezuela have fueled

Unaccompanied Children

DHS is addressing the needs of children who arrive at our Southern Border without a parent or legal guardian in the United States available to provide care and physical custody. In March 2021, DHS saw a significant influx of unaccompanied children, which led to overcrowding of CBP facilities. In response, FEMA supported a whole-of-government effort to assist HHS in increasing its capacity to receive and shelter the children, and USCIS personnel served as caseworkers to further support HHS efforts to release the children to vetted sponsors, including verified relatives here in the United States.

The results were dramatic. On March 29, 2021, more than 5,700 children were in Border Patrol facilities, 4,078 of whom were in such facilities for longer than the 72 hours mandated by statute, and the average length of time an unaccompanied child spent in a Border Patrol facility was 133 hours. By May 11, 2021, only 455 children were in Border Patrol facilities, none for more than 72 hours, and the average length of time a child spent in a Border Patrol station was 22 hours. The average amount of time children spend in CBP facilities was further reduced to 19 hours in February 2023.

Uniting for Ukraine

In March 2022, DHS launched Uniting for Ukraine, a process that enables certain Ukrainians, along with their immediate family members, to request advanced authorization to travel to the United States to seek parole at a port of entry. Administered by DHS with support from multiple federal agencies, Uniting for Ukraine provides Ukrainian citizens the safest and most efficient way to pursue temporary refuge in the United States.

Uniting for Ukraine provides a pathway for Ukrainian citizens and their immediate family members to seek authorization to travel to the United States to request parole for a 2-year period with the ability to gain employment. Through this process, Ukrainian citizens are supported by U.S. individuals or entities for the duration of their stay. Uniting for Ukraine builds on the robust humanitarian assistance the U.S. Government is providing and complements the generosity of our international partners that are hosting other Ukrainian citizens and their families. Since March 2022, the U.S. Government has admitted or paroled into the United States through various legal pathways over 270,000 displaced Ukrainians and their immediate family members, including over 115,000 through Uniting for Ukraine.

migration throughout the hemisphere, leading to large diasporas, including millions of Venezuelans who have fled to Brazil, Peru, Ecuador, Colombia, Costa Rica, and elsewhere in South America. These diasporas may lead to much larger migratory flows over the coming years.

To address these trends, DHS has developed and will continue to implement a plan consisting of six key pillars: surging resources; increasing efficiency to reduce strain on the border; administering consequences for unlawful entry; bolstering the capacity of NGOs and working with state and local partners; targeting and disrupting networks of cartels and smugglers; and working with our regional partners to deter irregular migration. DHS will also continue to operate in a coordinated

fashion with federal partners such as HHS to provide medical capabilities and care and facilitate placement of unaccompanied children; with the U.S. Department of Justice's Bureau of Prisons to provide transportation capabilities and the Executive Office for Immigration Review to reduce the immigration court backlog; with the U.S. General Services Administration to provide support for temporary sheltering; and with the U.S. Department of Defense to provide detection and monitoring capabilities and assistance with contracting. While CBP, ICE, and the USCG wield powerful law enforcement authorities on land and at sea, DHS works with other partners across the homeland security enterprise—including SLTT law enforcement agencies—to ensure border security operations are conducted in a safe, humane, and dignified manner.

The management of these migratory flows is a shared responsibility among all countries in the hemisphere, as agreed to in the *Los Angeles Declaration on Migration and Protection*.⁵ DHS will work with our interagency colleagues to engage regional partners to address the root causes of migration and enhance migration management and border enforcement through technical assistance, law enforcement cooperation, and migration agreements and arrangements throughout the Western Hemisphere. DHS will continue to work in close partnership across the Federal Government, including with our partners at the U.S. Agency for International Development (USAID) and Department of State, to help countries in the region enhance protection for migrants, create robust migration management mechanisms, foster economic opportunity, and increase resiliency to the effects of climate change within the region.

DHS will continue to work with the Department of State to expand access to legal pathways for migrants seeking opportunity or protection in the United States, and to help enhance reception and reintegration for returnees to their home countries. In addition, DHS is enabling opportunities for safe and orderly migration through the Central American Minors program, in which lawfully present U.S.-based family members can petition for minors in their home country to be brought safely to the United States. We are also promoting labor pathways, specifically through the H-2A and H-2B

programs, for temporary agricultural and non-agricultural workers, including allocating additional H-2B visas for certain Western Hemisphere countries under a time-limited statutory authority.

DHS will also continue to use its own authorities to establish safe, orderly, and lawful pathways to enter the country. In response to humanitarian crises, DHS has responded with unprecedented action. Following the evacuation of U.S. and allied forces from Afghanistan, DHS led a whole-of-government effort to coordinate the entry, domestic processing, and resettlement of Afghans into the United States. DHS created Uniting for Ukraine to provide Ukrainians with supporters in the United States a pathway to come and stay in the country for a temporary period, leading to a significant decrease in encounters of Ukrainians at the Southwest Border. In response to a sharp rise in the number of Venezuelans encountered at the Southwest Border, DHS created a similar process for Venezuelans meeting certain criteria to travel to and stay temporarily in the country while imposing consequences on those who cross the Southwest Border without authorization. DHS also created processes for nationals of certain other Western Hemisphere countries, including Cuba, Haiti, and Nicaragua, which has led to a significant decrease in the number of people seeking to enter the United States irregularly. Additionally, USCIS has worked closely with the Department's Family Reunification Task Force

by using its discretionary parole authority to allow previously separated family members to enter or remain in the United States temporarily.

Another important legal pathway is the U.S. Refugee Admissions Program. This resettlement program reflects our longstanding values and humanitarian commitment as a nation. Complex, large-scale humanitarian

emergencies are occurring with greater frequency and include mixed migratory flows that often require a regional and even global response to address adequately. To that end, the United States is working to rebuild and strengthen the U.S. Refugee Admissions Program to ensure it remains responsive to those fleeing persecution while safeguarding the integrity of the program and our national security.

Expanding Lawful Pathways while Addressing Acute Seasonal Labor Needs

DHS, in consultation with the U.S. Department of Labor (DOL), announced on October 12, 2022, that it would make available an additional 64,716 H-2B temporary nonagricultural worker visas available to employers for fiscal year 2023, on top of the 66,000 H-2B visas that are available normally each fiscal year. This allocation was made early in the fiscal year, shortly after the statutory authority was provided, and represents the maximum supplemental allocation permitted under that authority. It is also the first time the Departments have issued a single rule making available H-2B supplemental visas across an entire fiscal year, creating the conditions for American businesses to plan in advance to meet their seasonal labor needs. At a time of record job growth, these visas will also provide a safe and lawful pathway to the United States for noncitizens prepared to take jobs that are not filled by American workers.

The H-2B supplemental includes an allocation of 20,000 visas to workers from Haiti or the Central American countries of Honduras, Guatemala, and El Salvador. This advances the Biden Administration's pledge, under the *Los Angeles Declaration for Migration and Protection*, to expand legal pathways as an alternative to irregular migration. The remaining 44,716 supplemental visas will be available to returning workers who received an H-2B visa, or were otherwise granted H-2B status, during one of the last three fiscal years.

At the same time, DHS and DOL are working together to institute robust protections for U.S. and foreign workers alike, including by ensuring that employers first seek out and recruit American workers for the jobs to be filled, and that foreign workers hired are not exploited by subpar working conditions.

Additionally, DHS will improve migrant processing at the border to efficiently identify individuals seeking protection and adjudicate their protection claims (e.g., asylum, withholding of removal, and protection under the Convention Against Torture) in a fair and timely way. This includes tackling the unprecedented backlog of asylum applications that routinely forces individuals who merit protection to wait years for their claims to be heard and adjudicated. A timely and fair asylum process that quickly grants relief to those in need of protection and removes those who do not qualify alleviates pressure at the border and deters frivolous claims for the purpose of obtaining employment authorization.

DHS will break down barriers and promote access to immigration benefits and services for all who are eligible to seek them. DHS has published a fair and humane public charge rule,⁶ expanded H-2 labor visa pathways, and improved options for science, technology, engineering, and math (STEM) talent to use their skills in the United States. DHS will continue to eliminate communication barriers for those with limited English proficiency and provide equitable access for persons with disabilities to immigration programs and services. DHS will continue efforts to address the economy's demand for immigrant workers at all skill levels and reduce barriers in the immigration system. DHS will continue to ensure immigration benefits can be accessed easily by those who are entitled to and qualify

for them. As an example, USCIS exempted processing fees for benefits, such as employment authorization, for Afghan nationals who arrived in the United States as part of OAW. In June 2021, DHS also announced a new policy for individuals with pending bona fide U-type nonimmigrant petitions who, due to backlogs and a statutory visa cap, were facing a significant waiting period for employment authorization and deferred action. The new policy supports victims of crimes, including victims of hate crimes such as those in the Asian American, Native Hawaiian, and Pacific Islander communities, to enable them to receive the stability they need while working with law enforcement to investigate and prosecute criminal activity.

Supporting USCIS and its workforce will be critical to creating the capacity necessary to manage these processes. Since January 2021, USCIS has been able to reduce the number of pending naturalization applications by approximately 450,000.⁷ Access to counsel and legal representation support just and efficient adjudication of immigration benefits and court proceedings, thus contributing to the continued removal of barriers to access the immigration system.

These larger migratory flows and the changing composition of border encounters will require the Department to develop innovative solutions to longstanding challenges with the processing and detention of individuals seeking protection.

Efficient and Fair Processing of Asylum Claims

In March 2022, DHS and the Department of Justice issued a rule to improve and expedite processing of asylum claims made by noncitizens subject to expedited removal, ensuring that those who are eligible for asylum are granted relief quickly and those who are not are promptly removed.⁸ Due to existing court backlogs, the process for hearing and deciding these asylum cases currently takes several years on average. When fully implemented, the reforms and new efficiencies will shorten the process to several months for most asylum applicants covered by this rule.

The rule authorizes asylum officers within USCIS to consider the asylum applications of individuals subject to expedited removal who assert a fear of persecution or torture and pass the required credible fear screening. Previously, such cases were decided only by immigration judges within the Justice Department's Executive Office for Immigration Review. Any individual who is not granted asylum will be referred for a removal proceeding before an immigration judge. The rule establishes streamlined procedures for these removal proceedings, designed to promote efficient resolution of the case. The rule does not apply to unaccompanied children.

DHS will improve and expand its use of alternatives to detention and will ensure that the Department's network of civil immigration detention facilities uphold the civil and human rights of all detained individuals and operate in accordance with U.S. law and DHS policy.

Currently, an estimated 11 million people live in the United States without lawful immigration status—the vast majority of whom are deeply rooted in and significantly contribute to this country. DHS has worked to preserve and fortify Deferred Action for Childhood Arrivals (DACA) to ensure that recipients are protected from the threat of deportation and can continue to contribute to this country that is their home.⁹ DHS is adopting policies that support the enforcement of wage protections, workplace safety, labor rights, and anti-human trafficking

laws. In particular, the Department will focus its enforcement and compliance efforts on unscrupulous employers that seek to exploit an undocumented workforce. DHS will continue to transform enforcement efforts to focus on the most significant threats to the homeland. Finally, we will work to alleviate the fear that may prevent victims and witnesses from cooperating with law enforcement in investigations of exploitative employers, human traffickers, or other criminal actors. This will be accomplished through expanded training of investigators and victim specialists on deferred action, continued presence, parole, and all other available relief, and through enhanced protocols to expedite access to appropriate immigration relief for eligible victims and witnesses.

Facilitating and Expanding Naturalization Pathways

DHS remains committed to facilitating and expanding naturalization pathways for new Americans. The Department continues to grow its Citizenship and Integration Grant Program to move toward this aim, doubling funding to \$20 million in fiscal year 2022 from \$10 million in fiscal year 2021. DHS provides integration services to prospective American citizens under this program via grant recipient organizations. Partner organizations prepare immigrants for naturalization and promote civic integration in American society by increasing knowledge of English, U.S. history, and civics. DHS further expanded the program in 2022 to include not just formal citizenship and English acquisition classes but also opportunities for creative and innovative approaches to naturalization preparation.

DHS has also recently spearheaded numerous new naturalization initiatives. In 2021, DHS announced a new initiative, in partnership with the Department of Veterans Affairs, to better ensure receipt of eligible benefits by noncitizen service members and their families, a component of which entailed protecting and expanding naturalization opportunities for these noncitizens. The Department has continuously conducted reviews of naturalization access and institutional challenges, including those for disability exception-eligible individuals and underserved communities. DHS continues to take steps to remove such barriers to naturalization for eligible individuals across a variety of applicable contexts.

Together, these approaches will create a fair, orderly, and humane immigration system in which we enforce our immigration laws and responsibly manage our borders, acknowledge the contributions that immigrants make to our society, embrace our humanitarian responsibilities as a nation, and encourage those who are eligible to take advantage of the benefits of citizenship. At the same time, DHS will continue working with Congress on multi-faceted legislation to update our immigration laws, as almost 40 years have passed since the last comprehensive reform. Ultimately, Congress must make meaningful reforms to our legal immigration system, which are essential

for reuniting families and strengthening our workforce, creating a durable pathway to status for noncitizens long present in the United States like DACA recipients, providing meaningful humanitarian protection that reflects current causes for displacement, such as climate change, and providing resources for modernizing our strategic border security approach for the 21st century.

Crimes of Exploitation

Crimes of exploitation—child sexual exploitation and abuse (CSEA), human trafficking, and labor exploitation—occur at alarmingly high rates.¹⁰ These crimes represent not only a direct attack on our values and personal and public safety, but also threaten our physical and virtual borders, our immigration and customs systems, our prosperity, and our national security. Accordingly, the Department has redoubled its efforts to combat these crimes and is committed to further enhancing its work in this space.

Online CSEA has exploded in recent years. It encompasses a broad range of criminal acts that, at their core, involve the victimization of children for sexual gratification or some other personal or financial gain. 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 CSAM produced and shared on the dark web and through livestream platforms.

Human trafficking, which involves exploiting a person through force, fraud, or coercion for labor, services, or commercial sex acts, or any



exploitation of a minor for commercial sex, occurs throughout the United States and everywhere around the world. According to recent global estimates,¹¹ there are an estimated 28 million people in forced labor worldwide, including 3.3 million children in forced labor. In addition, there are 6.3 million people in situations of forced commercial sexual exploitation, with the great majority of them being women and girls. Human trafficking is perpetrated by an array of actors, ranging from individuals to loosely affiliated family-based networks to highly structured criminal enterprises. Human trafficking crimes can occur entirely within the United States or may operate transnationally, with victims lured into the United States and exploited for labor, services, or commercial sex upon arrival. Trafficking offenses frequently involve multiple forms of related criminal conduct, including financial crimes, document fraud, racketeering, other immigration violations, narcotics

distribution, sexual exploitation, violent offenses, and labor infractions.

DHS fights all types of human trafficking—sex trafficking and forced labor—including the importation of goods produced in whole or in part with forced labor. Forced labor occurs when individuals are compelled against their will to provide work or service based on force, fraud, or coercion. Victims may be any age, race, religious affiliation, gender identity, or nationality, but some groups, like migrant workers or those with disabilities, are especially vulnerable. Victims of forced labor in the United States may be U.S. citizens, or they may be noncitizens, with or without legal status.

Beyond crimes of exploitation, noncitizen workers are often afraid to report violations of law by exploitative employers or to participate in employment and labor standards investigations. This fear is often driven by threats of deportation or other immigration-related

retaliation by an abusive employer. As a result, law enforcement agencies are often unable to hold accountable employers who profit from exploiting vulnerable workers. This, in turn, creates unfair labor market conditions that harm U.S. workers and American businesses who comply with our labor laws. It also perpetuates the commission of unlawful and inhumane acts by employers, including nonpayment of wages, debt bondage, the imposition of unsafe working conditions, as well as chilling workers' ability to organize and collectively bargain to improve such conditions.

Goods produced abroad with forced labor in multiple countries and regions that are imported into the United States allow bad actors to profit from vile abuses of human rights and human dignity and undermine legitimate trade and competition. Government documents from the People's Republic of China (PRC) confirm that forced labor is part of the PRC's targeted campaign of repression, mass internment, and indoctrination of ethnic minorities in the Xinjiang Uyghur Autonomous Region (XUAR) and elsewhere in China. As a result, supply chains that have a nexus to the XUAR have a particularly high risk of involving forced labor. It is sometimes difficult, however, for U.S. importers to identify forced labor in their supply chains due to the growing complexity of supply chains, the challenge of tracing to the early stages of manufacturing (i.e., the raw or near-raw material level) where forced labor often occurs, and the commingling of legitimate



production processes with inputs made with forced labor.

DHS is prioritizing the fight against these crimes by establishing and growing the DHS Center for Countering Human Trafficking (CCHT), expanding and enhancing the Department's counter-CSEA work, highlighting efforts to combat these crimes among the Department's core 2022 and 2023 priorities, and recognizing this work as a homeland security mission for the first time. The codification of the CCHT in the *Countering Human Trafficking Act of 2022*,¹² in particular, has enabled the consolidation of numerous efforts across the Department in one place. The CCHT is a DHS-wide center with 16 Offices and Component agencies coordinating efforts to combat human trafficking and the importation of goods produced with forced labor. Consistent with this focus, DHS is undertaking a wide range of actions to 1) enhance prevention through public education and training, 2) identify, protect, and support victims, and 3) detect, apprehend, and disrupt perpetrators of exploitation.

Enhance Prevention through Public Education and Training

We cannot defeat crimes of exploitation solely by investigating, arresting, and prosecuting perpetrators. The lack of public awareness about these crimes creates space for them to flourish, so DHS is committed to educating partners and the public to identify and prevent crimes of exploitation.

In fiscal year 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, DHS's Federal Law Enforcement Training Centers (FLETC) 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 Blue Campaign and the DHS Center for Faith-Based and Neighborhood Partnerships also provide educational counter-trafficking materials in numerous languages, and the CCHT and USCIS offer public webinars on immigration protections for victims of human trafficking.

In fiscal year 2023, DHS will also launch a first-of-its-kind national public awareness campaign to counter the rapidly escalating crisis of online CSEA. The campaign will seek to educate children, caregivers, policymakers, and the broader public about the growing and myriad threats of online CSEA and how to keep children safe online. It will reside in the Homeland Security Investigations (HSI) Cyber Crimes Center as a permanent Department function.

This campaign, which will reach target audiences largely through social media and other online avenues, will build on existing efforts at HSI and USSS. HSI operates Project iGuardian in partnership with NCMEC

NetSmartz and the Internet Crimes Against Children Task Forces to educate children, teens, parents, and teachers throughout the country about online safety and how to stay safe from sexual predators. DHS and HSI are working to update and expand this program in fiscal year 2023, together with the launch of the new public education campaign. For its part, USSS operates the Childhood Smart Program, in partnership with NCMEC, to educate parents, teachers, and children about safe use of the internet, abduction prevention strategies, and combatting child sex trafficking.

Identify, Protect, and Support Victims

A victim-centered approach that seeks to minimize additional trauma, mitigate undue penalization of victims, and provide needed stability and support to victims of trafficking and exploitation is critical. This approach helps survivors begin to repair their lives and enables law enforcement to better detect, investigate, and prosecute perpetrators. Across the Department, 11 Offices and Components that interact with victims or carry out related mission sets drafted plans in fiscal year 2022 to incorporate a victim-centered approach into all relevant policies and programs. In October 2021, Secretary Mayorkas directed that DHS operations and activities promote a victim-centered approach. ICE, for example, issued a new directive, *Using a Victim-Centered Approach with Noncitizen Crime Victims*, to minimize the chilling effect that civil immigration enforcement may have on the

willingness and ability of noncitizen crime victims to contact law enforcement, participate in investigations and prosecutions, pursue justice, and seek benefits. DHS will build on this progress by developing a Department-wide policy on gender-based violence and trauma-informed care and working with the interagency to establish victim-centered screening protocols.



In fiscal year 2022, DHS also expanded the HSI Victim Assistance Program, increasing the number of victim assistance personnel by 40 percent. In fiscal year 2023, HSI will grow the program by another 60 percent. These investments have led to increases in the identification of victims of child sexual abuse and human trafficking, victim referrals for social services in local communities, and forensic interviews using trauma-informed, victim-centered methods to elicit accurate and complete information from victims while minimizing distress. The Victim Assistance Program helped 3,326 victims worldwide in

fiscal year 2022, including 1,138 victims of child exploitation, 765 human trafficking victims, 1,151 financial crime victims, and 272 others.

DHS's Child Exploitation Investigations Unit (CEIU), a global leader in CSEA law enforcement operations, identified or rescued more than 1,000 child victims of sexual exploitation in fiscal year 2022. The CEIU Victim Identification Program 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, CEIU's Victim Identification Program has identified or rescued more than 10,000 child victims of sexual exploitation. The DHS Science and Technology Directorate (S&T) 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 victims. These tools include live-stream capabilities, advanced facial-recognition technologies, and speech and language technologies.

Through USCIS, in fiscal year 2022, DHS also significantly increased the protections granted to qualifying victims of human trafficking and other serious crimes. USCIS more than doubled the number of T visas granted to trafficking victims, provided employment authorization and deferred action to victims with bona fide U visa petitions, and reached the cap of U visas

granted to victims of qualifying crime. These actions offered victims safety, stability, and a means to become self-sufficient. In addition, the CCHT is working to modernize and streamline the Continued Presence system, a temporary immigration designation for individuals identified by law enforcement as human trafficking victims who may be potential witnesses or have filed federal civil actions. Recipients are eligible for federal benefits and services that provide victims with stability, a means of support, and protection from removal. When used by law enforcement, Continued Presence is a critical tool that helps increase the likelihood of success in human trafficking investigations and prosecutions.

Detect, Apprehend, and Disrupt Perpetrators

As a leader in the fight against human trafficking, DHS works with partners at every level to prevent trafficking crimes and bring perpetrators to justice. Launched only two years ago in October 2020, the CCHT is already achieving significant results, including substantially more human trafficking investigations and arrests.

DHS is also enhancing its worksite enforcement capacities and leveraging them to hold exploitative employers accountable. Building on DHS's longstanding practice of providing discretionary protection on a case-by-case basis to noncitizen victims and witnesses, DHS established streamlined processes to facilitate

the ability of labor law and employment law enforcement agencies to seek DHS support on behalf of workers who are part of their investigations. The enhanced processes allow these agencies to enforce labor and employment laws more effectively and improve workplace conditions for all workers.

In addition to rescuing child victims of sexual exploitation, the DHS CEIU also detects and apprehends producers and distributors of CSAM and perpetrators of transnational child sexual abuse. CEIU employs 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, livestream, and other internet-based platforms. CEIU's Operation Predator targets child sexual predators on both the clear web and dark web, which in fiscal year 2022 led to the arrest of 4,459 individuals 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.

DHS is the primary federal agency responsible for enforcing civil and criminal laws to disrupt and dismantle the importation of goods produced in whole or in part with forced labor, a

Preventing Labor Exploitation

DHS has a critical role in ensuring that our nation's workplaces comply with our laws. DHS worksite enforcement efforts have a significant impact on the well-being of individuals and the fairness of the labor market. The Department is maximizing the impact of its efforts by focusing on unscrupulous employers who exploit the vulnerability of undocumented workers. These employers engage in illegal acts ranging from paying substandard wages to subjecting workers to unsafe employment conditions and facilitating human trafficking and child exploitation. In line with this focus on unscrupulous employers, HSI's "worksite enforcement" unit was re-named the "labor exploitation" unit in August 2021.

CBP, ICE, and USCIS developed policies and processes to achieve three goals: 1) reduce the demand of illegal employment by delivering more severe consequences to exploitative employers, 2) increase the willingness of workers to report violations of law, and 3) broaden and deepen cooperation between DHS and labor enforcement agencies at the federal, state, and local levels. Most recently, in January 2023, DHS announced that noncitizen workers who are victims of or witnesses to labor rights violations can access a streamlined and expedited deferred action request process. These improvements advance the Biden-Harris Administration's commitment to empowering workers and improving workplace conditions by enabling all workers, including noncitizens, to assert their legal rights.

form of human trafficking. The Department inspects the supply chains of imports for evidence of forced labor, investigates suspicious trade activity, issues notices to detain, exclude, or seize particular goods at our ports, and investigates and refers criminal prosecutions against individuals and companies involved in the importation of prohibited goods. DHS supports industry in taking proactive measures to prevent and eliminate human trafficking in their supply chains. Through CBP and the DHS Office of Strategy, Policy, and Plans (PLCY), DHS led efforts to implement the *Uyghur Forced Labor Prevention Act* (UFLPA).¹³ In June 2022, CBP began enforcing this landmark law, which established a rebuttable presumption that goods produced in XUAR or by an entity on the UFLPA Entity List are prohibited from entering the United States due to the use of forced labor. Further, in fiscal year 2022, CBP issued six Withhold Release Orders, two findings, and one Withhold Release Order modification related to the enforcement of U.S. law prohibiting the importation of goods produced in whole or in part with forced labor.

As chair of the Forced Labor Enforcement Task Force, DHS along with interagency members including the Departments of Labor, State, Justice, Treasury, Commerce, and the United States Trade Representative, will build out the UFLPA Entity List in the coming year. This represents a significant and novel multi-agency effort to identify entities that use or source labor or goods from the XUAR. The UFLPA Entity

List is an important component of UFLPA enforcement that protects U.S. workers and consumers from supporting or being harmed by PRC forced labor practices.

Going forward, DHS will continue to enhance and mature its work to combat crimes of exploitation. Following the recent enactment of the *Countering Human Trafficking Act* of 2022, which codified the CCHT, the Department is working to implement the law's important provisions, including the transfer of Blue Campaign to the CCHT to ensure integration of all counter-trafficking functions. In addition, as outlined above, the Department is heavily investing in CSEA prevention efforts, launching an ambitious national public education campaign that will become a permanent function within the Cyber Crimes Center. Additionally, the HSI Cyber Crimes Center will become the DHS Cyber Crimes Center to reflect its expanding functions that reach beyond the traditional law enforcement domain and involve broader Department equities. Finally, CCHT participates in a public-private working group to address forced labor in healthcare and public health supply chains with other federal agencies and stakeholders across the health sector in response to the *National Action Plan to Combat Human Trafficking*¹⁴ and the *National Strategy for a Resilient Public Health Supply Chain*.¹⁵

Transnational Organized Crime

Transnational criminal organizations pose a persistent threat to homeland security, driving illicit drug trafficking into the United States putting the lives of Americans and migrants at risk for profit, destabilizing our neighbors, and fueling illicit commerce around the world. DHS is uniquely positioned to address transnational organized crime, bringing together the enforcement capabilities of CBP and the USCG, the investigative capabilities of ICE and USSS, the strategic planning and analysis capabilities of PLCY, and the intelligence collection and analysis capabilities across the Department's Intelligence Enterprise, and capacity-building international partnerships.

Transnational criminal organizations destabilize governments by fostering corruption. They secure their power through intimidation and violence. They illegally smuggle drugs, including fentanyl, methamphetamine, cocaine, and heroin, into the United States, leading to increased availability and deaths across the country. They exploit and drive migration trends, spread disinformation to recruit migrants and place them in harm's way for profit, and sometimes turn human smuggling into human trafficking when sex trafficking, forced labor, and indentured servitude render the migrant's journey non-consensual. Transnational criminal organizations often leverage fraud, illicit use of digital assets, and



money laundering to fund their operations while remaining under the radar of law enforcement entities. They also traffic weapons out of the United States, fueling violence in Mexico, the Caribbean, and throughout Central and South America. Cybercriminal syndicates have expanded throughout the years as they offer their malware and infrastructure to malicious cyber actors, such as selling ransomware-as-a-service capabilities, which allows a wide-range of adversaries to launch cyberattacks against the homeland. The volume of transnational organized criminal activity impacting the United States is unlikely to decrease due to the sustained demand for illicit goods and services and the high profits available to those who supply them.

Throughout 2022, DHS and federal partners intensified disruption efforts, marshaling the largest-ever surge of resources against human smuggling networks. Because of these

increased law enforcement efforts, human smuggling organizations have been forced to change their tactics: some have shifted their routes; some have moved their stash houses—the locations where they hold people being smuggled or stash illicit weapons—further away from the border.

At and between ports of entry, CBP officers screen passengers and cargo for illicit narcotics, disrupt efforts to subvert border security measures, and stand ready to assist those who may be affected by human smuggling or be victims of trafficking. Through intelligence-based operations, CBP and the USCG have interdicted record amounts of cocaine and other drugs, as well as environmental crimes such as illegal, unreported, and unregulated fishing and seafood fraud, destined for the United States. DHS will work to coordinate and unify these efforts across DHS Components to counter transnational organized crime threats to the United States and its interests.

Countering transnational organized crime requires partnerships with other federal agencies, SLTT authorities, and international counterparts. Together, we will identify, investigate, prosecute, and counter human smuggling and trafficking connected to transnational criminal organizations to protect our borders, those already in the United States, and the well-being of the most vulnerable who seek to come to the United States.

Through joint interagency initiatives, CBP, ICE, TSA, USCG, USCIS, and USSS, alongside the Departments of Justice, State, and Treasury as well as international partners, will leverage their respective authorities and capabilities to deny transnational criminal organizations the means to smuggle people and traffic drugs and contraband into the United States or otherwise violate U.S. laws. Efforts such as Operation Sentinel have mapped foreign and domestic transnational criminal networks, their associates, and assets. Through Operation Sentinel, DHS and its partners have revoked travel documents, suspended and debarred trade entities from entering the U.S. market, and frozen financial assets connected to transnational criminal logistical networks.

DHS will also support efforts to bring transnational criminal organizations to justice through partnerships such as Joint Task Force Alpha. This task force brings together federal prosecutors along the Southwest Border with law enforcement agents and analysts from CBP and ICE to investigate and prosecute the most prolific and dangerous human smuggling and trafficking groups operating in Mexico and Northern Central America.

Additionally, we will bring together federal, state, local, and foreign partner resources to counter transnational criminal activity at and within our borders. The ICE-led Border Enforcement Security Task Force (BEST) teams, comprised of officers from more than 100

different law enforcement agencies, exemplifies these efforts. BEST teams have closed the gap between international partners in multinational criminal investigations and disrupted transnational criminal organizations at every level.

In 2022, DHS announced joint actions with Mexico to target human smuggling organizations and bring them to justice. Further, DHS has made historic investments in non-intrusive inspection technology to be deployed at ports of entry to increase our interdiction of illicit drugs, countering traffickers who seek to smuggle drugs in cars, trucks, and containers. 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. In collaboration with Joint Interagency Task Force-South, CBP operates aircraft throughout North and Central America, conducting counternarcotics missions to detect and interdict bulk quantities of illicit narcotics.

In the last two fiscal years, 2021 and 2022, DHS seized more fentanyl than in the previous five fiscal years combined. In the last two fiscal years, DHS arrested more criminals for committing crimes related to fentanyl and precursors chemicals than in the previous five years combined. In March 2023, Operation Blue Lotus, a DHS-led, coordinated surge effort to curtail the flow of illicit fentanyl smuggled

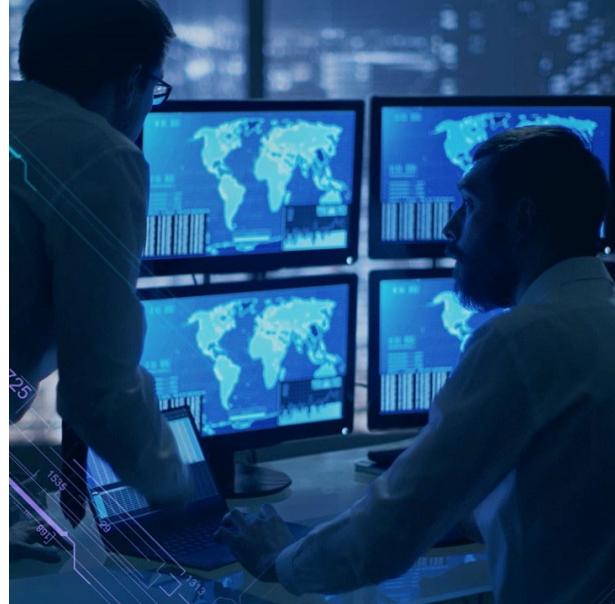
into the United States from Mexico and bring to justice the dangerous criminal organizations profiting from the illegal production, distribution, and sale of this dangerous substance, began. Operation Blue Lotus leverages advanced analytics and intelligence capabilities at HSI and CBP and includes the deployment of HSI personnel alongside CBP Officers at ports of entry so that they can immediately pursue investigations as contraband is discovered in order to expose the networks. Given that the vast majority of fentanyl is smuggled through U.S. ports of entry, further investments in non-intrusive inspection technology will be critical in bolstering these efforts.

Directly confronting transnational organized crime must also extend beyond our borders through capacity-building partnerships across the globe. ICE leads Transnational Criminal Investigative Units in more than a dozen countries to facilitate rapid bilateral cooperation on investigations and prosecutions. These units include foreign law enforcement, customs, and immigration officials, as well as prosecutors who undergo strict vetting and complete robust training. CBP and the USCG have deployed personnel internationally to advise local authorities on port security, customs modernization, and border enforcement. These exchanges and partnerships address the root causes of instability and corruption, mitigating transnational criminal threats before they reach our borders.

Proliferating Cyber Threats

Cyber threats have evolved and increased since the founding of the Department. Nation-state threat actors are becoming increasingly sophisticated, targeting federal, state, and local government agencies, critical infrastructure companies, and others. Likewise, cyber criminals have increased their malicious activities motivated by the significant profits they can make from using relatively accessible and affordable ransomware and malware tools. Today, almost anyone can become a hacker.

Whether motivated by profit or ideology, cyber adversaries are willing to harm the American people by targeting businesses, schools, hospitals, police departments, state and local governments, and critical infrastructure. This includes America's election infrastructure, which is why the Department remains committed to supporting election officials in safeguarding and securing election infrastructure, including continuing efforts to secure all upcoming and future election cycles. There are also actors who have used ransomware during an unprecedented and ongoing global pandemic, disrupting hospitals dealing with surges of COVID-19 patients. We need only look at recent events, such as the SolarWinds supply chain compromise or the ransomware attacks affecting Colonial Pipeline, to see the impacts.



As commercial network technologies are woven increasingly into our businesses, personal lives, and federal as well as SLTT government functions to provide the most critical services upon which we depend, there remain cyber risks and vulnerabilities that leave networks and systems at risk of exploitation and disruption. The ransomware attack on Colonial Pipeline illustrated that the real-world impacts of software vulnerabilities are not hypothetical. The attack undermined confidence in and availability of fuel for thousands of Americans. These consequences are significant in their own rights, but future disruptions could be more harmful, widespread, and long-lasting. The cascading effects mean cyber risks are becoming more complex and difficult to assess.

The intersection of these variables has placed the nation in a state of untenably high cybersecurity risk, with cyber incidents regularly disrupting our way of life. This heightened risk

requires moving beyond individual actions and toward coordinated defensive actions and cybersecurity measures that are commensurate with national security, economic security, and public health and safety. In furtherance of the National Cybersecurity Strategy released in March 2023, DHS—through CISA, as the nation’s cyber defense agency and national coordinator for critical infrastructure security and resilience, as well as other Components that include I&A, ICE, TSA, USCG, and USSS, and in tandem with private sector and SLTT partners, as well as the Intelligence Community, the interagency, and law enforcement as part of a whole-of-government approach—must manage national cyber risk.

Disrupting Active Threats

DHS will protect the American people by preventing and mitigating active threats. CISA collaborates with federal agencies and private industry to gain greater visibility into vulnerabilities and adversary activity occurring across government and critical infrastructure networks. CISA works to achieve visibility at scale by supporting broader deployment of endpoint detection capabilities across federal agencies. CISA also works with private sector critical infrastructure entities through SRMA partnerships and partnerships like the JCDC to share information about ongoing malicious campaigns and to coordinate defensive efforts. This includes increasing threat hunting and incident response capabilities as well as capacity for coordinating vulnerability



disclosures and responses. CISA further conducts outreach in coordination with SRMAs to private sector critical infrastructure entities and establishes relationships to enhance an organization’s ability to respond to cyber incidents. CISA provides products on insider threat mitigation, pathways to violence, and soft skills like employee vigilance to help build a proactive culture to identify and disrupt threats before they cause damage.

DHS will also disrupt threats by ensuring ICE’s HSI and the USSS remain capable of combatting 21st century crimes. Cybercrime affects the wallets of Americans across the country, with losses worth billions of dollars a year. The country’s most vulnerable, from the

elderly and unemployed individuals reliant on government assistance to communities of color and families, are those most impacted by cybercrime. DHS will empower the Cyber Fraud Task Forces, led by the USSS and their partners across the law enforcement community, to combat crimes involving cyberspace.

Our efforts also include combatting the illicit use of virtual currencies and digital assets. Successfully combatting illicit use of digital assets will require a whole-of-government effort. The Department's law enforcement Components, USSS and HSI, prioritize their global network of law enforcement and public and private partnerships to mitigate cybercrimes, identify and arrest the criminals, and return stolen funds to the victims. As technology changes and economic activity involving digital assets rises leading to increased exploitation by cybercriminals, DHS will continue to evolve its training and investigative methodologies to keep pace.

CISA and FBI, through the JRTF, will work with interagency, SLTT, and private sector partners to coordinate campaigns against transnational ransomware criminal groups. This will include providing support to private sector entities and SLTT communities to better protect themselves from ransomware. The JRTF will also collect, share, and analyze ransomware trends to inform federal actions while facilitating coordination and collaboration between federal entities and the private sector to improve our

actions against the ransomware threat posed by transnational cybercriminal groups.

Strengthening the Nation's Cyber Resilience

DHS is using innovative and novel approaches to strengthen our nation's resilience across critical infrastructure systems, including those that support National Critical Functions, with the goal that even if a natural disaster, physical security breach, or cyber incident occurs, the critical services remain functional.

As the majority of the nation's critical infrastructure is owned by the private sector, effective responses to threats demand close coordination between the public and private sectors. The Administration has established new cybersecurity requirements in certain critical sectors, while in other sectors, new authorities will be required to set regulation that can drive better cybersecurity practices at scale. This Administration has conducted sector specific engagement with industry to construct consistent, predictable regulatory frameworks for cybersecurity that focus on achieving security outcomes and enabling continuity of operations and functions while promoting collaboration and innovation. To build out cyber resilience more effectively across critical infrastructure and other stakeholders, DHS is investing in initiatives to enhance public-private collaboration. These innovative efforts include the Cybersecurity Advisory Committee for pre-event strategic planning, the JCDC for planning and real-time event coordination, and the Cyber

Safety Review Board (CSRB) for after-action analysis.

CISA will continue advancing national efforts to secure and protect against critical infrastructure risks, including implementing a national plan that recognizes both the expanding scale of terrorism and other threats and the emerging cybersecurity challenge of increasingly networked and internet-enabled infrastructure systems. The Department, in close partnership with SRMAs, has amplified its role as the coordinator of the national effort for critical infrastructure security and resilience. CISA is also developing a list of systemically important entities to focus on the most essential critical infrastructure, as well as reinvigorating the Federal Senior Leadership Council to further optimize this unified effort. These efforts will support security and resilience to all threats and hazards, not just cyber threats.

As directed by the President's *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*,¹⁶ CISA has developed, in coordination with the National Institute of Standards and Technology (NIST), cross-sector Cybersecurity Performance Goals—voluntary best practices that outline the highest-priority baseline measures businesses and critical infrastructure owners of all sizes can take to protect themselves against cyber risks—to ensure the security of critical infrastructure and reduce our escalating national cyber risk. DHS also leverages TSA's

authorities for the issuance of security directives to the pipeline and surface sectors, as well as security program amendments for the aviation sector, and USCG regulatory authorities for the marine transportation system. For example, TSA security directives now require pipeline entities to take several mitigating measures, including having contingency plans in the event of an intrusion and conducting robust vulnerability testing, that will lay foundations for more secure and resilient systems. These regulatory authorities, together with voluntary measures such as the July 2021 voluntary industrial control system cybersecurity performance goals developed in a partnership between CISA and NIST, are critical to enhancing security. In many cases, other departments and agencies have the authorities, expertise, and capabilities to manage risks to key critical infrastructure sectors and certain National Critical Functions. DHS will redouble its efforts to deepen coordination, synchronization, harmonization, de-confliction, and coordination across the Federal Government.

This also includes the *Cyber Incident Reporting for Critical Infrastructure Act of 2022* (CIRCIA).¹⁷ Enacting CIRCIA marks an important milestone in improving America's cybersecurity. Among other improvements, CIRCIA authorizes CISA to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA. These reports will allow CISA to work alongside

SRMAs to deploy resources rapidly and render assistance to victims experiencing a cyber incident, analyze incoming reporting across sectors to spot trends, and then quickly share that information with network defenders to warn other potential targeted entities. CIRCIA also provides for the DHS-led Cyber Incident Reporting Council that will develop and make recommendations to harmonize federal cyber incident reporting requirements.

DHS is leading transformational change in how we build cyber defense at the international level. Above and beyond the current international partnerships in place, DHS is focusing on increasing operational collaboration between governments and the private sector,

as well as among national governments. Most recently, DHS broke new ground for broadening international partnerships with the expansion of the Abraham Accords to include cybersecurity. As part of this effort, DHS and its Middle East partners, Israel, the United Arab Emirates, Bahrain, and Morocco, have committed to sharing information about cyber threats, incidents, and approaches to these challenges to increase global cybersecurity and resilience. These partnerships are already paying off: through these new channels, DHS has received actionable technical information on shared cyber threats and vulnerabilities, including on specific cyber activity targeting critical infrastructure.



Lastly, DHS will work with the interagency and the White House to ensure that infrastructure projects funded by the *Infrastructure Investment and Jobs Act*¹⁸ are built with cybersecurity in mind. DHS will support federal departments and agencies to include cybersecurity and all-hazards requirements into “notice for funding” opportunities and project lifecycles. CISA and FEMA will make significant advancements to enhance the cybersecurity of SLTT networks and public critical infrastructure through the State and Local Cybersecurity Grant program funded in the *Infrastructure Investment and Jobs Act*, the Department’s first grant solely dedicated to cybersecurity.

Driving Security-by-Default

To build the secure and resilient future we want, we must place responsibility on those within the

digital ecosystem that are best positioned to reduce risk. This includes driving the manufacturers of technology to build their products secure by design and secure by default. This will take a whole-of-government and whole-of-economy approach. At DHS, we will reduce risk across the cyberspace ecosystem by supporting the development of secure software and technologies, driving cybersecurity innovations, cultivating a national cyber workforce, and supporting international partnerships and norms. Software vulnerabilities are at the heart of the national cybersecurity crisis. Consistent with E.O. 14028, *Improving the Nation’s Cybersecurity*,¹⁹ DHS will help leverage the purchasing power of the government to drive down software vulnerabilities and ensure the government purchases secure technology. DHS will expand

Cyber Safety Review Board

To ensure the cyber security community is constantly enhancing its work and acting on lessons learned from experience, DHS established the CSRB in 2022. The CSRB is an unprecedented public-private partnership that brings together government and industry leaders to conduct fact-finding and make recommendations following significant cyber incidents. During its inaugural review of the Log4j software vulnerability discovered in December 2021, the CSRB interviewed and obtained data from over 80 organizations and security experts. The Board compiled an authoritative account of what happened, from the vulnerability discovery to the progression of the largest-scale cyber incident response in history, to patch the vulnerability across virtually every networked organization. The CSRB also provided industry, federal agencies, and the software development community with clear, actionable recommendations based on what the Board discovered, so that the community could be better protected going forward. The CSRB is an important example of operational collaboration between the private and public sectors following major incidents and has established itself as an enduring part of the cyber ecosystem.



its efforts to support technology vendors and developers to reduce the prevalence of vulnerabilities at their source and secure the information and communications technology supply chain. DHS will work with industry to ensure that technologies supporting critical infrastructure are appropriately secure before going to market and throughout their life cycle, including by driving adoption of the software and hardware bill of materials²⁰ and related secure development practices.

DHS will work to change business incentives to drive the design of more secure software and the adoption of best practices. While the actions of individuals, such as enabling multi-factor authentication, are essential to achieve such levels of security at scale, government and private industry must design commercial software products with sufficient levels of security inherent in their use. DHS will fully implement Zero Trust Architecture across our

internal systems, and support industry efforts to expand those same principles across the private sector and critical infrastructure.

CISA enables critical infrastructure owners to identify and mitigate known cyber vulnerabilities when the firms voluntarily sign up for CISA's no-cost Cyber Hygiene Scanning Services. The scanning notifies participating critical infrastructure owners when CISA finds vulnerable applications or weak configurations across the firms' internet facing infrastructure. By mitigating these vulnerabilities, firms can lessen the potential attack surface available to ransomware and nation-state cyber actors.

Protecting Federal Civilian Executive Branch Networks

DHS, in concert with its partners including the Office of Management and Budget, puts these goals into action with respect to its own networks and the broader .gov environment.

Joint Cyber Defense Collaborative

CISA established the JCDC to integrate unique cyber capabilities across multiple federal agencies, state and local governments, and private sector entities to achieve shared objectives. Specifically, the JCDC has developed:

- Strong strategic and operational alliances within the cybersecurity community.
- Increased visibility and insight into the cyber threat landscape.
- Diverse resources and expertise to fuel creative cybersecurity solutions.
- Vastly amplified capacity to gather, analyze, and share information to defend against cyber threats.

The efforts of the JCDC have already yielded concrete results, as the warning on the BlackMatter ransomware group²¹ was, in part, based on information provided by JCDC partners. DHS's goal is to bring together key federal, private sector, and SLTT partners who have visibility into, and the ability to understand, the threat landscape by virtue of their responsibilities, and to plan and exercise against the most serious threats to our nation.

CISA has the authority to issue Binding Operational Directives (BODs). BOD 22-01, for example, represents the concrete steps DHS is taking to enhance the security of federal and civilian networks, in this case by requiring agencies to remediate vulnerabilities on aggressive timelines. Altogether, the Department will work with federal partners to improve federal cybersecurity posture and incident response capabilities, limit supply chain risk for the Federal Government, and increase CISA's and other DHS Components' visibility across federal and contractor networks.

Cyber Talent

DHS is committed to developing a cybersecurity workforce with the size, skills, diversity, and

training necessary to meet our mission, protect our businesses and families, defend our critical infrastructure, and forge a more secure future. This will not be easy – a 2021 study revealed that there was a 2.7 million cyber worker shortage worldwide in 2021, with over 700,000 of those open positions residing in the United States.²² At DHS, we have been focused on recruiting, training, educating, and retaining top cyber talent across-the-board in the public, private, academic, and non-profit sectors. We are placing diversity, equity, inclusion, and accessibility at the center of our efforts because this is a challenge that affects all of us and we need every perspective at the table.

Strategic Competition

We live in an era in which nation states challenge the security of the homeland. The PRC, Russia, North Korea, and Iran are actively seeking to undermine U.S. competitiveness and our democratic institutions to achieve their geopolitical goals. Russia's invasion of Ukraine in February 2022 demonstrates that aggression abroad reverberates in the homeland, particularly in posing risks to critical infrastructure security. Those who wish to harm us exploit the openness that defines our modern world, through trade and investment flows, through the rapidly evolving technologies that connect us, and through information spread online. Now, more than at any point in the first 20 years of the Department's existence, threats from nation states impact the safety and security of the American people and the homeland.

The reality that nation states increasingly challenge the security of our country presents new challenges for a department created in the aftermath of the most devastating terrorist attack in our nation's history. While our mission to secure the flow of travel primarily faced threats from individuals or transnational criminal organizations in the past, we now also face the organized efforts of nation states. While the nation's cyber networks continue to be threatened by unsophisticated actors, we now also defend against sophisticated, well-resourced, and determined adversaries. While



we continue our work to build a free, open, and secure internet, we now face other nation states that are working to limit access and maximize control of the internet. And while we encounter ideological propaganda from foreign terrorist organizations, we now also see nation states using malign influence and predatory economic practices in the homeland to gain advantage.

The PRC, in particular, is engaged in a campaign to compromise the security of the United States and use its economic, diplomatic, military, and technological power to challenge the stable and rules-based international system. Their campaign is as broad as it is unprecedented. The PRC is looking to advance its capabilities by acquiring our intellectual property; taking advantage of our openness to immigration; sponsoring a relentless barrage of cyberattacks that threaten our competitiveness and our critical infrastructure; and continuing to

be a source of malign influence, disseminating mis-, dis-, and mal-information into our civic discourse. The PRC Government also undermines labor standards and human rights by exporting goods that are made with forced labor. The PRC also seeks dominance in the critical foundational technologies of the future which would serve only to threaten American national and economic security.

To address these challenges, DHS is undertaking a range of actions to keep the homeland secure. This begins with increasing the awareness of nation-state threats to the homeland throughout the entire homeland security enterprise through enhanced information sharing across all levels of government, civil society, and industry. To do this, the Department engages and alerts domestic and international partners on the scope and scale of the PRC's malicious cyber activities. DHS also publicizes information about the harmful intentions and activities sanctioned by the PRC so there can be no doubt of the threats to our homeland and economy from PRC-affiliated cyber actors. DHS also collaborates with our interagency partners to build a common understanding of strategic cyber threats to empower private sector network defenders, critical infrastructure owners and operators, and other federal and SLTT government partners to improve resilience and the integrity of National Critical Functions. DHS will also work to strengthen its enforcement of the prohibition on importing

goods produced, wholly or in part, with forced labor through trade enforcement and criminal enforcement, particularly with respect to the PRC's forced labor practices, and we will continue to facilitate the free flow of lawful trade and grow our trade partnerships with allies, thereby strengthening the economic security resilience here at home and abroad.

DHS is committed to combatting transnational repression—the practice of governments reaching across borders to silence dissent among diasporas and exiles through tools such as assassinations, illegal deportations, abductions, digital threats, INTERPOL abuse, and family intimidation. While there are other perpetrators, the PRC conducts the most sophisticated and comprehensive campaign of transnational repression in the world and DHS is taking all appropriate measures to ensure the PRC is not able to exploit and target U.S. persons. DHS is participating in federal efforts curbing abuse of INTERPOL channels of communication; protecting U.S. communities targeted by transnational repression and bolstering their resilience and knowledge of related threats; improving data and research on transnational repression; and raising awareness of transnational repression in multinational forums.

In the maritime domain, using a confluence of actors—from the People's Liberation Army Navy, the Chinese Coast Guard, to the Peoples Armed Forces Maritime Militia—the PRC flaunts

longstanding international norms to encroach, coerce, and acquire resources from other countries' sovereign waters around the world. Adversaries recognize the inability of many coastal nations to adequately monitor and defend their own territorial waters and exclusive economic zones and seek increasingly to take advantage of their situation through malign activities like resource predation, illicit smuggling, and intra-state confrontation. It is increasingly "coast guard work" which provides the proper response to counter malign activity plaguing the maritime domain. We will continue to support like-minded partners in their efforts to exercise maritime governance and protect their resources within their sovereign waters, reinforcing international order and reducing the likelihood of instability, violence, and mass migrations closer to home.

Ahead of the 2020 U.S. elections, the PRC intensified its efforts to influence the U.S. policy environment, sway political figures it viewed as antithetical to its interests, and deflect and counter PRC-related criticisms. The PRC is not the only foreign actor engaged in malign influence activity, as Russia also worked to sow divisions among the U.S. public and undermine faith in American institutions, and Iran attempted to stoke divisions within the United States and influence the U.S. policy environment. To strengthen our ability to counter such malign influence activity, DHS is growing its partnerships with local election leaders across the country to ensure our elections continue to be safe and secure.

Further, the PRC attempts to use PRC nationals seeking to study or conduct research at



American academic institutions as non-traditional collectors of intelligence and intellectual property. DHS's screening, vetting, and monitoring operations focus on curbing PRC exploitation of immigrant and nonimmigrant visa processes, including by identifying and, where necessary, denying admission to high-risk travelers from the PRC. These actions help protect cutting-edge U.S. technology and intellectual property, as the United States continues to be a nation of opportunity and of welcome for an overwhelming majority of nationals from China who do not pose a threat to study and work in the country each year.

The actions and intentions of Arctic and non-Arctic nations continue to shape the security

environment and stability of the region. Like the rapidly changing physical environment, the geopolitical environment is evolving as state and non-state actors seek to advance their own interests in the Arctic. Allies, partners, and competitors increasingly contend for diplomatic, economic, and strategic advantage and influence. Russia and the PRC exemplify this competition, with both nations declaring the Arctic a strategic priority. Additionally, both Russia and the PRC have made significant investments in new or refurbished capabilities and are exerting direct or indirect influence across the region, often with a willingness to violate international law to achieve their interests.



There are also opportunities to align with our allies and partners to address the flow of fentanyl and chemical precursors from China, which remains the primary source of these substances trafficked into the United States. In establishing global awareness of the United States' commitment to disrupt illicit fentanyl supply chains and galvanizing international cooperation as a foundation for voluntary action to prevent the exploitation of legitimate commerce, we will demonstrate American leadership in addressing this global problem. There are practical and commonsense steps nations, to include the PRC, can take to disrupt the global trafficking of synthetic opioids and their precursors. They include implementing "know your customer" standards to prevent the diversion of chemicals to illicit drug manufacturing, proper labeling of chemical shipments from host countries through enforcement of World Customs Organization standards, and monitoring for the diversion of uncontrolled chemicals and equipment in international flows. DHS, along with U.S. Government partners, will continue to work domestically and with its partners around the world to disrupt criminal organizations and will continue to make action against the synthetic drug supply chain a priority.

There are further tasks for which the government, along with industry, must take the lead. Building resilience to the impacts of climate change, for instance, will leave Americans better able to adapt and recover

from severe storms and extreme heat than other nations. Securing federal and civilian networks will make the nation resilient in the face of offensive cyberattacks from nation-state threat actors. Similarly, the processes by which DHS and other federal agencies screen foreign investments in U.S. assets—to include the Committee on Foreign Investment in the United States (CFIUS), Committee for the Assessment of Foreign Participation in the United States Telecommunications Sector (also referred to as Team Telecom), and Information and Communications Technology and Services programs—protect Americans from predatory economic practices while preserving the longstanding open investment policy of the United States.

There are important roles to play across the homeland security enterprise, but DHS and our Federal Government and major industry partners must take the lead in understanding the threats posed by the PRC and other nation states, sharing actionable information, and, ultimately, taking the necessary steps to enhance security at scale. Alongside our partners in communities throughout the country, as well as other federal partners, DHS will harness American diversity and ingenuity to withstand global disruptions and direct threats in the face of strategic competition.

Climate Change

Even with significant interventions, the planet will continue to warm, causing increasingly serious impacts on the American people and on DHS's missions and its workforce. Severe and frequent natural disasters, rising ocean temperatures, shrinking sea ice, rising sea levels, wildfires, heatwaves, droughts, and ocean acidification all produce serious threats. We have already experienced record rain events and wildfires, as well as increases in the number of coastal storms and inland flooding. Rising temperatures and natural disasters also increase the risk of infectious diseases. Such events disrupt our economy, result in loss of life and property, and cause suffering for millions of Americans and their communities. Moreover, chronic underinvestment in underserved communities leave residents more susceptible to the effects of severe weather events and make recovery more difficult afterwards. DHS will create a set of tools and reforms to promote national resilience and adaptation, bolster innovation and partnerships, and look internally at its own roles and responsibilities to decrease the overall risks to our nation associated with climate change.

The DHS Climate Change Action Group is coordinating DHS's efforts to build national resilience to ensure that a warmer country is not a more dangerous one. Over the next four years, DHS will provide information, expertise, and advice to communities and individuals



about the risks they face and how to mitigate them. DHS has already begun these efforts. DHS is striving to increase climate literacy. FEMA's release of the *Building Community Resilience with Nature-Based Solutions* guide helps communities understand how to implement nature-based solutions to build resilience, and FEMA's improved and updated National Risk Index provides information on community-level risk from 18 natural hazards to empower communities to make informed decisions about how to become more resilient. The release of FEMA's *Resources for Climate Resilience* guides communities to leverage FEMA's resources to become more resilient. Likewise, the USCG has worked actively to refine, improve, and expand contingency and response plans with strengthened Area Contingency Planning.

DHS will also promote innovation. S&T has created a new series of prize competitions

focused on strengthening nationwide resilience to climate change. The first in the series, the “Cooling Solutions Challenge,” led by S&T in partnership with FEMA, was designed to engage American innovators to find new ways to better protect people at risk of heat-related illness or death during extreme heat events or in connection with other disasters. Extreme heat is the nation’s leading cause of weather-related deaths. Through this challenge, DHS is working to advance climate resilience and further increase equity in its preparedness and response efforts as underserved communities are disproportionately impacted by extreme heat.

DHS will create new incentives for resilience and adaptation. We are modernizing our grant programs to address the threat environment we now face. FEMA’s Building Resilient Infrastructure and Communities program holds great promise, and we will support the scaling of this program to provide communities the resources to make necessary investments to build resilience at the local level. Together with FEMA’s Flood Mitigation Assistance and Hazard Mitigation Grant Programs, we must make resources accessible to all communities, including those in underserved areas, to empower them to take actions that reduce risk and increase resilience to environmental threats to life and property.

While we work to develop community resilience, we must also create the response capabilities

that the nation needs in this new era of climate change-exacerbated natural disasters. Due to the effects of climate change, there will be no off-season for disasters. Increasingly, DHS Components are responding year-round to severe weather events and other climate-related disasters, placing great strain on resources and personnel. To succeed in this environment, we will create a workforce structure that can function on a sustainable deployment and reset cycle, strengthen the capabilities of the National Response Coordination Center and Regional Response Coordination Centers, and establish a robust, integrated surge force capable of rapidly responding year-round to events.



The impacts of climate change, including food and water shortages, together with poor economic conditions are also likely to increase population movements from Mexico, Central America, South America, and the Caribbean, impacting neighboring countries. Increases in human migration will require more resources and operational capacity at U.S. borders to facilitate the application of immigration law, including the claims for humanitarian protection. DHS will work closely with USAID

and the Department of State to expand our capabilities to provide climate change adaptation expertise to build the resilience of impacted countries.

Climate change also demands that DHS and its Components adapt regulations. For example, the USCG is supporting industry adoption and use of green technologies while ensuring safety and sustainability of the marine transportation system. Using existing regulatory authorities,

Driving Equitable Outcomes for Communities Facing Disasters

It is DHS's responsibility to ensure that preparedness resources reach communities fairly and equitably and that response and recovery efforts recognize the needs and different circumstances of particular communities. Recently, FEMA changed the acceptable forms of documentation to make it easier to prove home ownership and occupancy. This change reduced barriers for obtaining rebuilding funds and promoted access for homeowners in communities that were disproportionately impacted by past requirements, as some homeowners in the South and U.S. territories live on inherited land that lacks documentation. FEMA has also taken steps to reduce barriers to financial assistance and grants so they can be accessed by underserved communities.

The COVID-19 vaccination mission highlighted FEMA's use of tools such as the Centers for Disease Control and Prevention's Social Vulnerability Index to drive equitable outcomes. FEMA has also used this and other data to expand equity in DHS's Individual Assistance program. FEMA has also expanded available assistance and is now providing limited financial assistance to survivors with property damage, even if their homes are not rendered uninhabitable. For example, DHS can now provide financial assistance for minimal repairs or to clean and sanitize a home to protect the health and safety of the household. FEMA has also begun conducting direct outreach to disaster assistance applicants who continue to be ineligible due to occupancy or ownership verification to assist them with navigating the document submission processes. FEMA first piloted this tailored approach in Michigan in 2021 and is now using this approach in Louisiana. With this direct outreach and reducing barriers in the application process, thousands of additional survivors are now eligible and able to apply for assistance.

this has already enabled the design, construction, and certification of the first hydrogen-powered ferry and has helped pave the way for future development of zero-emission vessels.

The effects of climate change will also continue to be felt in the Arctic, where thawing permafrost and melting polar ice will lead to increased commercial, military, and other activity while simultaneously degrading fixed infrastructure such as roads and aviation facilities. Climate-induced changes in the region will broaden the Department's roles related to stewardship, safety, scientific support, and strategic competition. As such, we will continue developing capabilities, enhancing collaboration with government partners in the region, and increasing our capacity to operate in an increasingly active and competitive environment.

DHS is focused on reducing our carbon footprint and integrating the resilience of our mission essential assets to reduce vulnerabilities to aid our personnel to carry out our mission. We have developed a robust resilience, energy, water, and sustainability management program in which we are making all our facilities sustainable, energy efficient, and as resilient as possible. This includes assessing our critical sites to reduce energy consumption, conserve water, and reduce the use of fossil fuels through integration of best practices, innovative processes, and technology. To support the

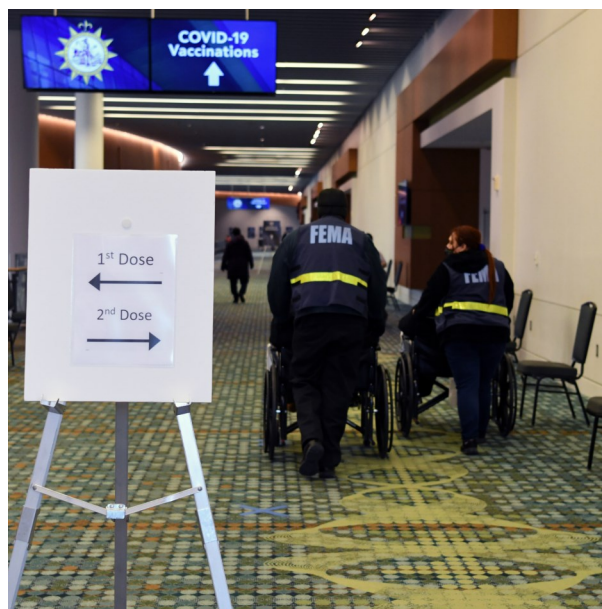
adoption of electric vehicles, we are assessing the electric vehicle capability at our sites. DHS was the first Department within the Federal Government to announce an aggressive goal to convert 50 percent of our 26,000-vehicle fleet to electric vehicles by 2030. Currently, 65 percent of the Department's greenhouse gas emissions are mobile fuels. Therefore, integrating electric vehicles into the DHS fleet supports reshaping the transportation sector and contributing to the reduction of carbon emissions.

The focus on environmental justice and racial equity is of utmost importance to the Department. In August 2011, DHS confirmed its commitment to environmental justice by signing the *Memorandum of Understanding on Environmental Justice*. This memorandum commits DHS to comply with E.O. 12898, *Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations*, by fully integrating environmental justice into its operations.²³ DHS is prioritizing programs and projects based on their contribution to resilience, sustainability, energy, water efficiency, and benefit to historically disadvantaged communities with environmental justice concerns, while supporting the execution of DHS missions. We will continue to identify and consider potential effects of DHS's actions to ensure there is not a disproportionate impact on low-income, minority populations.

Emerging Infectious Diseases

The interconnected world of international commerce and travel has made every nation susceptible to infectious diseases that emerge outside their borders. Infectious diseases transcend geographic and political boundaries, may be exacerbated by the impacts of climate change, and thus constitute a global threat that places the homeland at risk. Past global health crises, such as the 2013-2016 West African Ebola Virus Epidemic, the 2014-2015 Highly Pathogenic Avian Influenza Epidemic, the 2015-2016 Zika Virus Outbreak, the novel H1N1 Influenza Pandemic in 2009, and the ongoing H5N1 Avian Influenza outbreak have demonstrated the ability of infectious diseases to destabilize populations and economies. The COVID-19 pandemic continues to impact public health and the economy and highlights the need to improve our ability to detect, prevent, prepare for, respond to, recover from, and build resilience to pandemics and future biological threats, consistent with the goals of the 2022 National Biodefense Strategy.²⁴

As we welcomed new populations into the country, including record numbers of unaccompanied children in south Texas and Afghan nationals as part of OAW, COVID-related health and safety requirements and protocols became a key factor for both vulnerable populations as well as our own workforce. Through Operation Vaccinate Our Workforce,



DHS, in partnership with the Veterans Administration, provided COVID-19 vaccinations to over 75,000 frontline and mission-critical personnel. Additionally, the Department has provided over 500,000 COVID and influenza vaccinations to migrants processed under Title 8 authority. OAW operations were severely disrupted due to a measles outbreak, highlighting the large impact of vaccine-preventable diseases in under-immunized populations. The events of 2022 also required increased prevention and surveillance activities to enhance our preparedness for emergency response to global outbreaks of Ebola, African Swine Fever, and H5N1 Avian Influenza. Over the next four years, naturally occurring, accidental, and intentionally introduced biological and infectious disease threats will continue to be a key driver of homeland security risks that endanger the safety, health security, and resilience of the nation and our way of life.

DHS has played an important role in the whole-of-government and whole-of-community approaches to preventing and mitigating the adverse effects of public health emergencies, including coordinating the national response to the COVID-19 pandemic under the first-ever nationwide emergency declaration under the Stafford Act.²⁵ DHS secured and facilitated trade and travel to and from the United States, provided national emergency relief aid, including the 2021 mass vaccination campaign co-led by FEMA and HHS, and ensured the ongoing functionality of critical infrastructure. As the country continues to respond to and recover from COVID-19, concerns mount over the potential for future pandemics given the combination of increased human presence in wildlife habitats, people in close contact with animals, climate change, and the high probability for the rapid and broad spread of infectious disease through global commerce and travel. We must do more to effectively mitigate the impacts of future pandemics by working with our partners, including HHS, to promote robust health security and incident management processes and facilitate close coordination and engagement between SLTT government and private sector actors.

DHS must execute its homeland security operations while adapting to pandemic conditions to keep our employees safe and mission ready. DHS's frontline operators continue to execute critical missions, including inspecting cargo, managing immigration flows,

screening travelers, performing search and rescue, conducting protective details, and distributing aid and relief during natural disasters. Biological incidents overlay complex issues across homeland security missions and may require changes in Concepts of Operations (CONOPSs), as well as safety equipment and temporary protocols, to ensure the health and safety of the DHS workforce and the public. For example, during the COVID-19 pandemic, DHS supported the implementation of temporary travel restrictions, social distancing measures, and telework capabilities; facilitated and enabled the distribution of medical countermeasures; coordinated with HHS to provide medical personnel to support state, tribal, and territorial requests for federal assistance; and supported basic research to characterize the new virus and develop decontamination methods. Ensuring resilience and continuity of operations across the Department during a pandemic or other public health emergency requires adaptability and more robust measures to ensure the health readiness of the DHS workforce. DHS will continue to invest in capabilities that can ensure mission success and implement policies and procedures that can be applied to respond rapidly when a pandemic or health emergency occurs.

DHS was also involved in direct pandemic response efforts including coordinating and collaborating with HHS to help identify and detect public health threats early; detecting

potential biological threats and sharing information with the homeland security enterprise through the National Biosurveillance Integration Center; and facilitating the mobilization and distribution of national resources and supply chains to reach local communities. DHS worked with SLTT authorities and private sector partners, both directly and in coordination with federal partners, to assist with funding to support response efforts. To date, DHS has provided more than \$89.6 billion in COVID-19 assistance, including over \$7 billion for vaccination support. Throughout 2021, DHS, in coordination and collaboration with HHS, executed a national mass vaccination campaign that administered more than 5.6 million doses of COVID-19 vaccines. FEMA also provided nearly \$2.8 billion in reimbursements for funeral-related costs for deaths due to COVID-19 to more than 435,000 individuals. FEMA also activated the

National Response Coordination Center to help coordinate the response. DHS will continue to build relationships with SLTT partners to ensure information sharing on public health threats as well as to maintain situational awareness on supply chain needs.

To prioritize and strengthen this work, DHS, with the support of Congress, created the Office of Health Security (OHS), which leads DHS efforts in close coordination with partners including federal agencies, the private sector, state and local governments, health providers, and others, to build resiliency for public health crises. These partnerships begin with our work with HHS to build the capacity to manage complex incidents like COVID-19, as well as to develop better pandemic resilience planning across all federal agencies. We must also improve how we use data to understand, anticipate, and assess the homeland security

Vaccination Centers

DHS has played a vital role in coordinating vaccination distribution and access for the COVID-19 national response by establishing vaccination centers nationwide. On the first day of the Biden Administration, the President directed FEMA to stand up 100 new federally supported community vaccination centers in just 30 days. FEMA and the broader DHS enterprise rose to this challenge, establishing not 100, but 441 vaccination centers in that time. By mid-2022, that number grew to more than 3,600 locations nationwide. The President also set a goal for FEMA to support the administration of 100 million vaccinations in 100 days. FEMA met that goal in just 58 days and supported administration of more than 217 million vaccinations by day 100. Developing this critical health infrastructure in tandem with the mass national vaccination campaign was instrumental in facilitating its rollout. FEMA and DHS continue to strengthen pandemic response capacity through this initiative.

Office of Health Security

Since early 2020, the Department has managed a wide range of medical and public health responses, including: a variety of health issues associated with OAW; contributing significantly to the nation's COVID-19 pandemic response; leading "Operation Vaccinate Our Workforce" for DHS employees; managing a significant increase in unaccompanied children arriving at the Southwest Border; and addressing the increased prevalence and impact of natural disasters. Lessons from these efforts reinforce the need to consolidate and streamline health security activities within DHS.

To meet the current and future challenges in this space, the Department created OHS, which serves as the principal medical, workforce health and safety, and public health authority for DHS. Led by DHS's Chief Medical Officer, OHS strengthens the nation's health security through leadership and partnership, a safer and healthier DHS workforce, and optimal care for those entrusted to us. The Office will build resiliency, prevention systems, and the capacity to be nimble as public health needs arise. In doing so, OHS enables coordination, standardization, and accountability across the homeland security enterprise while helping enhance our workforce and nation's preparedness, response, and resilience to the health impacts of terrorism and other disasters.

risk of public health challenges and share that information with SLTT authorities to enable them to be anticipatory.

DHS will be nimble in our response. DHS must be able to operationalize responses to public health challenges, such as deploying medical personnel to conduct health screenings for refugees arriving from abroad and screening travelers using "touchless" technologies. DHS must also be prepared to enhance cybersecurity of digital systems crucial to pandemic response. These capabilities will allow us to be agile and responsive to the many ways public health challenges affect the homeland and to support state and local communities.

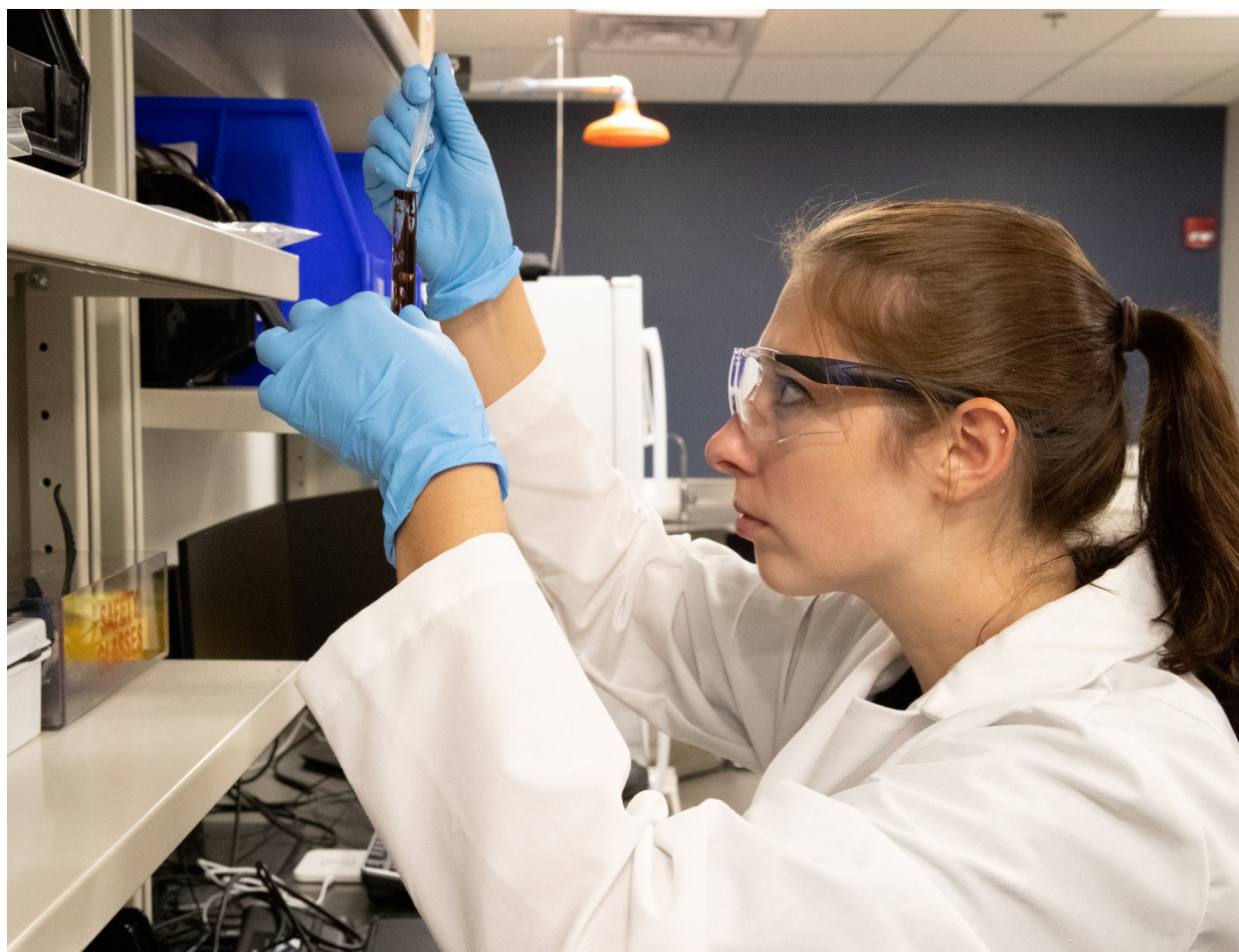
DHS will also prioritize contributing to the national risk communications effort to ensure that stakeholders, whether security officials or critical infrastructure owners and operators, have an accurate understanding of the potential effects of a pandemic and that there are proactive and transparent communications between the Department and its partners. DHS can also help disseminate U.S. Government messaging during a pandemic response.

The COVID-19 pandemic has demonstrated the devastating impacts of a biological incident, including loss of life and extreme economic and social disruption. DHS must remain vigilant against the full spectrum of biological threats,

including those caused by unintentional events, such as a laboratory accident, or by actors who wish to do harm, such as nations pursuing clandestine biological weapons programs and terrorist groups seeking to acquire and weaponize biological agents.

Further, the world is on the cusp of a biological revolution that will bring exciting technologies and cures, but also new risks and new threats. DHS will work to counter the potential for intentional misuse and unintentional outcomes through the following priority actions: 1) leverage the latest science and technology to advance the mission and protect the workforce

while partnering with the interagency on the development of sound policies addressing novel technologies and dual-use concerns; 2) develop and update threat-informed risk assessments to drive DHS decision-making and resource allocations while ensuring SLTT partners' awareness and education; and 3) continue to mature and invest in OHS to ensure a safer workforce, optimal care for those in our custody and to improve the Department's diverse supporting role within the national response framework.



Complex and Interconnected Incidents

The homeland security enterprise will be called upon to respond to increasingly complex, simultaneous, and interconnected incidents. Just in the past two years, DHS responded to incidents ranging from the COVID-19 pandemic, irregular migration at the Southwest Border, ransomware and other cyber incidents impacting critical infrastructure, and the rapid resettlement of thousands of vulnerable Afghan evacuees through OAW. DHS was also designated by the President as the lead federal agency to coordinate domestic preparedness and response efforts in the wake of Russia's 2022 invasion of Ukraine. In each of these cases, the response required integrating authorities and capabilities in novel ways across DHS Components as well as other federal agencies, SLTT partners, and even nongovernmental entities. At the same time, the Department has had to confront 'traditional' incident responses of intensifying scale and frequency, including the record-setting 2020 Atlantic hurricane season, the unprecedented 2021 wildfire season, a violent tornado outbreak in Kentucky in December 2021, and the widespread impacts of Hurricanes Ida and Ian, in 2021 and 2022 respectively. In isolation, each incident requires decisive action and incident management expertise. Combined, they have an expanding series of unpredictable consequences ranging from loss of life to severe supply chain disruptions.



Multi-domain, cross-functional responses are becoming increasingly frequent, as deepening supply chain integration and cyber vulnerabilities across critical infrastructure create a situation where disruptions have the potential to escalate into high-impact incidents that necessitate DHS response within potentially degraded or challenging operating environments. For example, the May 2021 Colonial Pipeline ransomware incident quickly escalated from a ransomware incident impacting a billing system to an incident with national consequences. Public fears over fuel supply drove up consumer demand for gasoline and resulted in shortages across the eastern half of the United States. The disruption highlighted the need for TSA to issue security directives raising the level of security and preparedness of the pipeline sector. Secretary Mayorkas granted Jones Act²⁶ waivers to permit rapid shipments of fuel to remedy near-term shortages. Ultimately, the incident required

Operation Allies Welcome

In August 2021, President Biden directed DHS to lead and coordinate efforts across the Federal Government to support vulnerable Afghans, including those who worked alongside us in Afghanistan for the past two decades, as they safely resettle in the United States. DHS worked with representatives across the Departments of Defense and State, HHS, and other government agencies to coordinate our response and ensure unity of effort, deploying approximately 400 DHS personnel from multiple Components around the world to support OAW. Supported by other federal agencies, this facilitated the efficient screening and vetting of individuals evacuated with dual goals of protecting the homeland and providing protections for vulnerable Afghans.

During OAW, DHS worked in close collaboration with partners in state and local government, NGOs, and the private sector to ensure a safe resettlement of more than 88,000 Afghan nationals who worked for the United States, as well as other vulnerable Afghans. The Federal Government utilized eight Department of Defense installations throughout OAW to temporarily house vulnerable Afghans, including those who are Special Immigrant Visa applicants, while they awaited resettlement in our communities. The last Afghan nationals temporarily housed on a Department of Defense installation departed in February 2022, and in September 2022, the last safe haven facility at the National Conference Center in Leesburg, Virginia, witnessed the last Afghan nationals depart to resettle in communities across the United States.

responses across DHS's mission areas and Components, including CBP, CISA, FEMA, TSA, and the USCG.

Multi-domain incidents will not be limited to the ripple effects of disruptions to critical infrastructure or cyber incidents. For example, OAW required DHS to lead a whole-of-government effort to evacuate and resettle vulnerable Afghans in the United States. The resources needed to prepare vulnerable Afghans for resettlement once in the United States strained not only existing resources but also the missions and services typically

provided by government agencies. OAW, which itself would have been a once-in-a-lifetime challenge for the enterprise, came on top of numerous other incidents, a scenario for which we must be prepared going forward.

The challenge is the complexity not only of handling any one incident but of managing several at the same time. The combined demand of these national responses placed an unprecedented strain on the Department's incident management personnel. Traditional deployable forces were quickly exhausted, and the Department had to leverage non-traditional

DHS's Response to Russia's Invasion of Ukraine

DHS remains committed to supporting the Ukrainian people and to honoring the United States' commitment to provide humanitarian relief to those who are fleeing Russia's unprovoked war. President Biden designated DHS as the lead federal agency to coordinate domestic preparedness and response efforts related to the current Russian-Ukrainian crisis. In response, DHS has launched numerous efforts, including U4U (for more information see page 14), Shields Up, and the DP&R UCG, in close collaboration with international partners.

When it became clear that Russia was planning its 2022 invasion of Ukraine, DHS and CISA mobilized the private sector to harden its cyber defenses proactively against disruptive Russian retaliatory or spillover actions through a public awareness campaign called Shields Up, the largest effort of its kind in history. DHS shared threat information broadly and in real time with our public and private sector partners, and we identified and mitigated vulnerabilities. These ongoing efforts are important for the homeland security enterprise to reduce the likelihood of a damaging cyber intrusion, including taking steps to detect a potential intrusion quickly, ensuring that the organization is prepared to respond if an intrusion occurs, and maximizing the organization's resilience to a destructive cyber incident.

The Department also leads the Domestic Preparedness and Response Unified Coordination Group (DP&R UCG) established in response to Russia's 2022 invasion of Ukraine. Leveraging the lessons learned from the COVID-19 response, OAW, and the Colonial Pipeline incident, DHS established coordination mechanisms between CISA's cyber response and critical infrastructure protection activities and FEMA's physical consequence management and federal continuity activities, engaging SRMAs, the Intelligence Community, and other federal partners to develop integrated plans for how the U.S. Government will respond to such incidents in the future. In particular, the DP&R UCG worked with federal partners to identify critical infrastructure interdependencies between federal departments and agencies having national security-related mission sets and key homeland security enterprise partners, such as SLTT governments and the private sector.

The staff detailed to the DP&R UCG were drawn from 14 DHS offices and agencies and SRMAs. The DP&R UCG integrated FEMA's incident management expertise with CISA's cyber and critical infrastructure expertise, providing the U.S. Government with a common situational awareness of current threats and related mitigation, preparedness, and federal mission resilience activities. Many of the coordination mechanisms and plans developed through the DP&R UCG will endure, both within DHS and across federal agencies, such as exchanges on infrastructure impact analysis, cyber threat reporting, and leveraging sector expertise to exercise consequence management response plans.

combinations of forces, including large numbers of FEMA and USCG personnel, to support these critical missions.

Over the next four years, DHS will have to respond to multi-domain incidents stretching across its operational Components. DHS must

be able to leverage its collective expertise and capabilities to directly manage all types of incidents, including those that invoke multiple responsibilities and authorities from across the Department, and to support incident response efforts led by other agencies.

Incident Management

Over the last several years the Department has gained substantial experience in coordinating responses to a variety of “new” and complex incidents—the COVID-19 response, OAW, the Colonial Pipeline incident, Mpox, and in leading the DP&R UCG established in response to Russia’s 2022 invasion of Ukraine.

These incidents have demonstrated the increasingly complex, simultaneous, and interconnected nature of incidents and incident management. The challenges we face are more intense, complex, and frequent than ever before. DHS must be able to leverage its collective expertise and capabilities to manage all types of incidents directly, including those that invoke multiple responsibilities and authorities from across the Department, and to support incident response efforts led by other agencies. DHS must also enhance its institutional capacity to coordinate incident responses that fall between or across the scope of Component authorities.

To support these efforts, DHS is enhancing its Department-wide incident management capabilities. The Department is leveraging current capabilities and establishing a workable CONOPS for its reserve and surge capacities, including the DHS Surge Capacity Force, the DHS Volunteer Force, and the USCG Reserves and Auxiliary, and shift to a continuous cycle of planning, organizing, equipping, training, and exercising.

The Department is also readying its entire workforce—not only those already trained in the National Incident Management System—to execute these incident management capabilities as well as regularly exercise and develop them alongside other federal, SLTT, and nongovernmental partners. With support from Congress, DHS created the new Homeland Security Incident Management Assistance Team which will support these incidents at the Secretary’s direction and coordinate the Department’s resources for response efforts. DHS is also training our workforce to take on leadership roles in future response efforts with the first Homeland Security Incident Senior Coordinating Official and Senior Response Official Cohort.

By normalizing interoperability, the entire homeland security enterprise can be capable of delivering the incident responses the nation deserves.

DHS must also enhance its institutional capacity to coordinate incident responses that fall between or across the scope of Component authorities. Building on the experiences of the OAW and the DP&R UCG, the Department can develop CONOPS for dedicated incident management task forces or unified coordination groups. DHS will develop a more integrated response capability matching the increasingly

interconnected incident consequences, starting with the new Homeland Security Incident Management Assistance Team and the new training program for Senior Coordinating Officials and Senior Response Officials. This will include enhanced external affairs and strategic communications functions, a key role for DHS during an incident.



Strengthening the Enterprise

DHS will continue to build its capacity to conduct its critical missions and anticipate the challenges to come. Essential to this is better understanding and protecting against threats from emerging technologies, as well as developing our most important assets: people, physical assets, data, and technology.

Emerging Technologies

In the coming years, advancements in emerging technologies present considerable opportunities for improvements in commercial activity, public health, critical infrastructure network connectivity, and aviation security. These advancements include trustworthy artificial intelligence (AI), quantum information

science, advanced communications technologies, microelectronics, nanotechnology, high-performance computing, biotechnology and biomanufacturing, robotics, advanced manufacturing, financial technologies, undersea technologies, and space technologies. When deployed with robust security and privacy



by design, they also present opportunities for DHS to adopt new and emerging technology to operate more effectively and improve customer experience.

Deployment

DHS will focus on developing and deploying new technologies and capabilities to execute our missions efficiently and effectively. DHS must also be a leader in the responsible use and adoption of emerging technologies, including AI and biometric capabilities. DHS issued its *Artificial Intelligence Strategy*²⁷ to promote the trustworthy use of AI across the Department in 2020, and in 2021, DHS issued a roadmap to prepare organizations for the transition to post-

quantum cryptography. DHS is also working to deploy next-generation passenger screening technology at airports, leveraging advancements in identity management to improve the passenger vetting process, and evolutions in screening equipment capability to improve security and enable a fluid, frictionless passenger experience.

At the same time, we must be alert to the ways in which threat actors could leverage such technologies and develop the necessary policies and means to mitigate those risks. For example, the threat landscape from unmanned aircraft systems (UAS) is concerning as the technology continues to evolve. UAS have been

Digitization

DHS is fully leveraging digitization and automation to reduce the amount of time our employees spend on manual, repetitive tasks and increase the time they spent on their critical homeland security missions. Saving agent and officer time processing cases gets our frontline workforce back into the field executing their security mission instead of completing paperwork that can be automated.

One example of this is the Southwest Border Technology Integration Program. DHS and its Components have made significant progress automating and digitizing immigration processes and border encounter information. This begins in the field where CBP's Mobile Intake application allows agents to begin intake processes in the field when they encounter a noncitizen. This saves time during future processing and strengthens officer safety by allowing for earlier identification of potential risks. Throughout the process, digitization of signatures and paperwork review have reduced the amount of time it takes Border Patrol agents to process a case by at least 10 minutes. Transferring cases and noncitizen A-files electronically, as opposed to sending files through the mail, significantly accelerates numerous DHS processing activities. In the next year, DHS will achieve fully electronic case files for the vast majority of new Southwest Border encounters, getting paper out of the process and delivering a modern, flexible system.

used to conduct kinetic attacks, interfere with aircraft and airports, and surveil, disrupt, and damage critical infrastructure and services. DHS will continue to test, train, and integrate new UAS detection and mitigation equipment to protect the homeland in collaboration with the Federal Aviation Administration and interagency partners. We will work with Congress and collaborate with the Federal Aviation Administration to sustain and expand the Department's authorities to counter UAS threats, including enhancing TSA's ability to protect airports and support limited use of counter-UAS technology by SLTT law enforcement and critical infrastructure partners. The ability of the private sector, and federal, state, and local governments to mitigate the risks drones create depends on legislation to reauthorize and expand such authorities. This initiative requires interagency collaboration to ensure safeguards and oversight to protect the safety of the National Airspace System, privacy, civil rights, and civil liberties.

As these technologies are evolving at different paces and are at different levels of maturity, over the next four years, DHS will scout, invest, and collaborate to fulfill our missions and must develop new approaches to engagement that meet the pace of business and technological change. DHS will continue expanding its technology scouting efforts to understand new developments from the private sector. Simultaneously, the Department will increase its engagement with interagency and

international partners who invest in research that could enhance or disrupt future capabilities. We will build this work on direct, open, and trusted relationships to leverage insights and innovations wherever they emerge through DHS's broad network of partners including industry, other federal agencies, academia, and international entities. DHS will leverage opportunities to participate in several international technology standard-setting processes, the outcomes of which will impact DHS's missions. DHS will also continue to broaden our non-traditional partners, understanding that entities with limited Federal Government engagement are often uniquely poised to bring novel solutions to support operational needs. DHS will also ensure that these technologies are developed, used, and continually assessed in ways that ensure equity.

Recognizing the value of science to many aspects of the homeland security mission, the Department will seek to expand its work in foundational and emerging research. Further, to get solutions into the hands of operators, we must develop new business opportunities to promote technology transfer and commercialization of DHS-funded research. DHS's ability to eliminate or reduce gaps in transitioning from innovation to deployment will benefit the entire homeland security enterprise, increasing mission effectiveness and supporting a distinct market for homeland security solutions.

For innovators, DHS's efforts will close the so-called "valley of death," where small businesses struggle to transition from research and development programs to sustained operational use of their technologies. We will also continue to support programs, such as the Homeland Security Startup Studio, that pair industry experts with government researchers to deliver

technology solutions. These programs are already delivering results. In 2022, nine of the 10 Homeland Security Startup Studio entrepreneurial teams completed the 18-week program and they continue to build early-stage companies to commercialize DHS-relevant technologies.

Responsible Use of Artificial Intelligence and Machine Learning

DHS must be a leader in the responsible use and adaptation of emerging technologies, including applying AI and machine learning (ML) to DHS missions. DHS issued its AI strategy in 2020 to promote the trustworthy use of AI across the Department. The DHS AI/ML Inventory, which includes information on over 80 AI projects and use cases, is a key milestone in the progress the agency is making towards improving the quality, accuracy, and speed of collecting, processing, analyzing, reporting, and securing its data.

Responsible use of AI and ML is already presenting significant benefits to DHS operations. USCIS has, for the past two years, used its Digital Evidence Viewer to tag high-volume and high-impact evidence with ML systematically so that case workers can more quickly find documents of interest, saving officers from spending hours sifting through documents to find one specific artifact.

As DHS realizes operational and customer experience benefits from AI and ML and other emerging technologies, the Department will also be vigilant in guarding against the ways in which these technologies introduce potential vectors for risk and abuse, including continuous assessment for bias and potential discrimination in the use of facial recognition tools. The Department will continue to ensure through rigorous governance, monitoring, and internal and outside technical reviews, as well as testing and validation studies, that technologies are safe and effective, free from bias and discrimination including disparate treatment, disparate impact, and other forms of algorithmic bias, ensure data privacy and control, provide transparency in how and why data is used, and maintain appropriate levels of human oversight and intervention. We will continue to ensure that appropriate governance mechanisms are in place to protect privacy, civil rights, and civil liberties, in the development and adoption of new technology, and put into place strong processes to govern and monitor their use.

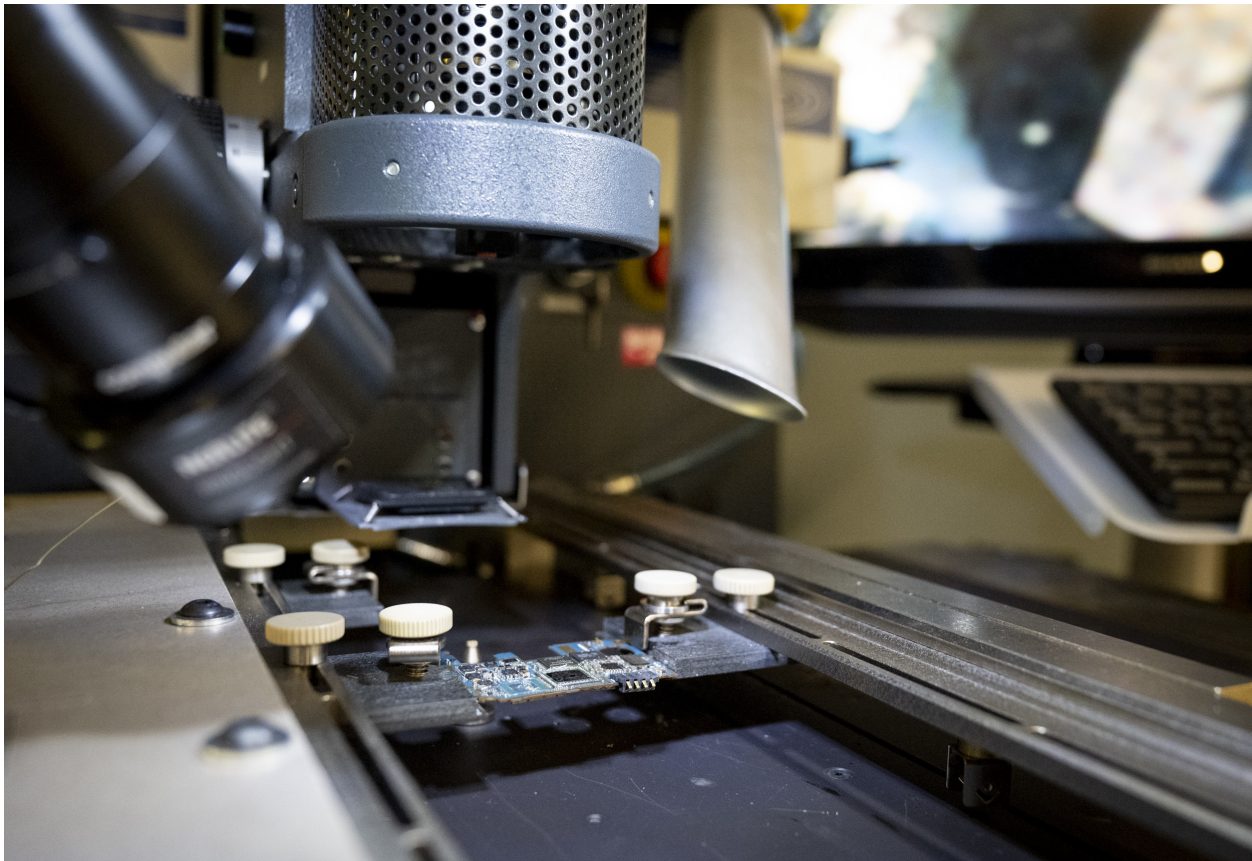
Innovation

Critical to our ability to deploy new technologies is opening more avenues for innovation. DHS requires strong partnerships to discover scientific advancements and technology innovations that address homeland security challenges. Understanding the diversity of potential partners, DHS offers a variety of research and development funding programs to encourage a unique group of innovators.

An example of this commitment is DHS's focus on small businesses and startups, whether they are developing products not yet on the market or offer fully commercialized capabilities that can be adapted for homeland security use. The Silicon Valley Innovation Program (SVIP), DHS's

Small Business Innovation Research (SBIR) programs; and CBP, S&T, and TSA's relationship with In-Q-Tel focus on bringing non-traditional performers with innovative ideas to tackle the toughest DHS challenges. SVIP streamlines S&T's access to innovators using Other Transaction Authority to make government awards on an accelerated timeline. Other Transaction Authority is currently an annual renewal that is subject to lapses, and that uncertainty provides challenges to those small businesses S&T is relying upon to execute the Department's missions.

SVIP began six years ago in California's tech corridor, but now has a global footprint and has successfully identified, developed, and



deployed technology in support of DHS's missions. As of this year, SVIP has provided funding to 71 startups, delivered nine solutions, and has three more solutions at operational pilot stage. These final-phase pilots include advanced ground-based radar focused on detecting non-traditional targets like drones, as well as ML and entity resolution capabilities that link CBP importer data to other large datasets to better inform risk assessments. SVIP reduces risk and lowers the barrier to drive commercial startup technologies using innovative contracting authorities and continues to deliver innovation to our operators in the field.

DHS uses prize competitions to crowdsource innovation and harness the creativity of the

American public to solve difficult homeland security challenges. Competitions provide a direct path and clear incentives for all types of innovators who want to share their ideas but, in many cases, may view working with the government as confusing or time consuming. The recent "Cooling Solutions Challenge" prize competition awarded a total of \$195,000 in prize funding to winners for their innovative, climate-friendly ideas to help first responders, individuals, households, and displaced populations keep cool during extreme heat events. S&T will continue to work with competition winners to help them develop their technology solutions. The DHS SBIR Program, a three-phase competitive award program, provides qualified small businesses with opportunities to propose innovative ideas that

Openness and Transparency

DHS must uphold our nation's highest values, making us worthy of trust from the public we serve. Accomplishing our mission requires a steadfast commitment to protecting civil rights, civil liberties, and privacy. These values are essential to our ability to succeed in our mission to secure the homeland. Incorporating these protections must begin in the earliest stages of development of policy, program design, operational plans, and assessments and must continue throughout the entire life cycle of these activities.

The Department's Office for Civil Rights and Civil Liberties and Privacy Office have statutory missions to lead this vital work across the Department. We will support efforts, whether through statute or Departmental guidance, to further codify and expand the role these offices play to ensure our rights and liberties are protected, including efforts to mature the civil liberties infrastructure and to strengthen their input across DHS. Our policymaking and operational decision-making processes will continue to incorporate oversight and protection—including for intelligence collection and analysis, combatting domestic violent extremism, watchlisting processes, immigration enforcement activities, as well as the deployment of law enforcement personnel—to provide security while protecting individual rights and liberties.

meet specific homeland security research and development technology needs. As of fiscal year 2022, the DHS SBIR Program has funded 790 Phase I awards, 378 Phase II awards, and over 200 Phase III awards.

Privacy, Civil Rights, and Civil Liberties

Underlying this need to adopt new technologies to enhance homeland security is the need to protect privacy, civil rights, and civil liberties. Transparency is key to using emerging technologies in a trustworthy manner. We are continually reviewing and assessing our use of emerging technologies across the Department. We will ensure that appropriate governance mechanisms are in place to consider privacy, civil rights, and civil liberties, as well as other implications of new technology. Governance of emerging technology adoption begins with

understanding the provenance of information and technology at the outset, then putting in place strong processes to oversee their use.

Governance alone is insufficient: the Department must build privacy safeguards into the processes we develop to leverage data and must apply privacy-enhancing technology. DHS is exploring the uses of mathematically-based, privacy-enhancing technologies, such as differential privacy, to make use of personal information for mission purposes while simultaneously preventing the data from being used for unauthorized, non-mission purposes.

Freedom of Information Act Compliance

DHS is firmly committed to upholding the core ideal of accountability to the public while fulfilling its critical homeland security missions as guardians of people's safety and security. One of the Department's priorities is to increase openness and accountability. The *Freedom of Information Act* (FOIA) is an important element of advancing that objective as it enables journalists, researchers, academics, and the general public to better understand DHS activities.

DHS maintains, by far, the largest FOIA program in the Federal Government. Some DHS Components regularly receive more FOIA requests than other Cabinet-level agencies. Overall, DHS accounts for 56 percent of all FOIA requests across the government. Over the course of fiscal year 2021, the Department responded to a record-breaking 467,347 requests. At the same time, DHS reduced its FOIA backlog by 30 percent, reaching the lowest level in nearly a decade. The Department is working to eliminate the backlog entirely and will continue our efforts to be as transparent as possible.

Building the Department's Capacity

As the threats and challenges that DHS will confront over the next 20 years will differ from those of the first 20 years, so too must the homeland security enterprise strengthen, mature, and align to meet them. This requires significant actions to support, empower, and promote our people and enhance our assets, beginning with our most precious asset, our people, and extending to the Department's physical assets, data, and technology.

People

The DHS workforce, together with our partners across the homeland security enterprise, is the core of the homeland security mission. The Department is committed to strengthening the homeland security enterprise by increasing workforce morale; improving recruitment, hiring, and retention efforts; enhancing career development opportunities; and improving performance management. DHS will make long-term investments in the health and well-being of our workforce, including suicide prevention resources, ensuring collective bargaining rights, and improving compensation structures for frontline workers contributing to our safety and security.

The more than 260,000 people that make up the DHS workforce answer the call every day to defend the homeland (see Fig. 2). Across the Department that is responsible for some of the



most difficult and important missions in the government, it is the dedication, skill, and integrity of our people that enable us to accomplish all that we do. As such, the Department is instituting DHS Professional-Public Service Ethos training, which will serve as the foundation of our workforce training, with the goal to instill in each member of the workforce a profound understanding of their part in a DHS culture that is dedicated to public service and trustworthy stewardship as we carry out DHS's missions with transparency and accountability.

The DHS workforce includes²⁸:

- 52,537 military veterans;
- 88,652 law enforcement officers²⁹;
- 1,656 personnel stationed abroad³⁰;
- 151,522 frontline workers³¹; and
- 44,813 uniformed military personnel.

Law Enforcement at DHS

DHS's over 88,000 law enforcement personnel serve honorably to protect America's communities, often at great personal risk. Our officers enforce the law with honor and integrity to advance justice while realizing our nation's ideals. To earn and maintain public trust as we protect the homeland, the Department is committed to transparency and accountability. To this end, DHS has established formal bodies, including the Law Enforcement Coordination Council, to build on the Department's longstanding commitment to achieving consistency and transparency in our law enforcement missions. Further, the Department has updated our policies and practices to ensure they are consistent with the law, align with best practices, and protect privacy, civil liberties, and civil rights. Much of this work takes the form of implementing 36 requirements in the E.O. on *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*.³²

It also takes the form of strengthened oversight and policy offices—including the Office for Civil Rights and Civil Liberties and Privacy Office—that are working to ensure that the Department's law enforcement activities are conducted in a lawful manner that respects rights. The integrity of our law enforcement workforce is also paramount; the Department is undertaking multiple reviews to ensure that discipline is consistently and correctly applied in investigations of officer misconduct. This includes work by the new Office of the Immigration Detention Ombudsman to address complaints lodged at custody and detention locations throughout the country and the DHS Public Complaint and Feedback System Working Group.

The DHS workforce is among the most diverse in the Federal Government, with 47 percent who are ethnically or racially diverse.

Investment in the workforce includes efforts to strengthen diversity, equity, inclusion, and accessibility at DHS to ensure the DHS workforce and its leadership are as diverse as the country we serve. Although DHS is diverse writ-large, we face challenges in key areas including a gender imbalance in law enforcement and cybersecurity.

We will borrow best practices from the private sector and academia and, given the wide range

of circumstances across the DHS workforce, we will empower frontline supervisors to address problems locally and will prioritize performance management. Specifically, the Department will focus on improving performance management IT systems, building a culture of continuous feedback, and updating performance management guidance to incentivize collaboration and reflection of the Department's values by all employees. The Department will follow best practices and equity in the development and use of these performance management systems. In addition, DHS is working to ensure that its workforce, and its

leadership, represents the diversity of the nation it protects by ensuring targeted outreach efforts to underserved communities and communities of color.

DHS recognizes that a diverse workforce creates opportunities for creativity, innovation, and engagement, and has programs and initiatives in place to foster them. DHS is committed to providing employment opportunities for all segments of society. The Department prides itself on offering robust opportunities to recruit talent using a variety of student and entry-level programs. The DHS *Inclusive Diversity Strategic Plan*³³ captures the spirit of the Department’s approach to diversity, equity, inclusion, and accessibility: putting our

people first to elevate the human experience at DHS. Now, more than ever, DHS is moving forward to take care of the whole person and treat employees as human beings first. We are taking measured efforts to hear the “ground truth” of the employees and provide trusted and safe spaces to dialogue across differences. These grassroots efforts provide a voice for employees to help DHS establish inclusive workplaces where employees from all backgrounds feel they belong.

Supporting the DHS workforce also involves competitive recruitment options and retention incentives. In 2021, DHS launched the Cybersecurity Talent Management System to grow the future cybersecurity workforce, with

Figure 2: DHS Employees by Component (as of pay period ending March 11, 2023)

Agency	Headcount
CBP	63,837
CISA	2,882
FEMA	22,781
FLETC	1,297
ICE	20,124
TSA	62,332
USCG – Civilian	9,331
USCG – Military	44,813
USCIS	20,066
USSS	7,756
Headquarters Total	6,621
Total	261,840

greater flexibility to attract and retain the best cyber talent. To date, DHS has processed over 5,000 applicants across a wide range of experience levels for an initial cohort of positions in both CISA and the Office of the Chief Information Officer. Effective cybersecurity across the nation requires expertise at all levels, and we are committed to supporting the development of the entire nation's cybersecurity human capital by helping America's academic institutions produce qualified entry-level employees and increasing the awareness of cybersecurity professional opportunities.

DHS will continue efforts to prioritize efficient hiring. The Department has made and will continue to make significant progress in improving hiring and has reduced the total security clearance process time. To further improve hiring across the agency, the Office of the Chief Human Capital Officer is bolstering the skills of human resources professionals on the use of hiring flexibilities such as direct hire authority, Schedule A, military spouses, and other DHS-specific and government-wide hiring flexibilities. DHS will undertake a comprehensive review of hiring across the Department to identify trouble spots and implement Department-wide efficiencies based on DHS's mission requirements and lessons learned from the Office of Personnel Management.

Physical Assets

The Department's physical assets, from vehicles to facilities, cutters to drones, and more, will be reviewed to ensure alignment with mission requirements. Procurement and acquisition processes must be based on analysis, leverage the scale of the Department, and have strong alignment with strategy. As one example, DHS has committed to electrifying 50 percent of its vehicle fleet by 2030 and is building new facilities to be energy efficient. The Department's systems will be matured, with the reinvigoration of the Deputy's Management Action Group and the continued evolution of the Acquisition Review Board, to provide coordination and oversight. In another example, the Department will focus on reducing our physical footprint both to save money but also to adapt for the hybrid workforce of the future.

As the third-largest department in the Federal Government and the nation's largest law enforcement agency, DHS is uniquely positioned to implement market-shaping investments into resilient and clean energy-efficient buildings and electric vehicles. DHS will work with other federal agencies, SLTT governments, and the manufacturing sector to ensure these investments are made in a way that advances unity of effort, improves mission resilience, and drives equitable growth.



Technology and Data

DHS collects and holds significant amounts of data. It is critical to leverage this data and improve our technologies, processes, and services to the greatest effect possible to accomplish our missions, while ensuring legal requirements and privacy safeguards are met. DHS is entrusted with handling the sensitive personal information of Americans, visitors, and businesses when there is a nexus to homeland security, and it is our duty to handle it responsibly and securely. To do this effectively, we must conduct this work in a manner worthy of the public's trust.

DHS has launched a Data Inventory Program to create a catalog of DHS data that is accurate,

complete, timely, and useful and provide a systematic approach for documenting how and where information is collected, the purposes for which it is being used, and how information flows. We will build on this effort to leverage data more effectively as a strategic asset across the Department, including identifying datasets that can be used for AI, assisting privacy oversight activities, and enabling increased data discovery and sharing. Among other benefits, this will make it possible for analysts to create accurate predictive models more easily that will allow us to better plan for changing operational dynamics in multiple mission areas. Wherever possible, the organization of data to assist in equity assessments will be prioritized.

Integrated data operations will be key to DHS's success for years to come. These operations require data standards that are consistent within DHS and that are aligned with other federal departments. Data standards make data platforms more efficient and strengthen our data analysis and statistical capabilities throughout the Department. In an important step forward on this effort, DHS established the Office of Homeland Security Statistics in 2022, which will work with the Department's Chief Data Officer to oversee the development of enterprise-wide data standards for operational and statistical data and will conduct independent reporting and analysis for all DHS mission domains.

DHS will continue to leverage technology to enhance our preparedness and resiliency, improve the interoperability of our operations, and better share information with the homeland security enterprise. We will become more resilient by enabling hybrid and remote work where possible. While the COVID-19 pandemic demonstrated the imperative for these efforts, effective technology implementation can turn this into a long-term advantage for the DHS workforce and, ultimately, for mission effectiveness. We will also focus on ensuring that different Components and work units within DHS can effectively communicate and collaborate to foster increased cohesion and unity of effort.



DHS interacts with more members of the public every day than any other federal agency, and we will focus on using technology and other levers to improve customer experience, enhance service delivery, and increase informed compliance with law enforcement. The recently launched Customer Experience Steering Committee will build practices of customer research and human-centered design into every level of the Department's operations and develop capabilities to better meet the needs of diverse communities and the general public to improve our mission outcomes. As a first step, DHS has pledged to eliminate 20 million administrative burden hours imposed on the public by May 2023. This will be accomplished by removing unneeded forms, steps, and processes, prepopulating known data, reducing errors, and improving ease of use through usability testing and plain language. These improvements will also reduce the administrative burden on employees, allowing them to focus on true mission needs.

OAW highlighted DHS's leadership in technology and data to fulfill a mission. The experience of OAW required DHS to integrate systems and share data between DHS Components and other agencies. Under traditional processes, this level of integration and data sharing could have taken years, but DHS accomplished it in weeks. As DHS continues to face evolving and unpredictable operational challenges, the Department will use data as a tool to integrate operations where individual DHS Components,



as well as interagency partners, see operational and strategic value from sharing data.

Lastly, as the lead agency for protecting and defending our federal civilian government networks, in close partnership with the Office of Management and Budget, we will continue to lead the Federal Government by example when it comes to our own cybersecurity practices. We will develop new ways to validate and enforce contract requirements around vendor cyber hygiene practices and implement the use of software bills of materials and other new technologies to enhance the security of our information and communications technology supply chains. We are more secure when we are open and transparent, and we will build on efforts like the "Hack DHS" bug bounty program to enable private security researchers to report vulnerabilities and embrace open-source software throughout the Department.

Conclusion

The homeland security enterprise has never been more fit for the mission before us: we safeguard the American people with honor and integrity. The core capabilities of our Department have become key to solving the challenges of tomorrow. Finding and sharing information, forging robust partnerships with the communities we serve, and our adaptability will help us fulfill our mission for the 20 years to come.

Over the next 20 years, the DHS missions are going to grow more complex as new threats emerge with increasing speed and even greater potential for harm. Foreign adversaries are

waging new kinds of war. They do so through trade and investment flows and through the rapidly evolving technologies that connect us. In our increasingly interconnected world, our work to reinforce our homeland security has never been more important to our national security.

The changes described in this Report reflect a Department and a homeland security enterprise that is more prepared, more secure, more resilient, more capable, more adaptable, and more forward-looking to meet this moment. It is a Department and enterprise that is focused firmly on preparing for the challenges of the





future while confronting the challenges of today. It takes direction from the President's *National Security Strategy*³⁴, ensuring that our actions fit into the broader efforts of the U.S. Government and our partners. It is a Department that is more fit for purpose than ever to meet today's threats and challenges using the core competencies of DHS and our homeland security enterprise partners.

Implementing this strategic vision over the next four years will require the combined work of the more than 260,000 employees of DHS, together with our stakeholders and partners

across the homeland security enterprise. We are ready for the challenge; the work is already well underway.

Appendix A: Legal Requirement for the Review and Report

Pub. L. No. 107-296 provides the legal requirement for the review and report in Section 707 of the *Homeland Security Act of 2002*, as amended by the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Pub. L. No. 110-53), which includes the following requirements:³⁵

6 U.S.C. 347. QUADRENNIAL HOMELAND SECURITY REVIEW

(a) REQUIREMENT. -

- (1) QUADRENNIAL REVIEWS REQUIRED. - In fiscal year 2009, and every 4 years thereafter, the Secretary shall conduct a review of the homeland security of the Nation (in this section referred to as a “quadrennial homeland security review”).
- (2) SCOPE OF REVIEWS. - Each quadrennial homeland security review shall be a comprehensive examination of the homeland security strategy of the Nation, including recommendations regarding the long-term strategy and priorities of the Nation for homeland security and guidance on the programs, assets, capabilities, budget, policies, and authorities of the Department.
- (3) CONSULTATION. - The Secretary shall conduct each quadrennial homeland security review under this subsection in consultation with—
 - (A) the heads of other Federal agencies, including the Attorney General, the Secretary of State, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of the Treasury, the Secretary of Agriculture, the Secretary of Energy, and the Director of National Intelligence;
 - (B) key officials of the Department, including the Under Secretary for Strategy, Policy, and Plans; and
 - (C) other relevant governmental and nongovernmental entities, including State, local, and tribal government officials, members of Congress, private sector representatives, academics, and other policy experts.
- (4) RELATIONSHIP WITH FUTURE YEARS HOMELAND SECURITY PROGRAM. - The Secretary shall ensure that each review conducted under this section is coordinated with the Future Years

Homeland Security Program required under section 874.

- (b) CONTENTS OF REVIEW. —In each quadrennial homeland security review, the Secretary shall—
- (1) delineate and update, as appropriate, the national homeland security strategy, consistent with appropriate national and Department strategies, strategic plans, and Homeland Security Presidential Directives, including the National Strategy for Homeland Security, the National Response Plan, and the Department Security Strategic Plan;
 - (2) outline and prioritize the full range of the critical homeland security mission areas of the Nation;
 - (3) describe the interagency cooperation, preparedness of Federal response assets, infrastructure, budget plan, and other elements of the homeland security program and policies of the Nation associated with the national homeland security strategy, required to execute successfully the full range of missions called for in the national homeland security strategy described in paragraph (1) and the homeland security mission areas outlined under paragraph (2);
 - (4) identify the budget plan required to provide sufficient resources to successfully execute the full range of missions called for in the national homeland security strategy described in paragraph (1) and the homeland security mission areas outlined under paragraph (2);
 - (5) include an assessment of the organizational alignment of the Department with the national homeland security strategy referred to in paragraph (1) and the homeland security mission areas outlined under paragraph (2); and
 - (6) review and assess the effectiveness of the mechanisms of the Department for executing the process of turning the requirements developed in the quadrennial homeland security review into an acquisition strategy and expenditure plan within the Department.
- (c) REPORTING. -
- (1) IN GENERAL. - Not later than December 31 of the year in which a quadrennial homeland security review is conducted, the Secretary shall submit to Congress a report regarding that quadrennial homeland security review.
 - (2) CONTENTS OF REPORT. - Each report submitted under paragraph (1) shall include—
 - (A) the results of the quadrennial homeland security review;

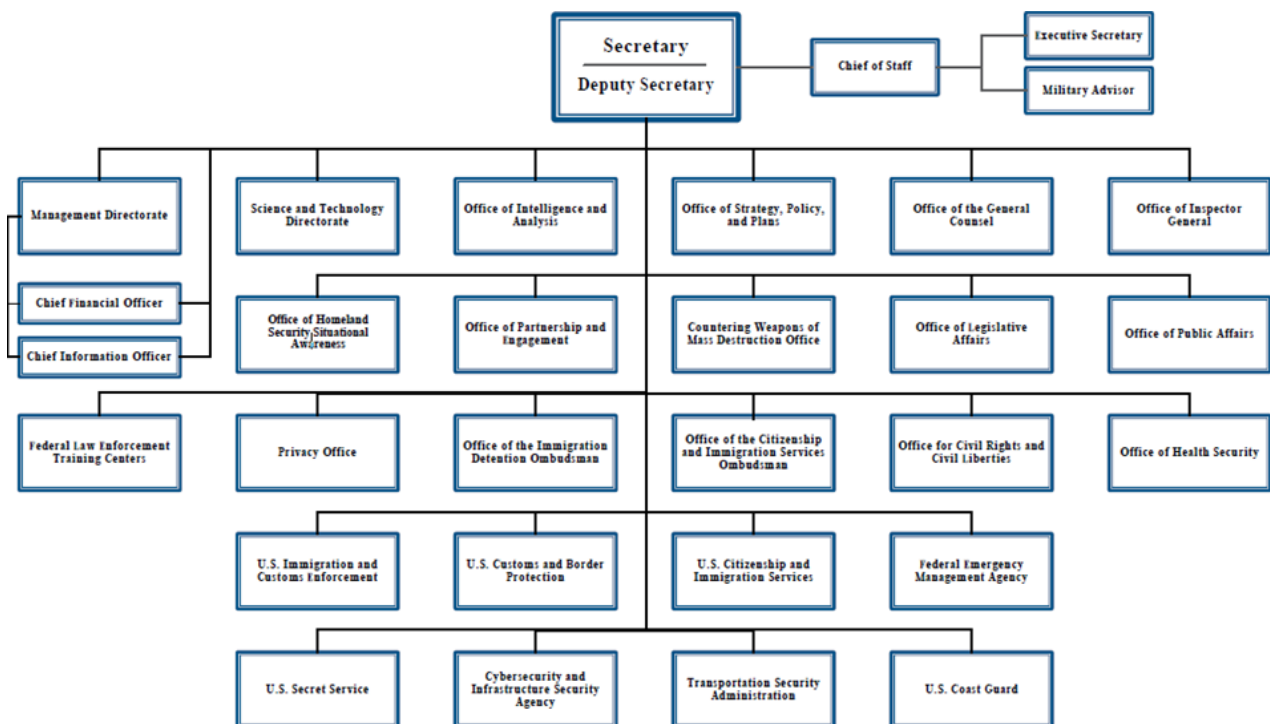
- (B) a description of the threats to the assumed or defined national homeland security interests of the Nation that were examined for the purposes of that review or for purposes of the quadrennial EMP and GMD risk assessment under section 320(d)(1) (E);
 - (C) the national homeland security strategy, including a prioritized list of the critical homeland security missions of the Nation;
 - (D) a description of the interagency cooperation, preparedness of Federal response assets, infrastructure, budget plan, and other elements of the homeland security program and policies of the Nation associated with the national homeland security strategy, required to execute successfully the full range of missions called for in the applicable national homeland security strategy referred to in subsection (b)(1) and the homeland security mission areas outlined under subsection (b)(2);
 - (E) an assessment of the organizational alignment of the Department with the applicable national homeland security strategy referred to in subsection (b)(1) and the homeland security mission areas outlined under subsection (b)(2), including the Department's organizational structure, management systems, budget and accounting systems, human resources systems, procurement systems, and physical and technical infrastructure;
 - (F) a discussion of the status of cooperation among Federal agencies in the effort to promote national homeland security;
 - (G) a discussion of the status of cooperation between the Federal Government and State, local, and tribal governments in preventing terrorist attacks and preparing for emergency response to threats to national homeland security;
 - (H) an explanation of any underlying assumptions used in conducting the review; and
 - (I) any other matter the Secretary considers appropriate.
- (3) PUBLIC AVAILABILITY. - The Secretary shall, consistent with the protection of national security and other sensitive matters, make each report submitted under paragraph (1) publicly available on the Internet website of the Department.
- (d) AUTHORIZATION OF APPROPRIATIONS. - There are authorized to be appropriated such sums as may be necessary to carry out this section.

Appendix B: Organizational Alignment of the Department with Homeland Security Strategic Priorities and Mission Areas

The Department is strengthening its capacity to execute its five enduring missions and a new sixth mission across the Department's many functions:

- *Mission 1: Counter Terrorism and Prevent Threats*
- *Mission 2: Secure and Manage Our Borders*
- *Mission 3: Administer the Nation's Immigration System*
- *Mission 4: Secure Cyberspace and Critical Infrastructure*
- *Mission 5: Build a Resilient Nation and Respond to Incidents*
- *Mission 6: Combat Crimes of Exploitation and Protect Victim*

Figure B-1: DHS Organizational Chart



DHS's diverse and complex missions require integration across eight Operational Components, 17 Headquarters Offices, and two Directorates. The Operational Components conduct front-line counterterrorism, law enforcement, cybersecurity, prevention, mitigation, preparedness, and response operations to execute the Department's missions. The remaining Headquarters Offices and Directorates provide key mission support resources, intelligence and analysis, equipment, research, outreach and public-private sector coordination, policies, and support to facilitate mission execution.

Each DHS Component's specific mission set is described below, along with the mission areas where each Component plays a lead or substantial role. For each of the Department's missions, multiple Components share responsibility, emphasizing the need for enhanced coordination and cohesion to achieve mission success.

Operational Components

U.S. Citizenship and Immigration Services (USCIS): The federal agency that oversees lawful immigration to the United States.

Missions: 1, 2, 3, 6

U.S. Coast Guard (USCG): The only military service within DHS, the USCG protects the marine transportation system, responds to marine pollution events, defends the nation from maritime threats, supports defense operations, and saves those in distress.

Missions: 1, 2, 4, 5

U.S. Customs and Border Protection (CBP): CBP's priority mission is to keep terrorists and their weapons out of the United States. CBP also secures and facilitates trade and travel while enforcing regulations, including immigration and drug laws.

Missions: 1, 2, 3, 5, 6

Cybersecurity and Infrastructure Security Agency (CISA): Leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

Missions: 1, 4, 5

Federal Emergency Management Agency (FEMA): Supports our citizens and first responders to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from,

and mitigate all hazards.

Mission: 5

U.S. Immigration and Customs Enforcement (ICE): Promotes homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.

Missions: 1, 2, 3, 4, 6

Transportation Security Administration (TSA): Protects the nation's transportation systems to ensure freedom of movement for people and commerce.

Missions: 1, 2, 4

U.S. Secret Service (USSS): Ensures the continuity of government through protection of our national leaders and National Special Security Events (NSSEs), as well as preserves the integrity of our nation's financial infrastructure.

Missions: 1, 4, 6

Headquarters Offices and Directorates

Management Directorate (MGMT): Responsible for budget, appropriations, expenditure of funds, accounting and finance; procurement; management, administration, and oversight of the Department's acquisition programs and acquisition management systems; human resources and personnel; information technology systems; facilities, property, equipment, and other material resources; providing biometric identification services; securing federal infrastructure across the country; and identification and tracking of performance measurements relating to the responsibilities of the Department.

Science and Technology Directorate (S&T): The primary research and development arm of the Department, S&T provides federal, state, local, and tribal officials with the technology and capabilities to protect the homeland.

Office of the Citizenship and Immigration Services Ombudsman (CISOMB): Improves the quality of citizenship and immigration services delivered to the public by providing individual case assistance, and by identifying systemic issues and making recommendations to improve the administration of

immigration benefits by USCIS.

Office for Civil Rights and Civil Liberties (CRCL): Provides legal and policy advice to Department leadership on civil rights and civil liberties issues, investigates and resolves complaints, and provides leadership for Equal Employment Opportunity Programs. Engages with diverse American communities whose civil rights may be affected by Department activities and coordinates international human rights treaty reporting.

Countering Weapons of Mass Destruction Office (CWMD): Leads and coordinates Departmental efforts to safeguard the United States against chemical, biological, radiological, and nuclear threats posed by terrorists and other threat actors.

Office of the Executive Secretary (ESEC): Provides direct support to the Secretary and Deputy Secretary, as well as related support to leadership and management across the Department, including the accurate and timely dissemination of information and written communications from throughout the Department and our homeland security partners to the Secretary and Deputy Secretary.

Federal Law Enforcement Training Centers (FLETC): Provides career-long training to law enforcement professionals to help them fulfill their responsibilities safely and proficiently.

Office of the General Counsel (OGC): Integrates over 3,000 attorneys from throughout the Department into an effective, client-oriented, full-service legal team. OGC comprises a headquarters office with subsidiary divisions and the legal offices for nine Department Components.

Office of Health Security (OHS): Enables coordination, standardization, and accountability as the principal medical, workforce health and safety, and public health authority for DHS, while helping enhance our workforce and nation's preparedness, response, and resilience to the health impacts of terrorism and other disasters.³⁶

Office of Homeland Security Situational Awareness (OSA): Provides situational awareness, a common operating picture, and decision support for the homeland security enterprise on threats, incidents, hazards, and events impacting the homeland.

Office of the Immigration Detention Ombudsman (OIDO): An independent office reporting directly to the Secretary that assists individuals with complaints about the potential violation of law, policy, standards and rights in immigration detention standards or other misconduct by DHS and other personnel or contract personnel, provides oversight of immigration detention facilities, and makes recommendations for improving immigration detention conditions and care.

Office of the Inspector General (OIG): Provides independent oversight and promotes excellence, integrity, and accountability within DHS.

Office of Intelligence and Analysis (I&A): Supports the homeland security enterprise by providing the timely intelligence and information needed to keep the homeland safe, secure, and resilient.

Office of Legislative Affairs (OLA): Serves as primary liaison to Members of Congress and their staff, the White House and Executive Branch, and to other federal agencies and governmental entities that have roles in ensuring national security.

Office of the Military Advisor (MIL): Provides counsel and support to the Secretary and Deputy Secretary in affairs relating to policy, procedures, preparedness activities, and operations between DHS and the Department of Defense.

Office of Partnership and Engagement (OPE): Coordinates the Department's outreach efforts with key stakeholders nationwide, ensuring a unified approach to external engagement.

Privacy Office (PRIV): Protects individuals by embedding and enforcing privacy protections and transparency in all DHS activities.

Office of Public Affairs (OPA): Coordinates the public affairs activities of all DHS Components, Offices and Directorates, and serves as the Federal Government's lead public information office during a national emergency or disaster.

Office of Strategy, Policy, and Plans (PLCY): Serves as a central resource for the Secretary and other Department leaders for strategic planning and analysis and facilitates decision-making on the full breadth of issues that may arise across the dynamic homeland security enterprise.

Appendix C: Process

The process that DHS uses to develop the QHSR is representative of how the Department serves the American people. The QHSR is for the entire homeland security enterprise. Accordingly, the process incorporates the statutory guidance for including stakeholder outreach, U.S. Government outreach, and other substantive elements. Critical to this process is a summary review of the first two QHSR Reports, the first from 2010 and the second from 2014. This QHSR Report is the Department’s third.

Review Phase

The QHSR development process leveraged existing and concurrent policy development, strategic planning, threat assessment, and risk assessment efforts. Further phases included extensive consultation with senior DHS leadership, federal agency partners, SLTT government leaders, and other external stakeholders. At each phase, the Department incorporated recent learnings from other assessment, review, and stakeholder engagement efforts to avoid duplication of effort and repetitive outreach to stakeholder groups.

Figure C-1: Four-Phased Review Process



Phase 1: Research and Analysis

The Department collected existing analytic documents, Component strategies and strategic plans, Departmental budget documents, risk assessments, and intelligence assessments. DHS also

reviewed statements by Administration and Department leadership, including congressional testimony and speeches.

Phase 2: Consultations

PLCY consulted with DHS leadership, DHS Component subject matter experts and congressional staff, as well as U.S. Government, SLTT, industry, academic, faith-based, and NGO partners. DHS conducted 90 individual consultations, including 52 with DHS senior leaders, 21 with interagency partners, and 17 with external stakeholders, in which participants were provided an overview of the key themes the Department was reviewing for the QHSR and were given an opportunity to convey feedback on the Department's performance and areas requiring improvement, as well as emerging threats and challenges that our partners anticipated we would face over the next four years.

Phase 3: Issue-Based Reviews and Drafting

Based on the input from the first two phases and key documents, including the development process for the Biden-Harris Administration's National Security Strategy, the Department selected the 11 most impactful topics to DHS's enduring missions and then conducted Issue-Based Reviews (IBRs) for in-depth examination and policy development for each topic.

The IBRs consisted of four elements:

- Review and synthesis of existing DHS congressional testimony, policies, assessments, Intelligence Community products, and other documentation;
- Consultations with DHS senior leaders;
- Consultations with U.S. Government partners; and
- Consultations with external stakeholders.

I&A arranged three Intelligence Community briefings for DHS leaders. These were attended by PLCY leadership as well as members of PLCY's QHSR team, representatives from relevant Components, and relevant DHS Front Office Senior Counselors. I&A also provided a draft of the Homeland Threat Assessment to ensure its characterization of threats were aligned in the QHSR.

Phase 4: Finalization

The draft QHSR was reviewed by all DHS Components. DHS also provided the eight federal departments and agencies specified in the statute governing the QHSR, as well as the White House, the opportunity to comment on the draft Report. This was followed by a final review by DHS leadership and, ultimately, approval by the Secretary of Homeland Security.

Endnotes

1. The “homeland security enterprise” refers to the collective efforts and shared responsibilities of federal, state, local, tribal, territorial, nongovernmental, and private-sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities. It connotes a broad-based community with a common interest in the safety and well-being of America and American society. See *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (DHS; February 2010, pp. 12-13); <https://www.dhs.gov/sites/default/files/publications/2010-qhsr-report.pdf>.
2. *Countering Human Trafficking Year in Review: October 2021 to September 2022* (DHS Center for Countering Human Trafficking, January 2023); see https://www.dhs.gov/sites/default/files/2023-01/23_0131_CCHT_year-in-review.pdf.
3. National Critical Functions are functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. See <https://www.cisa.gov/national-critical-functions>.
4. Signed by President Biden and released by the White House National Security Council in June 2021; see <https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf>.
5. Signed by President Biden on behalf of the United States on June 10, 2022, and co-signed by the Heads of State and Governments of the Argentine Republic, Barbados, Belize, the Federative Republic of Brazil, Canada, the Republic of Chile, the Republic of Colombia, the Republic of Costa Rica, the Republic of Ecuador, the Republic of El Salvador, the Republic of Guatemala, the Co-operative Republic of Guyana, the Republic of Haiti, the Republic of Honduras, Jamaica, the United Mexican States, the Republic of Panama, the Republic of Paraguay, the Republic of Peru, and the Oriental Republic of Uruguay; see <https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/10/los-angeles-declaration-on-migration-and-protection/>.
6. See <https://www.federalregister.gov/documents/2022/09/09/2022-18867/public-charge-ground-of-inadmissibility>.
7. As of June 2022, USCIS eliminated the pending queue of Application Support Center biometric appointments and is now back to its regular two-week scheduling window.
8. See <https://www.federalregister.gov/documents/2022/03/29/2022-06148/procedures-for-credible-fear-screening-and-consideration-of-asylum-withholding-of-removal-and-cat>.
9. For additional information, see <https://www.uscis.gov/DACA>.
10. See <https://www.missingkids.org/blog/2022/sextortion-the-hidden-pandemic>; and the DHS Countering Human Trafficking Year in Review: October 2021 to September 2022 (https://www.dhs.gov/sites/default/files/2023-01/23_0131_CCHT_year-in-review.pdf).
11. *Global Estimates of Modern Slavery: Forced Labour and Forced Marriage* (International Labour Organization; September 2022); see https://www.ilo.org/wcmsp5/groups/public/-ed_norm/-ipec/documents/publication/wcms_854795.pdf.
12. Pub. L. No. 117-322; signed into law by President Biden on December 27, 2022.
13. Pub. L. No. 117-78; signed by President Biden on December 23, 2021.
14. The White House, December 2021. See <https://www.whitehouse.gov/wp-content/uploads/2021/12/National-Action-Plan-to-Combat-Human-Trafficking.pdf>.
15. Developed in compliance with Executive Order (E.O.) 14001, *On a Sustainable Public Health Supply Chain*, this is a joint DHS, Department of Defense, HHS, and Department of Veterans Affairs report released in July 2021. See <https://www.phe.gov/Preparedness/legal/Documents/National-Strategy-for-Resilient-Public-Health-Supply-Chain.pdf>.
16. Signed by President Biden on July 28, 2021; see <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/>.

17. "Division Y" of Pub. L. No. 117-103; signed into law by President Biden on March 15, 2022.
18. Pub. L. No. 117-58; signed into law by President Biden on November 15, 2021.
19. Signed by President Biden on May 12, 2021; see <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>.
20. See <https://www.cisa.gov/sbom>.
21. See <https://www.cisa.gov/uscrt/ncas/alerts/aa21-291a>.
22. See <https://www.cyberseek.org/>.
23. President Biden has twice amended E.O. 12898 to strengthen federal environmental justice initiatives, through E.O. 14008 (*Tackling the Climate Crisis at Home and Abroad*; signed January 27, 2021; see <https://www.federalregister.gov/documents/2021/02/01/2021-02177/tackling-the-climate-crisis-at-home-and-abroad>) and E.O. 14082 (*Implementation of the Energy and Infrastructure Provisions of the Inflation Reduction Act of 2022*; signed September 12, 2022; see <https://www.federalregister.gov/documents/2022/09/16/2022-20210/implementation-of-the-energy-and-infrastructure-provisions-of-the-inflation-reduction-act-of-2022>).
24. *National Biodefense Strategy and Implementation Plan for Countering Biological Threats, Enhancing Pandemic Preparedness, and Achieving Global Health Security* (The White House; October 2022). See <https://www.whitehouse.gov/wp-content/uploads/2022/10/National-Biodefense-Strategy-and-Implementation-Plan-Final.pdf>.
25. *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, Pub. L. No. 100-707, signed into law November 23, 1988; see <https://www.fema.gov/disaster/stafford-act>.
26. 46 U.S.C § 55102; see https://help.cbp.gov/s/article/Article-23?language=en_US.
27. U.S. Department of Homeland Security Artificial Intelligence Strategy, released December 3, 2020; see https://www.dhs.gov/sites/default/files/publications/dhs_ai_strategy.pdf.
28. Data is current as of February 11, 2023.
29. DHS employees authorized by statute to enforce the laws of the United States, carry firearms, and make criminal arrests in the performance of their assigned duties.
30. DHS personnel stationed outside of the United States at facilities operating under either Chief of Mission Authority or Combatant Commander Authority. Personnel stationed abroad include law enforcement officers, frontline workers, and military veterans.
31. Frontline workers are defined as the Priority Mission Critical Occupations, and all law enforcement officer and law enforcement-related occupations.
32. E.O. 14074, signed by President Biden on May 25, 2022; see <https://www.federalregister.gov/documents/2022/05/31/2022-11810/advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and>.
33. For the fiscal years 2021-2024 plan, see https://www.dhs.gov/sites/default/files/2022-12/DHS_Inclusive_Diversity_Strategic_Plan.pdf.
34. Signed by President Biden for release in October 2022; see <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>.
35. The Department recognizes that Congress recently amended requirements for subsequent productions of the QHSR in the *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023* (Pub. L. No. 117-263, as enacted on December 23, 2022). The Department substantially completed the enclosed Review prior to the enactment of these amended requirements and has sought to avoid or mitigate any further delay in submitting it to Congress.
36. In 2022, Congress provided an exception to a limitation on DHS reorganization that allowed for the establishment of the OHS. (See *Consolidated Appropriations Act, 2022*, Pub. L. No. 117-103, 136 Stat. 337 (2022); see <https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf>.)



Homeland
Security