DHS STRATEGIC PLAN:

Fiscal Years 2023-2027

Table of Contents

Letter from the Secretary....1

Department of Homeland Security....3

DHS Strategic Goals and Objectives....9

DHS Missions and Objectives....13

- Mission One: Counter Terrorism and Prevent Threats....13
- Mission Two: Secure and Manage our Borders....17
- Mission Three: Administer the Nation's Immigration System....24
- Mission Four: Secure Cyberspace and Critical Infrastructure....28
- Mission Five: Build a Resilient Nation and Respond to Incidents....35
- Mission Six: Combat Crimes of Exploitation and Protect Victims....40

Enable Mission Success by Strengthening the Enterprise....47

Appendix A: DHS Organizational Performance Management and Measurement....52

Appendix B: DHS Evaluation and Evidence....54

Letter from the Secretary

The Department of Homeland Security is charged with ensuring the safety and security of the American people. DHS leads the federal government's efforts to prepare for, prevent, mitigate, respond to, and recover from any and all threats to our nation, its people, and their way of life.

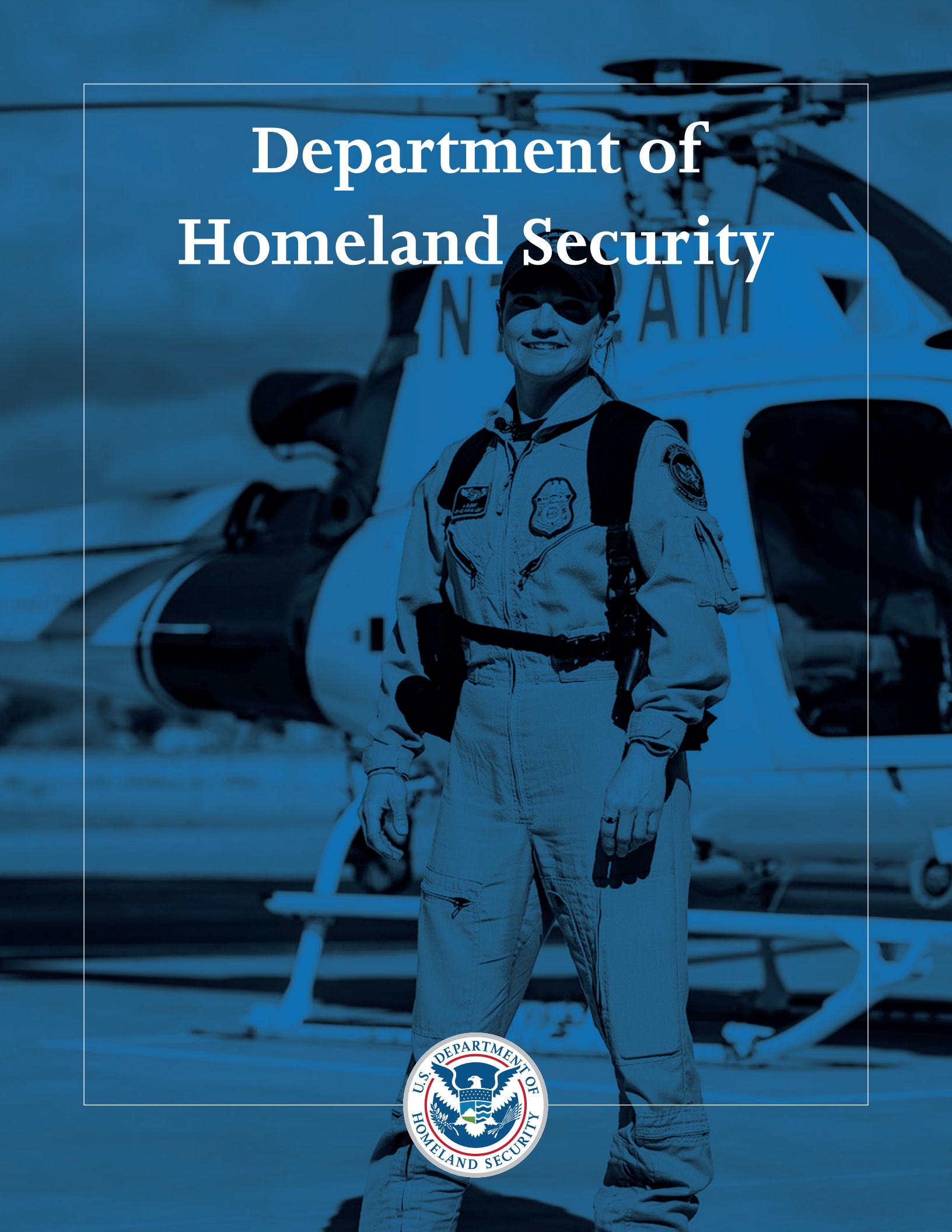
In the over 20 years since our founding, the threat landscape we confront has evolved and expanded, dramatically and constantly. As has the work of this Department.

I am proud to continue that work. Pursuant to the Government Performance and Results Act (GPRA) of 1993, as amended by the GPRA Modernization Act of 2010, I present this DHS Strategic Plan for Fiscal Year 2023-2027.

The 2023 Quadrennial Homeland Security Review (QHSR) reviewed the strategic environment in which the Department operates, provided strategic guidance, and updated the Department's mission framework. The FY 2023-2027 Strategic Plan organizes the Department's strategic goals and objectives into six missions defined in the QHSR, articulates the desired outcomes the Department works to achieve within each of these mission areas, and identifies the parts of the Department that contribute to each mission.

Each of the 260,000 men and women who serve across our Department will have an important role to play in implementing this strategic vision and achieving its goals. I have the utmost confidence in their ability to do so. The integrity, dedication, and skill of the DHS workforce is unparalleled. Americans are safer – on land, at sea, in the air, and in cyberspace – because of their continued service.

Department of Homeland Security



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

ABOUT THE DEPARTMENT

Congress established the U.S. Department of Homeland Security (DHS) in 2002 as a Cabinet-level agency to consolidate the nation's approach to homeland security.[1] The new Department combined the functions of 22 different federal departments and agencies with broad responsibilities to prevent attacks, mitigate threats, respond to national emergencies, preserve economic security, secure the border, and administer the immigration system. In the years since its formation, DHS has improved management and cohesion across its Operational Components, Headquarters Offices, and Directorates, and within the broader homeland security enterprise (HSE).[2]

The world today is more interconnected than at any time in our Department's 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, illicit trade and investment, the exploitation of rapidly evolving technologies that connect us, and malign influence 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 when our Department was founded.

The Department has matured by streamlining and improving the execution of myriad responsibilities and enabling effective joint operations such as the Secretary's Incident Management Assistance Team, Joint Task Force East, Operation Allies Welcome, 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 artificial intelligence and 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. Additionally, 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 by identifying it as the newest homeland security mission 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 vaccination

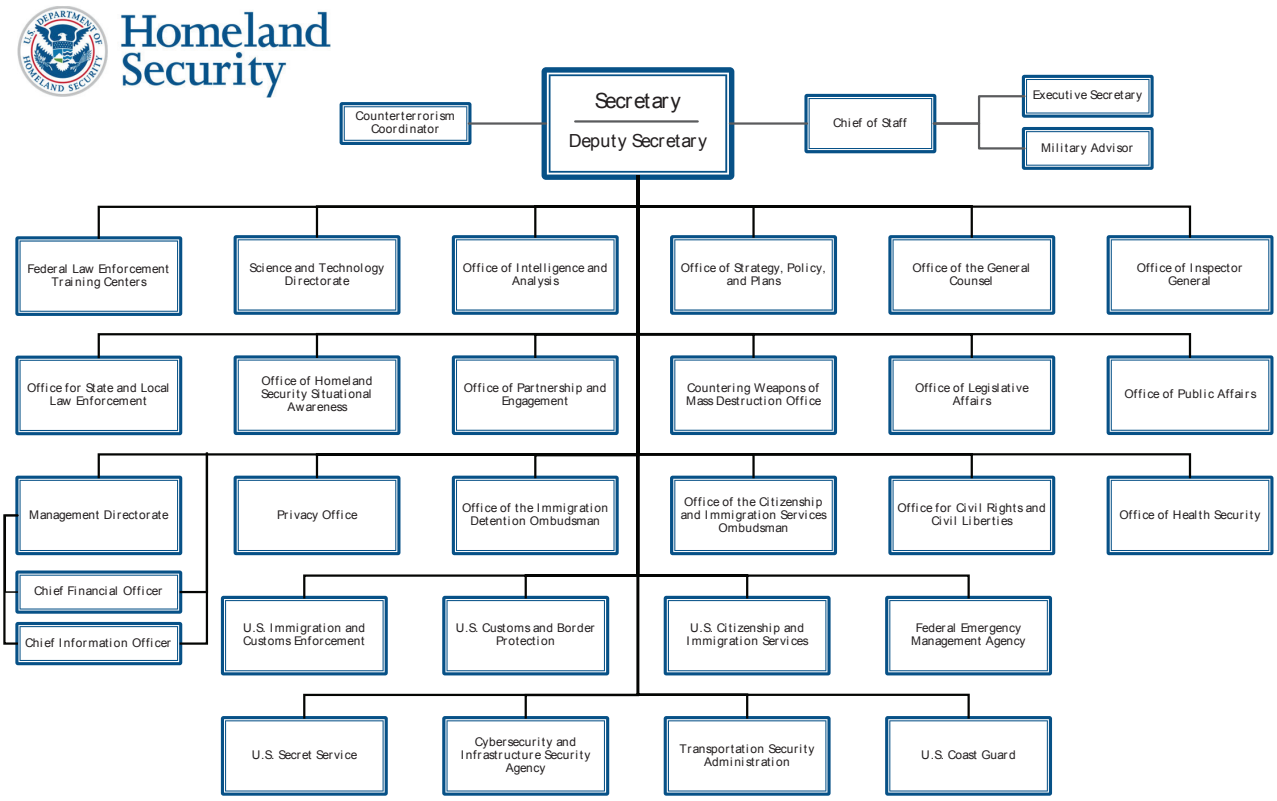
1 *Homeland Security Act of 2002, Pub. L. No. 107-296;* https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf.

2 The HSE consists of the federal, state, local, tribal, territorial, nongovernmental, and private sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of the United States and its people. See https://www.dhs.gov/topics/homeland-security-enterprise.

campaign and the establishment of the Office of Health Security.

As DHS moves forward, the Department will continue to strengthen its core functions to ensure the Department effectively and efficiently accomplishes its missions.

FIG. 1. Organizational Structure[3]



DHS includes eight Operational Components, 19 Headquarters Offices, and two Directorates. The Operational Components conduct front-line counterterrorism; law enforcement; cybersecurity; and prevention, mitigation, preparedness, response, and recovery operations to execute the Department's missions. The Headquarters Offices and Directorates provide key mission support, including resources and equipment, intelligence and analysis, research, outreach and public-private sector coordination, and policies to facilitate mission execution.

3 The Office for State and Local Law Enforcement was transferred from the Office of Partnership and Engagement to the Office of the Secretary through the FY23 Consolidated Appropriations Act.

OPERATIONAL COMPONENTS:

U.S. Citizenship and Immigration Services (USCIS): Oversees lawful immigration to the United States.

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.

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.

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

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.

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.

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

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

HEADQUARTERS OFFICES AND DIRECTORATES:

Management Directorate (MGMT): Oversees the 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 the identification and tracking of performance measurements relating to the responsibilities of the Department.

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 USCIS' administration of immigration benefits.

Office for Civil Rights and Civil Liberties (CRCL): Provides 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 individuals and communities whose civil rights and civil liberties 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.

Counterterrorism Coordinator (CTC): Serves as the principal counterterrorism adviser to the Secretary and Deputy Secretary and coordinates the Department's counterterrorism-related activities – including intelligence, planning, and operational matters – across DHS and with interagency partners.

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 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.[4]

Office of Homeland Security Situational Awareness (OSA): Provides situational awareness, a common operating picture, and decision support for the HSE 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 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 the 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.

---

4 In 2022, Congress provided an exception to a limitation on DHS reorganization that allowed the Secretary to establish an Office of the Chief Medical Officer, which became OHS. (*Consolidated Appropriations Act, 2022*, Pub. L. No. 117-103, 136 Stat. 337 (2022); https://www.congress.gov/bill/117th-congress/house-bill/2471/text.)

Office of the Military Advisor (MIL): Provides counsel and support to the Secretary and Deputy Secretary for 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.

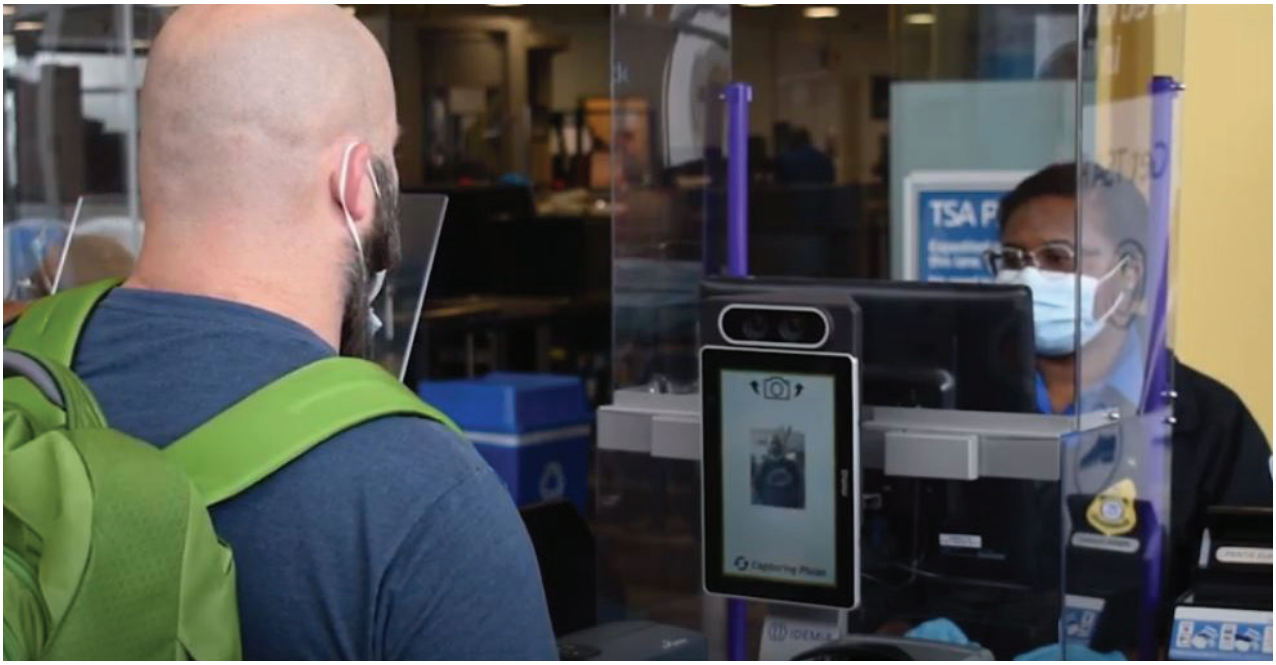
Privacy Office (PRIV): Protects individuals by embedding and enforcing privacy protections and transparency in all DHS activities.

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.

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 technology and capabilities to protect the homeland.

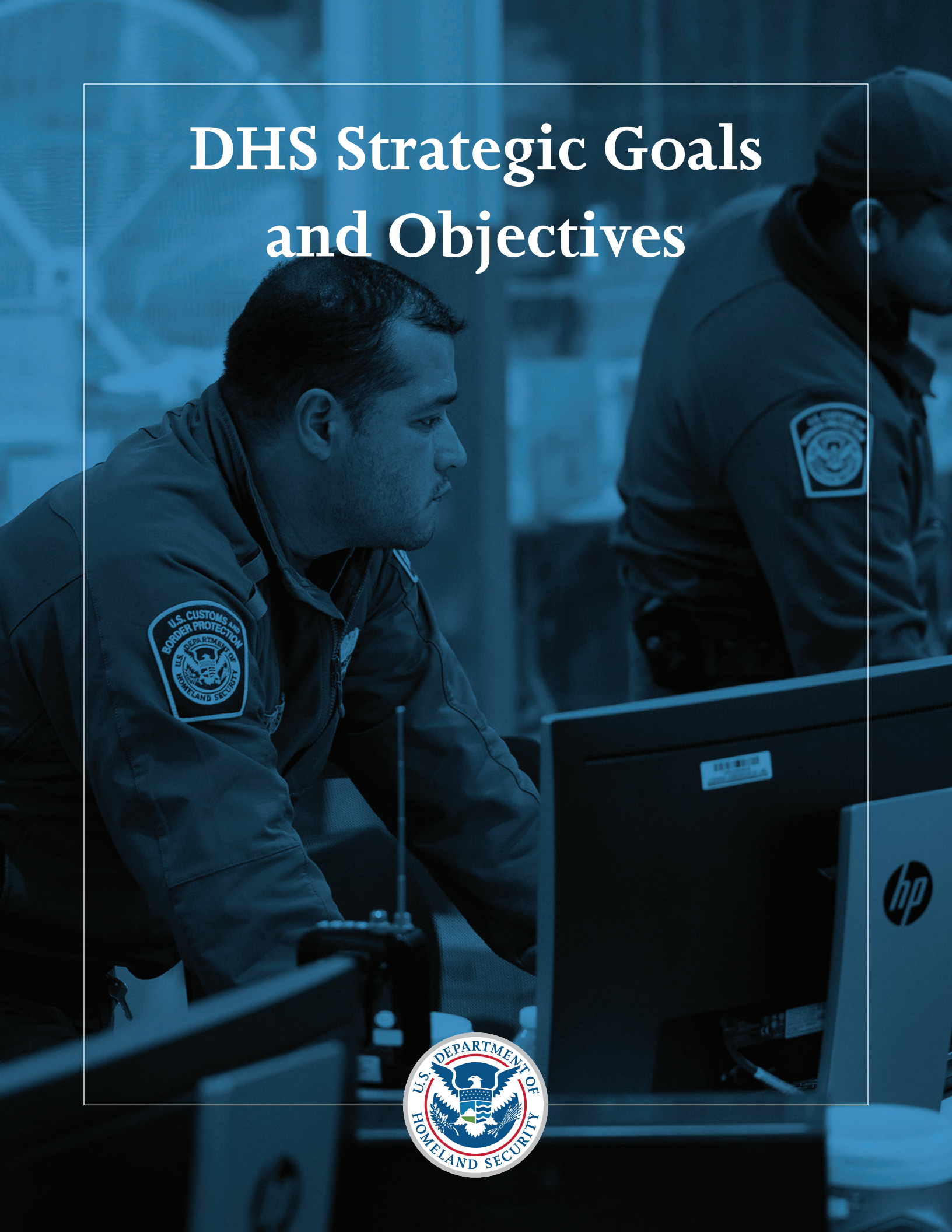
Office for State and Local Law Enforcement (OSLLE): Provides primary coordination, liaison, support, and advocacy on behalf of state, local, tribal, territorial, and campus law enforcement.

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 HSE.



TSA uses new credential authentication technology to improve checkpoint screening capabilities.

DHS Strategic Goals and Objectives



DHS Strategic Goals and Objectives

The guidance contained in the *Government Performance and Results Act Modernization Act of 2010* (GPRAMA)[5] and the Office of Management and Budget (OMB) Circular A-11[6] requires each federal agency to determine its strategic goals and objectives. In accordance with the *Homeland Security Act of 2002*,[7] DHS organizes by mission areas, which, for strategic planning purposes, serve as the Department's strategic goals. DHS priorities are captured in strategic guidance developed throughout the Department. Aligning this guidance to the Department's activities enables progress towards achieving measurable mission outcomes.

As part of the development of the *2023 Quadrennial Homeland Security Review* ("2023 QHSR"), DHS reviewed the authorities and mission areas of the Department, the strategic environment in which the Department operates, and the approaches the Department is taking to achieve mission success. The table below reflects DHS's Missions, Goals, and Objectives as articulated in the 2023 QHSR. The Homeland Security Missions and Objectives framework identifies the five enduring mission areas and a new mission, *Combat Crimes of Exploitation and Protect Victims*. This Strategic Plan articulates the desired outcomes for the nation that the Department works to achieve within each mission area and identifies the parts of the Department that contribute to each. The final category, the *Enabling Mission Success by Strengthening the Enterprise,* lays out strategic objectives that apply to the Department's processes and actions through every level of management and administrative function.

5 Pub. L. No. 111-352.

6 See Part 6, Section 230, "Agency Strategic Planning"; *https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf*.

7 Pub. L. No. 107-296, as amended.

Fig. 2. Homeland Security Missions and Objectives

Strategic Goals	Strategic 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 Boarders
	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 Asses 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 Prevention
	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

As outlined in the following sections, all DHS activities work toward achieving a given desired outcome that aligns to a Strategic Objective. The Components and Offices leading each Objective will coordinate operational activities with appropriate DHS Headquarters and field offices. This coordination complements internal Departmental processes that align activities with budget development, acquisitions and requirements development, policy development, partnership building, and research and development.

The alignment of a Component's or Office's activities enables the Department to plan for mission impact in a way that is measurable, efficient, and sustainable. DHS Components, Offices, and Directorates work to achieve the objectives and bring about the desired outcome within each mission area on behalf of the nation.[8]

DHS'S VISION

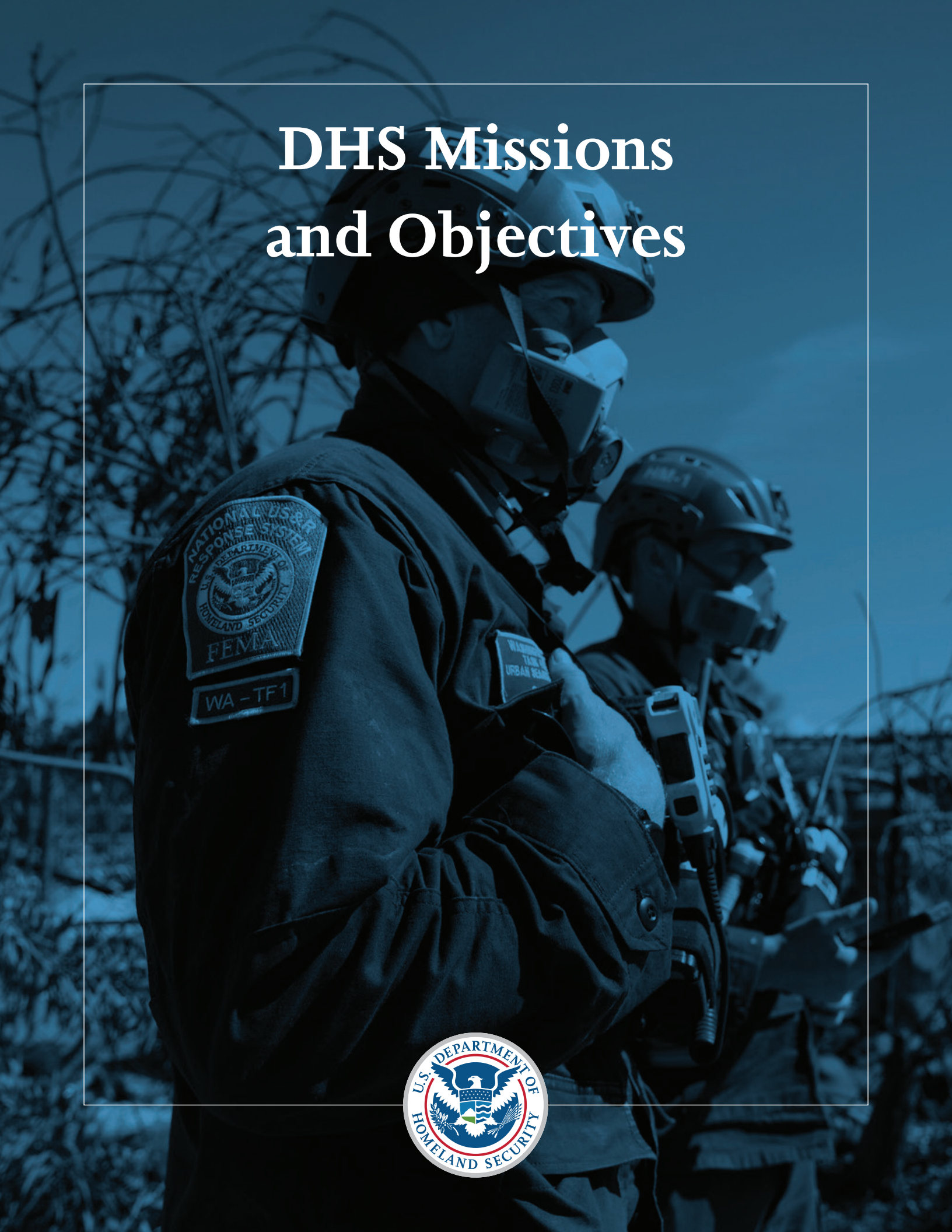
"Over the next twenty years, our mission is going to grow even more complex as new threats emerge with increasing speed and perhaps even greater potential for harm. Foreign adversaries are waging new kinds of war, no longer constrained by borders or military maneuvers. They do so through trade and investment flows and through the rapidly evolving technologies that connect us. While, for example, we harness the power of artificial intelligence to become effective and efficient in our work to secure the homeland, its potential for harm in the hands of a nefarious actor has yet to be fully assessed. In our increasingly interconnected world, our work to reinforce our homeland security has never been more important to our national security. Our Department will continue to evolve and meet the challenges not only of today, but those of tomorrow."

*— Secretary Alejandro N. Mayorkas**

8 The *lead* is primarily accountable for mission delivery; where two or multiple Components are lead, they have accountability to their specific role and authority to deliver that Objective. The *stakeholder* is resourced to provide a capability or capacity to support the lead's delivery of the Mission, Objective, and desired outcome.

* From Secretary Mayorkas Remarks on the 20th Anniversary of the Department, March 1, 2023. See https://www.dhs.gov/news/2023/03/01/secretary-mayorkas-remarks-20th-anniversary-department.

DHS Missions and Objectives



MISSION ONE:
Counter Terrorism and Prevent Threats

DESIRED OUTCOME:
The U.S. homeland and its vital interests are safe from terrorists, hostile nation-state threats, and other emerging threats.

Counterterrorism remains an enduring mission of the Department. 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 domestic and international terrorism. Today, the most significant terrorist threat facing the homeland stems from domestic violent extremists (DVEs), lone offenders, and small groups of individuals who commit acts of violence motivated by a broad range of racial, ethnic, political, religious, anti-government, societal, or personal ideological beliefs or grievances.

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, or HVEs — have continued to launch attacks in their names. Within the United States, the threat from HVEs likely will remain the most prominent form of international terrorism facing the homeland. Although capabilities to conduct large-scale attacks have been severely 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.

In addition to non-state terrorist actors, nation-states are also actively seeking to undermine U.S. competitiveness and our democratic institutions to achieve their own geopolitical goals. Now, more than at any point in the Department's existence, threats from nation-states impact the safety and security of the American people and the homeland. DHS will continue to work closely with government, nongovernmental organizations, international actors, and industry partners to secure the homeland against these threats.

In the coming years, advancements in emerging technologies, notably artificial intelligence, present considerable opportunities to improve daily life for Americans, such as in commercial activity, public health, critical infrastructure network connectivity, aviation security, and marketplace efficiencies. These advancements create the need to develop a mature security architecture to assist the Department's ability to counter emerging threats and threat actors arising from new technology. As these technologies evolve, DHS needs to maintain a technological advantage through long-term research, experimentation, investments, and effective partnerships with industry. As DHS addresses the opportunities and challenges of advancing technology, we will ensure that appropriate governance mechanisms are in place to protect privacy, civil rights, and civil liberties.

OBJECTIVE 1.1:
Collect, Analyze, and Share Actionable Intelligence and Information

DESIRED OUTCOME:
DHS shares timely and actionable information and intelligence with federal, state, local, tribal, territorial, campus, private sector, and international partners, achieving awareness and a comprehensive understanding of threats across the HSE.

The dynamic and evolving nature of threats to the homeland will continue to drive the need for timely information sharing and actionable intelligence and analysis that enables effective operations for DHS and its partners. The Department works alongside the HSE, Intelligence Community, and international partners to gather, produce, and share information on evolving situations and emerging threats through innovative technologies and partnerships to anticipate changes and prepare responses. In 2021, DHS created a dedicated domestic terrorism unit within I&A to improve its capability to focus on and address threats posed by DVEs. The Department will continue to collaborate with homeland security advisors in every state and territory and utilize the national network of fusion centers and other field-based sharing partners to share timely and actionable information and intelligence to enable both DHS and our partners to keep the homeland safe. The Department will also leverage the National Operations Center — the primary, national-level hub for situational awareness, a common operating picture, information fusion, information sharing, and executive communications — in the face of threats, hazards, incidents, or events.

LEAD: I&A, OSA
STAKEHOLDER: ALL

OBJECTIVE 1.2:
Prevent and Disrupt Terrorist and Nation-State Threats

DESIRED OUTCOME:
Threats to the homeland from terrorists, nation-states, and other threat actors are prevented, disrupted, and mitigated.

DHS is undertaking a range of actions to increase its awareness of terrorist and nation-state threats throughout the entire HSE through enhanced information sharing across all levels of government, civil society, and industry. To protect against these threats, DHS will utilize and expand its strong international partnerships to increase sharing of criminal and terrorism-related information, including biometric and biographic data, on all threat actors. With our federal government and major industry partners, DHS will identify and respond to threats posed by the People's Republic of China (PRC), Russia, North Korea, Iran, and other nation-states, by sharing actionable information with our partners, and ultimately, taking the necessary steps to enhance security at scale.

To counter domestic threats, DHS will increase prevention efforts, enhance information sharing, improve our understanding of online content associated with all forms of targeted violence and terrorism, and continue significant outreach to partners, stakeholders, and the public. DHS will also utilize its multi-layered screening and vetting architecture, to include utilizing modernized identity technologies to prevent terrorists from traveling to our country and encourage interagency partners to expand on their existing screening and vetting architectures.

To strengthen the Department's internal and interagency coordination and execution of foreign and domestic counterterrorism and targeted violence mission responsibilities, DHS established the Counterterrorism Coordinator's office.

LEAD: CBP, CISA, CTC, CWMD, I&A, ICE, MGMT, PLCY, TSA, USCG, USSS

STAKEHOLDER: ALL

OBJECTIVE 1.3: Protect Leaders and Designated Individuals, Facilities, and Events

DESIRED OUTCOME:
Designated persons, special events, and protected facilities are kept safe and secure.

Ensuring the protection and safety of our nation's highest elected leaders is a paramount responsibility. DHS maintains a highly skilled and motivated workforce that employs innovative technologies and advanced countermeasures to protect designated leadership and visiting foreign heads of state and government. The Department also protects federal facilities and supports state, local, tribal, and territorial (SLTT) governments to protect personnel and people attending events of national significance (e.g., National Special Security Events and Special Event Assessment Rating events). DHS leads efforts to mitigate vulnerabilities by leveraging our unique capabilities like counter unmanned aircraft systems (C-UAS)[9]; detection of Chemical, Biological, Radiological, and Nuclear (CBRN) threats; explosives detection and mitigation; perimeter protection technologies; and hardening structures; all while upholding the privacy, civil rights, and civil liberties of the American people. DHS also shares intelligence bulletins and analysis with homeland security stakeholders, develops and shares best practices to counter potential attacks against soft and hard targets, promotes a dynamic process to assess targets and address security gaps, and invests in research and development for technological solutions to counter threats.

LEAD: MGMT, USSS

STAKEHOLDER: CBP, CISA, CWMD, FEMA, I&A, ICE, PLCY, TSA, USCG

9 The ability to conduct C-UAS activities was granted to the Secretary under 6 U.S.C. 124n. State, local, tribal, and territorial law enforcement jurisdictions have not been granted such authority, and therefore must rely on DHS to provide protection from UAS threats at qualified events.

OBJECTIVE 1.4:
Identify and Counter Emerging and Chemical, Biological, Radiological, and Nuclear Threats

DESIRED OUTCOME:
DHS and the homeland security enterprise are aware of emerging chemical, biological, radiological, and nuclear and health security threats to the homeland and are able to prevent and counter those threats.

Emerging technology — such as 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 — increase the variety and scope of threats for which we need to prepare and mitigate. Emerging technology empowers nation-states and non-state actors to threaten the homeland at a lower cost and with increased sophistication and transnational reach. However, these same technologies also present considerable opportunities for DHS to optimize operations to counter threat actors who exploit them. DHS is focused on reducing or mitigating the vulnerabilities, threats, and potential consequences posed by emerging technology through long-term research, experimentation, investments, policy development, and effective partnerships across the DHS enterprise.

DHS also remains vigilant against the full spectrum of CBRN threats, including those caused by natural events, accidents, or by actors who wish to do harm, such as nations pursuing clandestine CBRN weapons programs and terrorist groups seeking to acquire these weapons. The Countering Weapons of Mass Destruction Office (CWMD) leads and coordinates DHS efforts to safeguard the United States against chemical, biological, radiological, and nuclear threats posed by terrorists and other threat actors. International engagements with like-minded allies actively developing and testing new biodefense capabilities are opportunities for the United States to enhance access to solutions and knowledge developed outside of our borders.

Advancements in biological information and technology offer opportunities for finding cures for current and emerging diseases, but also present new risks and threats. To meet the current and future challenges in this space, the Department created the Office of Health Security (OHS), which serves as the principal medical, workforce health and safety, and public health authority for DHS. OHS will build resiliency, prevention systems, and the capacity for nimbleness as public health needs arise. DHS fosters preparedness by increasing the prevention and response capabilities of public safety personnel through security threat training and support to operational partners such as the Department of Health and Human Services, SLTT governments, and private sector actors.

LEAD: CWMD, I&A, OHS, PLCY, S&T

STAKEHOLDER: CBP, CISA, FEMA, ICE, TSA, USCG, USSS

MISSION TWO:
Secure and Manage our Borders

DESIRED OUTCOME:
U.S. borders are secured and managed efficiently, preventing threats from reaching the homeland while expediting and welcoming lawful trade and travel.

Over the past decade, there has been a fundamental change in trade, travel, and migratory patterns with far reaching impacts for DHS and the nation. Violence, food insecurity, severe poverty, corruption, climate change, the fall-out of the COVID-19 pandemic, and dire economic conditions have all contributed to a significant increase in irregular migration around the world and in the Western Hemisphere.

Transnational criminal organizations (TCOs) encourage and facilitate these migratory flows, spreading disinformation about what individuals will encounter along the route and at our border, so they can exploit migrants as part of a billion-dollar criminal enterprise. The increasing role that drug cartels are playing in human smuggling throughout the region is particularly concerning given their complete disregard for human life.

In response to these changing dynamics, DHS has made significant policy adjustments and investments in technology, human capital, and infrastructure to secure and manage our borders, putting in place tougher consequences for irregular migration within the confines of an outdated and broken immigration system. DHS also continues to work with international partners to stem extrahemispheric migration. In coordination with the Department of State, DHS also continues to deepen its engagement with partner nations to expand lawful pathways and processes, address the root causes of irregular migration, and reduce the flows of migrants to our Southern border. Moreover, the Department collaborates with interagency partners to expand the use of enforcement measures against entities and individuals that profit from irregular migration.

DHS concurrently facilitates the flow of lawful trade and travel while protecting our supply chains from threats and preventing exploitation by those who wish to do us harm. The Department's efforts protect the U.S. economy to ensure consumer safety and create a level playing field for American businesses. DHS prevents and investigates the illicit importation of goods and pirated content that violate the copyrights and trademarks of rights holders. DHS will continue to work with our partners across the HSE to accomplish this mission.

OBJECTIVE 2.1:
Secure and Manage Air, Land, and Maritime Borders

DESIRED OUTCOME:
The unlawful entry of people and goods across U.S. air, land, and maritime border is prevented.

DHS enhances the security of our air, land, and maritime borders using law enforcement methods, policies, and technological innovations that both facilitate inspection and processing at ports of entry while supporting prevention of illegal border crossings and denial of access to the United States to threat actors. These efforts include screening and vetting air travelers prior to their departure for the United States and inspecting persons and goods arriving in the United States.

DHS continues to make investments in policy, technology, human capital, and infrastructure to better position our Components to secure our nation's borders while enabling the implementation of an orderly immigration process and lawful trade and travel. Technological innovations in biometric collection for the purpose of vetting - and vetting at the earliest opportunity - significantly enhance our ability to confirm the identity and associated information of an individual seeking access to the United States. In the maritime domain, the Department will continue to support consistent, timely, and decisive maritime threat response coordination and the implementation of the *National Strategy for Maritime Security*.[10] DHS works with partners across the HSE to ensure border security operations are conducted in a safe, humane, and dignified manner, while upholding the privacy, civil rights, and civil liberties of migrants.

Along with increased resources, and process and infrastructure improvements at U.S. borders, DHS has issued several new rules that have expanded the capacity of DHS to secure the homeland. On May 11, 2023, as part of the Administration's work to prepare for the end of the Centers for Disease Control and Prevention's public health Order under Title 42 of the U.S. Code, and to return to processing all noncitizens under Title 8 immigration authorities, DHS and the Department of Justice (DOJ) issued a joint final rule, *Circumvention of Lawful Pathways* (Lawful Pathways rule), which incentivizes the use of lawful pathways by imposing a rebuttable presumption of asylum ineligibility, with limited exceptions. This was complemented by an historic use of the expedited removal process, in lieu of heavy reliance on a backlogged immigration court system, through which one's immigration processing and removal can be completed more swiftly, and significantly increasing the number of flights that ICE is able to operate to countries throughout the hemisphere.

On June 4, 2024, President Biden issued a Presidential Proclamation to temporarily suspend the entry of noncitizens across the southern border. The Secretary of Homeland Security and the Attorney General jointly issued an interim final rule that, consistent with the Proclamation, generally restricts asylum eligibility for those who irregularly cross the Southwest

10 See https://www.dhs.gov/national-plan-achieve-maritime-domain-awareness.

land and coastal borders. These actions enhance border security by facilitating timely decisions and delivering consequences for noncitizens without a lawful basis to enter or remain in the United States and who declined to avail themselves of available lawful pathways. These measures will be discontinued when there has been a sustained decrease in the number of encounters at the southern border such that the Department can manage border operations safely and effectively.

In parallel, this Administration has overseen a historic increase in access to lawful processes for migrants to come to the United States in a safe, orderly, and lawful manner. This includes an innovative approach that provided Cubans, Haitians, Nicaraguans, and Venezuelans with a safe, orderly way to come to the United States and imposed new consequences on those who crossed unlawfully, and CBP One, a scheduling tool to enable CBP to process individuals in a safe and orderly manner at ports of entry.

The work of managing the border must also include measures taken beyond our border. DHS actively works with interagency and international partners to stem hemispheric migration through increased use of transit visas and passenger vetting. For example, in coordination with DOS, DHS has expanded the use of enforcement measures against entities and individuals that profit from irregular migration, including sanctions on transportation companies that facilitate irregular migration. Interagency coordination has resulted in visa restrictions for countries who failed to stem migrant smuggling networks profiting off of irregular migration to the United States. DHS also supports the continued enforcement efforts of foreign partners through strong diplomatic relationships and information sharing to disrupt irregular migration.

DHS will continue to meet its mission of discouraging irregular migration and preventing the unlawful entry of people and goods across U.S. borders by utilizing every tool at its disposal including the aforementioned rules, technological enhancements, and procedural advancements.

LEAD: CBP, PLCY, TSA, USCG

STAKEHOLDER: CRCL, CWMD, I&A, ICE, OIDO, OSLLE, S&T, USCIS

OBJECTIVE 2.2:
Expedite Lawful Trade and Travel

DESIRED OUTCOME:
The flow of lawful trade and travel is secured and expedited, including by enforcing U.S. trade laws, safeguarding the transportation system, enhancing border infrastructure, and maintaining the accessibility of waterways.

DHS faces increasingly complex systems and threats in managing the flow of lawful trade and travel and in ensuring that the United States is secured against trade violations that pose risks to the public and our nation's values. DHS protects the United States from anticompetitive trade practices, duty evasion, counterfeit goods, and intellectual property theft that deprives the United States of substantial lawful revenue, harms individual consumers, and threatens U.S. economic security. Furthermore, DHS enforces export control laws to prevent the illicit export and transfer of sensitive military and dual-purpose technology and defense articles to transnational criminal organizations, terrorist groups, adversarial nation-states, and other nefarious entities operating around the world.

DHS applies expertise and technology to streamline processes and provide transparency and predictability in cross-border trade, including through the Automated Commercial Environment, National Centers of Excellence and Expertise, the Trusted Trader program, and the Free and Secure Trade program for clearance of low-risk shipments entering the United States from Canada and Mexico. CBP also works closely with the Government of Mexico to harmonize cargo data manifests, implement unified cargo processing at various border locations, and employ our respective authorized economic operation programs as part of our commitment to shorten wait times at ports of entry and expedite lawful trade and travel at the Southwest Border. DHS enforces customs laws, including within the priority trade issues of import safety, intellectual property rights, revenue, antidumping and countervailing duties, agriculture and quota, textiles and wearing apparel, and trade agreements.

DHS is similarly enforcing laws against environmental crimes as criminal organizations develop more complex smuggling networks to move fish, wildlife, and plant products illegally, such as raw timber, seafood, and animal parts. To address these challenges, DHS continues to leverage environmental authorities like the Lacey Act,[11] the Convention on International Trade in Endangered Species,[12] the Endangered Species Act,[13] and the United States-Mexico-Canada Agreement's environmental provisions[14] to ensure plant and animal products entering U.S. ports are produced, harvested, and sold legally.

11 18 U.S.C. 42; 16 U.S.C. 3371-3378; see https://www.cbp.gov/trade/entry-summary/public-laws-impacting-trade/public-law-110-246/amended-lacey-act/lacey-act.

12 See https://www.fisheries.noaa.gov/national/international-affairs/convention-international-trade-endangered-species-wild-fauna-and.

13 16 U.S.C. § 1531 et seq.; See https://www.fws.gov/law/endangered-species-act.

14 See https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/benefits-environment-united-states-mexico-canada-agreement.

DHS combats climate-related threats by developing incentives to promote environmentally beneficial trade practices and supply chains, as well as through strong environmental trade enforcement and investments in green innovation. Recent severe storms, floods, pandemics, and other disruptions have exposed the importance of strengthening U.S. supply chains. DHS continues to promote trade resilience and secure global supply chains to ensure the commercial flow of food, medicine, energy, and other vital goods and services.

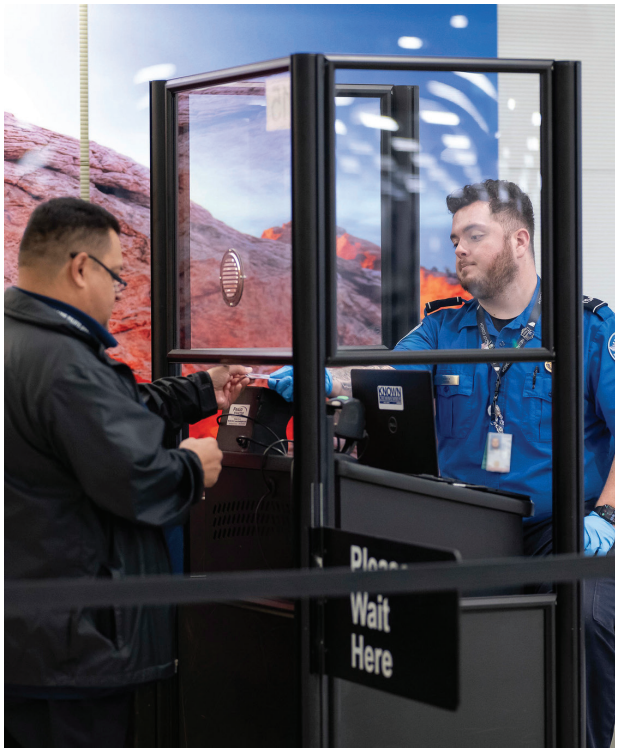
Travel and tourism are critical drivers of economic growth and employment in the United States. DHS facilitates and safeguards legitimate trade and travel across our borders, from container shipping to tourist and business travel. DHS enforces U.S. trade and travel laws as part of its mission to promote economic security and competitiveness, while also ensuring the safety of the American public. USCG safeguards waterways and the transportation system to ensure the lawful flow of trade and travel and promote U.S. resilience.

Meanwhile, the nation's economic prosperity and security are contingent upon sound and robust infrastructure. The Marine Transportation System (MTS), composed of critical infrastructure that forms our waterways, ports, and land-side connections, is a vital component of the nation's gross domestic product, contributing over $5.4 trillion annually in economic activity. The MTS is responsible for conveying 90 percent of commercial goods across the United States. DHS safeguards the MTS through robust safety and security standards that facilitate lawful trade and travel, while ensuring the safety, security, and environmental stewardship of our waterways.

DHS promotes lawful travel through DHS's trusted traveler programs, such as the TSA PreCheck® program and CBP's NEXUS and Global Entry programs, to expedite pre-vetted, low-risk travelers through security processes. Additionally, CBP's Preclearance Operations Program facilitates lawful travel by strategically stationing CBP officers and agriculture specialists at foreign airports to inspect and process travelers and baggage prior to boarding U.S.-bound flights. TSA and CBP are expanding the use of facial comparison and authentication technology, as part of a touchless travel experience, and are exploring ways to accept digital identity credentials, while protecting civil rights, civil liberties, and privacy. In addition, DHS promotes international travel and security by administering the Visa Waiver Program and the Electronic System for Travel Authorization.

LEAD: CBP, TSA, USCG

STAKEHOLDER: I&A, ICE, PLCY, S&T



OBJECTIVE 2.3:
Counter Transnational Criminal Organizations and Other Illicit Actors

DESIRED OUTCOME:
Threats from transnational criminal organizations to the homeland are disrupted.

DHS works closely with law enforcement partners at home and abroad to identify, investigate, and interdict the networks of criminals engaged in transnational organized crime, including those engaged in cybercrime, fraud, counterfeiting, and illicit smuggling or trafficking of persons, drugs, arms, sensitive technologies, finance, wildlife, or other natural resources. Furthermore, transnational criminal organizations exploit the trade system and utilize trade-based money laundering aimed at disguising the source of criminal proceeds from arms and narcotics trafficking, human smuggling, and other transnational crime using legitimate and illicit trade lanes. With both domestic and international partners, DHS identifies, investigates, prosecutes, and counters 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, DHS—alongside the Departments of Justice and State, as well as our SLTT and international partners—leverages respective authorities and capabilities to disrupt and dismantle transnational criminal organizations, including to combat the threat of fentanyl and other illicit narcotics. Arresting those who engage in transnational crime prevents further criminal activities, disrupts criminal operations, and deters others from participating in such groups. Coordinated Department surge efforts such as Operation Sentinel[15] have mapped foreign and domestic transnational criminal networks, their associates, and assets, revoked travel documents, suspended and debarred trade entities, and frozen financial assets connected to transnational criminal logistical networks. Operation Plaza Spike, announced April 2024, is a multi-agency, targeted effort to further disrupt the fentanyl supply chain by going after the cartel territories or "plazas" and the plaza bosses along the southwest border. Operation Apollo, a holistic counter-fentanyl effort that began in October 2023, in southern California, and expanded to Arizona in April 2024, focuses on intelligence collection and partnerships, and utilizes local CBP field assets augmented by federal, state, local, tribal, and territorial partners to boost resources, increase collaboration, and target the smuggling of fentanyl into the United States.

DHS's strategy has evolved to target not just fentanyl, but the tools and materials TCOs use to make it. The Department is interdicting and seizing precursor chemicals, pill press

15 See https://www.cbp.gov/newsroom/national-media-release/dhs-announces-operation-target-criminal-smuggling-organizations.

machines, die molds, and pill press parts used in the manufacturing process. Additionally, DHS is targeting pill press supply chains, pill press brokers, TCOs and U.S. recipients who are producing and moving fentanyl, and the money launderers who help facilitate this illicit trade. In September 2023 ICE Homeland Security Investigations (HSI) released its Strategy for Combating Illicit Opioids, an intelligence-driven approach to disrupting and dismantling TCOs and keeping dangerous substances like illicit fentanyl and other synthetic narcotics off America's streets. In October 2023, CBP released its Strategy to Combat Fentanyl and Other Synthetic Drugs, which aligns resources, enhances partnerships, and builds on the successful enforcement intelligence and data-driven operations CBP executed in FY 2023, while leveraging CBP's vast expertise and data holdings to disrupt the TCOs responsible for the production, distribution, and trafficking of illicit fentanyl, its analogues, and other synthetic drugs in the U.S.

LEAD: CBP, ICE, PLCY, TSA, USCG, USSS

STAKEHOLDER: CISA, I&A, OSLLE, S&T, USCIS

MISSION THREE:
Administer the Nation's Immigration System

DESIRED OUTCOME:
The U.S. legal immigration system is administered efficiently and fairly, and immigration laws are enforced.

The United States' past and future success is rooted in our heritage as a nation of immigrants, compassionately welcoming those seeking protection and drawing talent from around the world to our shores. However, DHS continues to confront increasing challenges due to the nation's broken and outdated immigration system. As such, DHS is undertaking various efforts to improve our nation's legal immigration system, such as expanding lawful pathways for migrants seeking opportunity in the United States and enforcing consequences for migrants who do not use these legal pathways.

Overall, DHS is working towards administering an efficient and fair immigration system in which we enforce our immigration laws and responsibly manage our borders, acknowledge the contributions that immigrants make to our society, support our humanitarian responsibilities as a nation, and encourage those who are eligible to embrace the benefits and responsibilities of citizenship.

OBJECTIVE 3.1:
Administer the Immigration System

DESIRED OUTCOME:
The U.S. immigration system is administered in an efficient and fair manner and immigration benefits are delivered expeditiously to eligible applicants.

DHS is committed to improving the nation's immigration system and safeguarding its integrity by efficiently and fairly adjudicating requests for immigration benefits. This includes a range of lawful pathways and processes, humanitarian programs such as the U.S. Refugee Admissions Program (USRAP), the U.S. asylum process, lawful permanent residence, and the naturalization process. To ensure that the legal immigration system is accessible and humane, DHS has worked to uphold America's promise as a nation of welcome and possibility by reducing backlogs, improving customer experience, addressing humanitarian needs, and strengthening employment-based immigration. As part of these efforts, we are working closely with the Department of State to resettle up to 125,000 refugees from around the world in FY 2024.

DHS, through U.S. Citizenship and Immigration Services (USCIS), and in coordination with our interagency colleagues, help meet the needs of

U.S. employers by issuing employment-based immigrant. Furthermore, the Department has worked with our interagency and private sector partners to expand access to H-2 nonimmigrant visa programs. For example, in FY 2024, the U.S. has issued nearly 450,000 H-2 visas—the highest number ever. Expansion of the H-2 program has helped deter irregular migration by making it easier for individuals seeking economic opportunity in the U.S. to do so lawfully, while at the same time addressing labor shortages facing U.S. businesses.

DHS has streamlined and improved access to work permits for eligible applicants who are already living in the United States. By increasing the maximum validity period of Employment Authorization Documents (EADs) to five years for adjustment of status applicants, we are strengthening our efforts to meet the demands of the U.S. labor markets. These endeavors have significantly reduced processing times for employment authorization documents (EADs) over the past year. Further, DHS announced a temporary final rule (TFR) to increase the automatic extension period for certain employment authorization documents (EADs) from up to 180 days to up to 540 days. This measure will prevent already work-authorized noncitizens from having their employment authorization and documentation lapse while waiting for USCIS to adjudicate their pending EAD renewal applications and better ensure continuity of operations for U.S. employers.

As part of our commitment to promoting family unity in the immigration process, DHS has expanded and modernized the Family Reunification Parole (FRP) processes, an umbrella term used for processes that allow certain nationals from Colombia, El Salvador, Guatemala, and Honduras, and their immediate family members, who have approved family-based petitions filed on their behalf by a U.S. citizen or lawful permanent resident, to come to the United States while they wait for their visa to become available.

DHS continues to address growing humanitarian needs around the globe, as individuals seek protection in the United States from oppression, violence, and other urgent circumstances. At a time when the world is experiencing the greatest displacement of people since World War II, our Department's dedicated employees continue to advance our humanitarian mission and provide protection to vulnerable populations. As part of this effort, DHS has launched programs to streamline the screening and adjudication of immigration benefits and related requests overseas. For example, in June 2023, DHS partnered with the Department of State to launch the Safe Mobility Initiative, a program that aims to accurately and efficiently determine a prospective migrant's eligibility for a lawful pathway to the U.S. before they make a dangerous and irregular journey north. Through Safe Mobility Offices (SMOs) in Colombia, Costa Rica, Ecuador, and Guatemala, DHS and its partners have met prospective migrants where they are, providing them with credible information about the U.S. immigration system and the opportunity to screen for lawful pathways to the U.S. and other countries while remaining overseas. Foremost among the innovations piloted out of the SMOs has been a mechanism for expediting the adjudication of refugee claims. Through a streamlined process designed in coordination with UNHCR and the Department of State, DHS has cut the average wait-time from initial screening to the resettlement of refugees by approximately one third.

LEAD: CBP, ICE, USCIS

STAKEHOLDER: CISOMB, CRCL, ICE, OIDO

OBJECTIVE 3.2:
Enforce U.S. Immigration Laws

DESIRED OUTCOME:
U.S. immigration laws are enforced in an effective and humane manner.

DHS continues to address the challenges presented by increased irregular migration at the Southwest Border with limited resources and within the constraints of an outdated immigration system. However, DHS works tirelessly to secure our borders through a combination of highly trained personnel, ground and aerial monitoring systems, and robust intelligence and information sharing networks. DHS enacts swift consequences to those who are apprehended crossing the border unlawfully—to include the expanded use of expedited removal—and has worked closely with the law enforcement partners, the interagency, and foreign partners to establish processes to ensure that removals are accomplished safely, efficiently, and quickly. To do this, DHS has digitized processes, surged personnel, and, with the cooperation of partner governments, increased removal flights, as described above in mission 2 and herein.

DHS, through U.S. Immigration and Customers Enforcement (ICE) has significantly expanded its capacity to ultimately remove those processed for expedited removal without a legal basis to stay in the United States. DHS is optimizing air charter contracts to ensure the maximum amount of repatriation flights can be effectuated weekly and has negotiated commitments from a range of countries from Central and South America and around the world, to conduct dozens of regular removal flights and will continue to expand those partnerships as needed. These commitments allow for the regular scheduling and processing of removal flights between the United States and relevant countries, indicating to those nationals that swift consequences will be delivered to those who attempt irregular migration. Additionally, through close partnerships with the interagency and partner countries, DHS has imposed various transit visa requirements and sanctioned charter airlines to drastically reduce the number of noncitizens arriving at the Southwest Border.

DHS also continues to explore the digitization of processes to improve the coordination of removals operations. For example, DHS developed electronic methods to enable more efficient issuances of travel documents and more accurate online identity verifications, allowing more efficient collaboration with partner countries to accept their nationals who have not established a legal basis to remain in the United States.

DHS established civil immigration enforcement priorities to most effectively achieve our goals with the resources we have. DHS has taken steps to better focus the Department's resources on the apprehension and removal of noncitizens who are a threat to our national security, public safety, and border security and advance the interests of justice by ensuring a case-by-case assessment of whether an individual poses a threat. Consistent with our exercise in prosecutorial discretion, DHS has ended the practice of mass worksite enforcement operations, and has established guidance that further ensures our enforcement efforts are being conducted responsibly and away from

protected areas such as schools, medical facilities, and places of worship.

For those noncitizens who arrive at the border who do not pose a threat to national security or public safety and do not warrant ICE's limited detention resources, DHS utilizes ICE's Alternatives to Detention (ATD) programs, including GPS monitors and enhanced supervision, such as curfews, and expanding case management services. Such an example can be found in ICE's Family Expedited Removal Management (FERM), which places certain heads of household for family units on ATD technology. The process provides supervision while the family awaits an interview to assess their credible fear of persecution or torture. While FERM initially began in four locations, DHS is quickly expanding to cities across the country and is removing families who are determined to be ineligible for relief and are ordered removed through this non-detained enforcement process. ATD, which has allowed noncitizens to remain in their communities and contribute to their family and community organizations, as they move through immigration proceedings. Technological enhancements such as these contribute to DHS's ability to effectively enforce U.S. immigration laws and enact swift consequences those who enter the United States through irregular migration.

LEAD: CBP, ICE, USCIS

STAKEHOLDER: OIDO, OSLLE, USCG

MISSION FOUR:
Secure Cyberspace and Critical Infrastructure

DESIRED OUTCOME:
The continuity of National Critical Functions is ensured through the security and resilience of critical infrastructure against cyber and physical threats and disruptions.

Cyber threats have evolved and increased. Nation-state threat actors are becoming increasingly sophisticated, targeting federal, state, and local government agencies, critical infrastructure entities, and others. Likewise, cybercriminals have increased malicious activities motivated by the significant profits they can make from using relatively accessible and affordable ransomware and malware tools. And, as commercial network technologies are woven increasingly into our businesses, personal lives, and critical federal and SLTT government functions, there remain cyber risks and vulnerabilities that leave those systems open to exploitation and disruption.

DHS works with government and private sector partners to manage national cyber and critical infrastructure risk. This heightened risk requires moving beyond individual actions and toward coordinated defensive actions and cybersecurity levels that bolster national security, economic security, and public health and safety. This is why DHS initiated the Cyber Safety Review Board, chaired by the Undersecretary for Strategy, Policy, and Plans, to review, assess, and provide actionable recommendations, in the wake of significant cybersecurity incidents, so that government, industry, and the broader security community can better protect our nation's networks and infrastructure in the future.

OBJECTIVE 4.1:
Support the Cybersecurity of Federal Civilian Networks

DESIRED OUTCOME:
Federal civilian information technology systems are secure from cyber threats and intrusions.

DHS secures its networks and the broader *.gov* environment. CISA enhances resilience by driving and facilitating the adoption of modern, secure, and resilient technologies, improving incident response capabilities, limiting supply chain risk to the U.S. Government, and increasing visibility into cyber threats across federal networks. DHS will leverage its authorities to the maximum extent possible to drive and measure the adoption of strong cybersecurity practices among federal civilian agencies. CISA develops and oversees the implementation of Binding Operational Directives (BODs), which require federal civilian departments and agencies to take action.[16]

CISA ensures that federal civilian agencies have access to the best cybersecurity tools, incident response support, and risk management capabilities to safeguard networks that support our nation's essential operations. CISA and PLCY participate in an Information and Communications Technology and Services (ICTS) Supply Chain Risk Management body[17], being established by the White House in the Office of the National Cyber Director, and another at the Department of Commerce.[18] In addition, the Interagency Security Committee,[19] led by CISA, safeguards U.S. nonmilitary facilities, from all hazards, by developing state-of-the-art security standards in collaboration with public and private homeland security partners.

PLCY also works through the Committee on Foreign Investment in the United States to secure federal civilian networks from the potential exploitation of cybersecurity vulnerabilities by means of foreign adversary investment in U.S. hardware and software providers. Altogether, these efforts improve the federal cybersecurity posture and incident response capabilities, limit the Federal Government's supply chain risk, and increase CISA's and other DHS Components' visibility across federal and contractor networks.

LEAD: CISA, MGMT, PLCY

STAKEHOLDER: ALL

---

16 A BOD is a compulsory direction to federal departments and agencies for purposes of safeguarding federal information and information systems. Section 3553(b)(2) of title 44, U.S. Code, authorizes the Secretary of Homeland Security to develop and oversee the implementation of BODs. Federal agencies are required to comply with these DHS-developed directives, except for statutorily defined "national security systems" and certain other systems operated by the Department of Defense and the Intelligence Community.

17 See https://www.dhs.gov/publication/supply-chain-security-leadership-subcommittee.

18 Pursuant to Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, and Executive Order 14028, Improving the Nation's Cybersecurity, as signed by President Biden.

19 See https://www.cisa.gov/resources-tools/groups/interagency-security-committee-isc.

OBJECTIVE 4.2:
Strengthen the Security and Resilience of Critical Infrastructure

DESIRED OUTCOME:
Strengthened security deters cyber and physical attacks or disruptions against critical infrastructure. When attacks occur, National Critical Functions experience minimal impact, and the equitable reconstitution of services is expedited.

DHS is using innovative and novel approaches to strengthen our nation's resilience across critical infrastructure systems, including National Critical Functions[20], and facilitates continuity with the goal that if a natural disaster, physical security breach, or cyber incident occurs, the critical services remain in place. DHS reduces risk across critical infrastructure sectors and the cyberspace ecosystem by supporting the development of secure software and technologies, driving cybersecurity innovations, cultivating the national cyber workforce pipeline to defend critical infrastructure, supporting international partnerships, and establishing norms of responsible state behavior in cyberspace.

The Department is committed to identifying vulnerabilities and ensuring that software and hardware are designed and built with security as a top priority. 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 sector. DHS will expand 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 must work with industry and the cybersecurity research community to ensure that technologies supporting critical infrastructure are appropriately secure before going to market and throughout their life cycle.

Through the *State and Local Cybersecurity Grant Program*, DHS helps enhance the cybersecurity of SLTT networks and public critical infrastructure by addressing cybersecurity risks, strengthening the cybersecurity of their critical infrastructure, and ensuring resilience against persistent cyber threats for the services they provide their communities. DHS is also working to ensure that all grants offered through the *Infrastructure Investment and Jobs Act*[21] secure SLTT's current and future infrastructure. These grants will allow states to build their infrastructure with secure-by-design, rather than approaching cybersecurity as an afterthought.

In close collaboration with the private sector, federal regulators, and Sector Risk Management Agencies (SRMAs), DHS will continue to provide guidance on how to build resilience and advocate for the adoption of best practices. CISA, USCG, and TSA work with businesses, communities, the transportation sector, and federal and SLTT

20 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 national security, economic security, public health or safety, or any combination thereof. See https://www.cisa.gov/national-critical-functions.

21 Pub. L. No. 117-58; signed into law by President Biden on November 15, 2021. See https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf.

government partners to provide training, tools, and resources related to critical infrastructure security. DHS leverages TSA's authorities for the issuance of security directives to the pipeline and surface transportation sectors, as well as security program amendments for the aviation sector and USCG regulatory authorities for the MTS. CISA provides training on a range of topics related to cyber and critical infrastructure security, including bombing prevention and active shooter preparedness. CISA also offers a rapid physical security assessment that assists with implementing effective security programs and helps stakeholders understand the benefits of a holistic security strategy that aligns cybersecurity and physical security functions with organizational priorities and business objectives. Successful public-private partnerships like the DHS-led Cyber Safety Review Board, the CISA Cybersecurity Advisory Committee, and the Joint Cyber Defense Collaborative (JCDC) will continue to be used to incorporate private industry recommendations and drive new approaches throughout the critical infrastructure ecosystem.

As an SRMA and the national coordinator for critical infrastructure security and resilience, CISA works with fellow SRMAs to reduce risk, and build resilience against, cyber and physical threats to the nation's infrastructure. This includes identifying which systems and assets are truly critical to the nation, understanding how they are vulnerable, and taking action to manage and reduce risks to them.

CISA also promotes cross-sector critical infrastructure resilience by leveraging the Federal Senior Leadership Council—the primary cross-sector council that convenes SRMAs—to ensure it is supporting SRMAs effectively and implementing recommendations from "9002(b) reports."[22]

DHS will work to change business incentives to drive the design of more secure software and the adoption of best practices. To ensure that our collective security posture is aligned with national and economic security needs, private industry must be incentivized to consistently adopt secure-by-design and secure-by-default principles in commercial software products and services. In October 2022, cross-sector Cybersecurity Performance Goals (CPGs) were released to provide a benchmark for critical infrastructure organizations to measure and improve their cybersecurity maturity.[23] The CPGs provide voluntary guidance to critical infrastructure partners to help them prioritize security investments toward areas that will have the greatest impact on their cybersecurity, and they are to be implemented in concert with the National Institute of Standards and Technology's Cybersecurity Framework. Critically, the CPGs are designed to ensure security levels commensurate with national security, economic security, and public health and safety. CISA will be working with SRMAs and critical infrastructure entities to ensure adoption of the CPGs and the release of subsequent guidance.

---

22 Pub. L. No. 116-283, § 9002(b), *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, which requires a periodic reevaluation and report to the President for his/her consideration. See https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf.

23 In accordance with the *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (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/), CISA released the *CPG: Cross-Sector Cybersecurity Performance Goals 2022* (see https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf).

DHS supports state, local, and other partners in securing election infrastructure, with CISA acting as DHS's hub for identifying risks to election infrastructure and ensuring election officials and their private sector partners have the information they need to manage risks to their systems. CISA gains unique insights from the services and assessments offered through voluntary partnerships with elections officials and venders, and from the contributions of federal partners like the FBI, the U.S. Election Assistance Commission, and the Intelligence Community.

LEAD: CISA, PLCY, TSA, USCG

STAKEHOLDER: CBP, FEMA, I&A, S&T

OBJECTIVE 4.3: Assess and Counter Evolving Cyber and Emerging Technology Risks

DESIRED OUTCOME:
DHS and the homeland security enterprise achieve awareness of cyber threats and emerging technology risks and develop and field capabilities to counter related threats.

DHS advances capabilities to actively detect threats across government networks and works with industry partners to enhance the understanding of threats targeting private networks. The USCG's Maritime Cyber Readiness Branch and Cyber Protection Teams collaborate with maritime industry to harden the MTS from cyber vulnerabilities that threaten economic and national security. In addition, CISA collaborates with federal agencies and private industry to gain greater visibility into vulnerabilities and adversary activity occurring across government and critical infrastructure networks. Specifically, the National Risk Management Center's (NRMC's) dynamic, cross-sector risk management process builds from a foundation of risk analysis to spur government and industry collaborative risk reduction. The interconnectedness of critical infrastructure and sophistication of threats and hazards means that the consequences of an attack or incident no longer impact only one entity or sector. The NRMC conducts functions-based risk assessments to illuminate these complex risks and point the way toward collective risk reduction opportunities.

The JCDC unifies public and private entities across the global cyber community in the collective defense of cyberspace. JCDC members gather, analyze, and share actionable cyber risk information to enable synchronized, holistic cybersecurity planning, cyber defense, and response. The JCDC provides real-world value and proactive solutions to defend today and prepare for tomorrow. The JCDC is a leader in integrated public-private sector cyber defense planning, cybersecurity information fusion, and the dissemination of cyber defense guidance to reduce risk to critical infrastructure and National Critical Functions. Additionally, DHS will expand work with commercial providers through partnerships like the JCDC to share information about ongoing malicious campaigns and, ultimately, to coordinate defensive efforts. As transforming technologies surface, DHS must

remain vigilant and agile to identify and mitigate these key emerging technology risks, such as the transition to post-quantum cryptography.[24]

DHS can achieve visibility of vulnerabilities and adversary activity at scale by increasing resources for broader deployment of federal network dashboarding, detection, and reporting capabilities and expanding access to voluntary information feeds from critical infrastructure industry partners. Using this data, DHS will identify and correlate trends to better understand the attack surface and enhance understanding of cyber risk and endpoint detection capabilities across federal agencies. DHS will work with its partners to incentivize identification and response to vulnerabilities. CISA has developed an Automated Indicator Sharing initiative to enable the timely exchange of cyber threat indicators and defensive measures among federal and non-federal entities. These cyber threat indicators and defensive measures are shared consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats, in a manner that ensures appropriate incorporation of privacy, civil liberties, and other compliance protections. Additionally, the U.S. Computer Emergency Readiness Team collaborates with international partners to broaden the scope of our cyber security effort in disseminating cyber threat warning information, sharing vulnerability information, and coordinating across stakeholders.

Through S&T's relationships with international partners, DHS shares information on emerging technology in order to understand their risks and opportunities for the HSE. CISA will enable timely and coordinated vulnerability disclosure and recommend appropriate mitigation countermeasures to ensure that network defenders are able to identify and proactively mitigate threats to their most critical networks before damaging intrusions occur.

DHS is at the forefront of employing Artificial Intelligence (AI) and machine learning technologies and serves as an example of responsible adoption of AI by government Agencies. To that end, the Secretary has appointed DHS's first Chief AI Officer to promote AI innovation and responsible use within the Department. The Chief AI Officer advises the Secretary and Department leadership on AI strategy and risk mitigations. The Chief AI Officer also leads the Department's engagements with experts across its agencies, mission-spaces, and disciplines to ensure a holistic approach to the responsible use of AI at DHS.

DHS is tasked with critical roles related to AI under Executive Order 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." The Department is responsible for five tasks under the EO. DHS will manage AI in critical infrastructure and cyberspace through CISA and the Artificial Intelligence Safety and Security Board (AISSB). DHS will promote adoption of AI safety standards globally through the Office of Policy and Office of International Affairs. The Department will combat AI-related intellectual property theft through Homeland Security Investigations and the Intellectual Property Rights Center. We streamline the immigration process to attract AI talent to the United States. Finally, the Department will reduce the potential misuse of AI to proliferate weapons of mass destruction.

The AISSB brings together AI experts from the private sector, civil society, academia, and

24 Through partnership with the National Institute of Standards and Technology, DHS created a roadmap for those organizations that should be taking action to prepare for a transition to post-quantum cryptography. See https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf.

government. The purpose of the AISSB is to advise the Secretary, the critical infrastructure community, and the broader public on the safe and secure development and deployment of AI. The board will provide information and recommendations for improving security, resilience, and safety, including publishing specific and actionable principles, guidelines, and best practices for the use of AI in critical infrastructure. The board will also develop processes to review and respond to incidents related to the use of AI in critical infrastructure.

LEAD: CISA, I&A, S&T, PLCY

STAKEHOLDER: CBP, TSA, USCG

OBJECTIVE 4.4: Combat Cybercrime

DESIRED OUTCOME:
Criminal actors are deterred and prevented from committing criminal acts in cyberspace or undermining the integrity of financial payment systems, and those who commit criminal acts are swiftly detected and held accountable.

DHS will disrupt threats by ensuring USSS and HSI remain capable of combatting 21st century crimes. DHS will continue to strengthen our efforts as part of the law enforcement community to pursue, counter, reduce, and disrupt illicit cyber activity by leveraging our specialized expertise and capabilities to target financial and transborder cybercrimes. The transnational and cross-jurisdictional nature of cyberspace, as well as the sheer size of the challenge, require closer collaboration with other federal, state, local, and international law enforcement partners, along with the private sector.

DHS will empower the USSS's network of Cyber Fraud Task Forces, and leverage training for law enforcement partners at the National Computer Forensics Institute, to develop this collaboration. DHS also combats ransomware through CISA's Joint Ransomware Task Force, which convenes interagency partners to coordinate an ongoing nationwide campaign against ransomware attacks.

The DHS Cyber Crimes Center (C3) supports HSI's mission through coordination of investigations of cyber-related criminal activity and provides forensic, intelligence and investigative support services across all HSI programmatic areas. C3's mission is to keep pace with emerging computer technology and cyber processes by proactively using these new technologies to combat criminal activity and address vulnerabilities; disseminating to field offices and worldwide law enforcement and intelligence organizations the most current trends, risks, procedures, lessons learned and investigative leads; and supporting investigations into cyber related criminal activities and vulnerabilities with state-of-the-art cyber investigative methods and computer forensic techniques.

LEAD: ICE, USSS

STAKEHOLDER: CISA, I&A, OSLLE, PLCY

MISSION FIVE:
Build a Resilient Nation and Respond to Incidents

DESIRED OUTCOME:
The nation is resilient to the impacts of natural and man-made disasters, including disasters exacerbated by the impacts of climate change, and can respond rapidly and effectively to the effects of multiple simultaneous disasters across the country.

The HSE will be called upon to respond to increasingly complex, simultaneous, and interconnected incidents. In recent years, DHS led the federal response to incidents ranging from the COVID-19 pandemic, irregular migration at the Southwest Border, cyberattacks on critical infrastructure, and the rapid resettlement of thousands of vulnerable Afghan nationals through Operation Allies Welcome. DHS was also designated by the President as the lead federal agency to coordinate domestic preparedness and response efforts following 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 nongovernmental entities.

Climate change-related risks pose a grave threat to the safety, security, and prosperity of our communities today, in the near-term, and in the long-term. The Department, through FEMA, has responded to natural incidents of intensifying scale and frequency in recent years, including the widespread impact of Hurricane Ida in 2021 and Hurricanes Fiona and Ian in 2022, the devastating wildfire in Maui and severe flooding from atmospheric rivers in California and Nevada in 2023, and the multiple tornadoes that affected dozens of communities across the country in the Spring of 2024. From extreme heat and fires in the West, extreme storms in the Southeast, and flooding in the Midwest, to melting ice in the polar regions, DHS plays a leading role in helping communities to develop resilience and respond to these events. DHS reduces risk to communities, businesses, and individuals by providing relevant prevention and preparation information; offering grants and technical assistance; promoting innovation; and issuing regulations to increase national resilience and adaptation to minimize the hazards aggravated by climate change.

Disruptions caused by the global forces of pandemic disease and climate change have given new impetus to building resilience to all hazards and developing new approaches to prepare for, prevent, protect against, mitigate, and if necessary, respond and recover to natural and man-made events. As part of its responsibilities, DHS invests in community resilience; provides information on minimizing risks and improving disaster readiness through response and recovery capabilities; makes the disaster assistance process more accessible and equitable; and implements the Department's *Environmental Justice Strategy,*[25] the *DHS Strategic Framework for Addressing Climate Change,*[26] and the *DHS Climate Action Plan.*[27]

25 See https://www.dhs.gov/dhs-environmental-justice-strategy.

26 See https://www.dhs.gov/sites/default/files/publications/dhs_strategic_framework_10.20.21_final_508.pdf.

27 See https://www.dhs.gov/sites/default/files/publications/21_1007_opa_climate-action-plan.pdf.

OBJECTIVE 5.1:
Coordinate Federal Response to Incidents

DESIRED OUTCOME:
DHS achieves effective coordination amongst federal and supports state, local, tribal, and territorial responses to incidents.

DHS responds continuously to multi-domain incidents stretching across its Operational Components. DHS leverages its collective expertise and capabilities to manage all types of incidents, whether covered by the Stafford Act[28] and the Cyber Response and Recovery Fund, or otherwise. DHS also leverages its reserve and surge capacities, including the DHS Surge Capacity Force,[29] the DHS Volunteer Force,[30] and USCG Reserve.[31]

DHS coordinates the national response to significant cyber incidents, working closely across the Operational Components, the interagency, and private sector to ensure greater unity of effort and a whole-of-nation response. As part of this response, DHS provides assistance to cyber-impacted entities, analyzes the incident's potential effects across critical infrastructure, and investigates those responsible in conjunction with law enforcement partners. For example, in early 2022, CISA developed a Russia-Ukraine Tensions Plan with JCDC members that lays out phases and objectives of operational coordination between the U.S. Government and private sector partners amidst escalating geopolitical tensions. The same stakeholders then conducted a tabletop exercise to practice a 'test' scenario and run through operational coordination. The plan serves to guide and align collective operational posture and supports the ability to synchronize defensive actions to mitigate harmful impacts to U.S. critical infrastructure from Russian cyber operations.

DHS will develop a robust response capability matching the increasingly cross-functional nature of incidents, including those related to weapons of mass destruction, and deliver effective consequence management. This includes enhanced external affairs and strategic communication functions, key roles for DHS during an incident. The Department must ready its entire workforce—not only those already trained in the National Incident Management System[32]—to execute incident response capabilities as well as regularly exercise and develop them alongside federal, SLTT, and nongovernmental partners. With support from Congress, DHS created the new Homeland Security Incident Management Assistance

---

28 *Robert T. Stafford Disaster Relief and Emergency Assistance Act* (Pub. L. No. 100-707; 42 U.S.C. 5121-5207); see https://www.fema.gov/sites/default/files/documents/fema_stafford_act_2021_vol1.pdf.

29 The Post-Katrina Emergency Management Reform Act of 2006 (Public Law 109-295) established the Surge Capacity Force (SCF) to deploy Federal employees in the aftermath of a catastrophic event to help support response and recovery efforts.; See https://www.dhs.gov/surge-capacity-force.

30 The DHS Volunteer Force provides humanitarian and logistical support for humanitarian and security crises.

31 The USCG Reserve is a flexible, responsive operational force that exists to support the USCG roles of maritime homeland security, national defense (domestic and expeditionary), and domestic disaster operations.

32 The National Incident Management System guides all levels of government, nongovernmental organizations, and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from incidents. See https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf.

Team which will support these incidents at the Secretary's direction and coordinate the Department's resources for response efforts. Only by normalizing interoperability will the entire HSE be capable of delivering the incident responses the nation deserves.

LEAD: CISA, FEMA, MGMT, USCG

STAKEHOLDER: ALL

OBJECTIVE 5.2: Strengthen National Resilience

DESIRED OUTCOME:
The nation is more resilient to the effects of disaster and climate-related risk.

DHS will ready the nation to respond to, and recover from, all hazards and threats. DHS will actively combat climate change by prioritizing the creation and expansion of programs that incentivize communities and individuals to invest in climate resilience, including the Building Resilient Infrastructure and Communities Grant Program and the National Flood Insurance Program (NFIP). This will also include programs that ensure the equitable treatment of communities that previously have not been the focus of disaster mitigation and resilience programs. This ensures that programs and incentives are risk-informed, equitable, and accessible to communities and individuals in underserved populations that often suffer disproportionately from disasters. This includes reforming our grant system to make it more equitable and accessible by identifying and removing barriers to participation and improving accessibility to all communities. For example, in the 2023 Nonprofit Security Grant Program cycle, DHS incentivized increased participation from nonprofits that have never received funding and for nonprofits located in underserved communities. DHS also simplified the application for 2023 Nonprofit Security Grant Program sub-applicants and conducted targeted outreach to communities, resulting in a roughly 50 percent increase over FY 2022 applications.

As natural disasters grow in frequency and magnitude, the time it takes for communities to recover has also increased. Research shows that the damage and disruption caused by these disasters can be reduced when communities take certain pre-disaster actions, such as addressing aging infrastructure. Hazards and threats do not respect borders and DHS will work with international partners who are addressing similar threats from climate change to share effective practices to protect communities and infrastructure.

In addition to building resilience to natural disasters, we will also build resilience to other threats, particularly in the areas of cyber, CBRN, domestic terrorism, and more. As such, DHS will continue to work to fortify and build upon the nation's resilience by leveraging grants, programs, and services that will assist private and public entities in how they respond to and recover from these hazards and threats. This includes guidance on greenhouse gas emission reduction and the authority to use regulation where necessary.

LEAD: FEMA

STAKEHOLDER: CISA, S&T, USCG

OBJECTIVE 5.3:
Support Equitable Community Recovery

DESIRED OUTCOME:
All communities have access to resources to support recovery after a disaster.

We will instill equity as a foundation of emergency management. A community's history, culture, demographics, and economic status influence its ability to access federal services, and it is DHS's responsibility to ensure that disaster resources can be accessed and leveraged by all communities in ways that meet their needs and support their recovery following a disaster. In 2021, FEMA implemented changes to accept a broader range of homeownership and occupancy documentation to improves access to disaster assistance for underserved communities. FEMA built on this work in 2024, making major changes to the Individual Assistance programs to address historic challenges faced by disaster survivors, including flexible funding provided directly to survivors when they need it most, expanded eligibility to help more people recover faster, a simplified application process to meet survivors' individual needs, and easier-to-navigate websites to apply for assistance and transitional shelter.

To better serve Tribal Nations, FEMA also published its first ever "National Tribal Strategy" to take critical steps toward delivering training and assistance that meets the unique needs of tribal communities. DHS will continue to drive transformational change to break down barriers that underserved communities have faced historically accessing and leveraging recovery resources by reforming the disaster assistance process to make it more equitable and accessible, and by partnering with agencies to better sequence federal disaster recovery programs. DHS will, therefore, identify potential gaps in recovery programs that, when mitigated, will better enable individuals and communities to use federal support to drive their own recovery. By instilling equity as a foundation of emergency management and striving to meet the unique needs of underserved and under resourced communities, we can build a more resilient nation.

LEAD: FEMA

STAKEHOLDER: NONE

OBJECTIVE 5.4:
Enhance Training and Readiness of First Responders

DESIRED OUTCOME:
First responders are trained and ready to respond to incidents.

Emergency management is a shared responsibility among all levels of government, the private sector, nonprofits, and individuals. DHS provides training and professional development to ensure emergency managers and first responders are prepared. Through engagement, training, and exercise, DHS improves the response capabilities of first responders and ensures that when high consequence natural disasters or other events occur, those responders know where to go for the expertise and resources their communities need. DHS will increase the nation's emergency management capabilities through expanded training to include individuals and community groups that help their communities respond to and recover from disasters, but who may not identify as "emergency managers." For example, FEMA and the DHS Center for Faith-Based and Neighborhood Partnerships engaged with diverse communities across the country to better understand how to meet their needs for disaster preparedness by sharing resources and direct access to disaster management experts.

FEMA also works to ensure preparedness information is available to all communities, especially those often hit hardest by disasters and emergencies. In 2021 and 2022, FEMA's Ready Campaign launched its first-ever public service preparedness campaigns aimed at underserved communities. Investing in readiness at all levels enables emergency managers to leverage state, local, tribal, territorial, and national resources as they coordinate within their community to create a more efficient, effective, and unified response.

Climate change is a critical challenge facing emergency managers today — and it will continue to shape the next several decades. To meet this challenge, we must understand how climate change impacts our collective work. Increasing the climate literacy of emergency managers, communities, and across DHS Components is a key area for enhanced training that will improve disaster outcomes. When individuals and communities are climate literate, they are better positioned to take the necessary steps to apply that knowledge to build safe, secure, and resilient communities. Similarly, incorporating equity considerations into training increases the ability of emergency managers to understand the complexities within their communities and tailor solutions to meet unique needs. DHS will grow its climate literacy by integrating climate science into policy, programs, partnerships, field operations, and training, and by developing a broad nationwide understanding of climate adaptation competencies for first responders and communities.

LEAD: CWMD, FEMA

STAKEHOLDER: CBP, CISA, FLETC, OSLLE, S&T, USCG

MISSION SIX:
Combat Crimes of Exploitation and Protect Victims

DESIRED OUTCOME:
DHS and its partners identify crimes of exploitation and protect victims through expanded education, digital forensic technology, support services, and partnerships with federal, state, local, tribal, territorial, international, and private sector partners.

Crimes of exploitation—including online child sexual exploitation and abuse (CSEA), human trafficking, and labor exploitation—occur at alarmingly high rates. 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.

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 36 million cyber tips in 2023, corresponding to more than 88 million images and videos of child sexual abuse—a roughly 75 percent increase in just five years. These numbers represent only detected CSAM on the open web; they do not include the massive amount of CSAM produced and shared on the dark web and through livestream and closed platforms.

DHS fights all types of human trafficking, including sex trafficking and forced labor. 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. 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 occur transnationally, with victims lured into the United States and exploited for labor, services, or commercial sex upon arrival. Trafficking frequently involves multiple forms of related criminal conduct, including financial crimes, document fraud, racketeering, immigration violations, narcotics distribution, sexual exploitation, violent offenses, and labor infractions.

Forced labor occurs when individuals are compelled against their will to provide labor or service based on force, fraud, or coercion. Victims may be any age, race, religious affiliation, gender identity, immigration status, 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 noncitizens with or without legal status. According to recent global estimates, 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 vast majority of them being women and girls.

"Combat crimes of exploitation and protect victims" was added as a new Homeland Security mission in the 2023 QHSR. This step reflects the overriding importance of supporting victims and stopping perpetrators, and the heroic work of the DHS workforce and our partners in the HSE. Every day, DHS works 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 trafficking and other crimes of exploitation. DHS is prioritizing the fight against these crimes by growing the Center for Countering Human Trafficking (CCHT) and other offices involved in this work. - Additionally, the HSI Cyber Crimes Center was elevated to the DHS Cyber Crimes Center in recognition of its expanding functions that reach beyond the traditional law enforcement domain and involve broader Department equities.

OBJECTIVE 6.1: Enhance Prevention through Public Education and Training

DESIRED OUTCOME:
The DHS workforce, Departmental partners, and the public are aware of indicators that help identify and prevent crimes of exploitation.

DHS 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. To remedy this, DHS is committed to educating our workforce, our HSE partners, and the public on how to identify and prevent crimes of exploitation. When investing in successful prevention efforts, stakeholders combating all elements of these illicit activities will have fewer victims to identify, assist, and protect, and fewer criminals and criminal networks to investigate, prosecute, and dismantle. Public education efforts raise awareness around best practices to identify human trafficking, child sexual exploitation and abuse, forced labor, and the related illicit financial activity associated with these crimes. With respect to human trafficking, for example, DHS personnel holding public-facing jobs throughout the United States are well positioned to witness indicators of potential human trafficking, interact with potential traffickers and victims, and report suspicious activity. An informed public and educated workforce will be our first layer of defense in preventing crimes of exploitation.

In FY 2023, the DHS Blue Campaign—the Department's national human trafficking public awareness initiative—trained more than 280,000 Federal Government, nongovernmental organization, industry, law enforcement, and public participants on how to recognize the indicators of human trafficking. The USCG

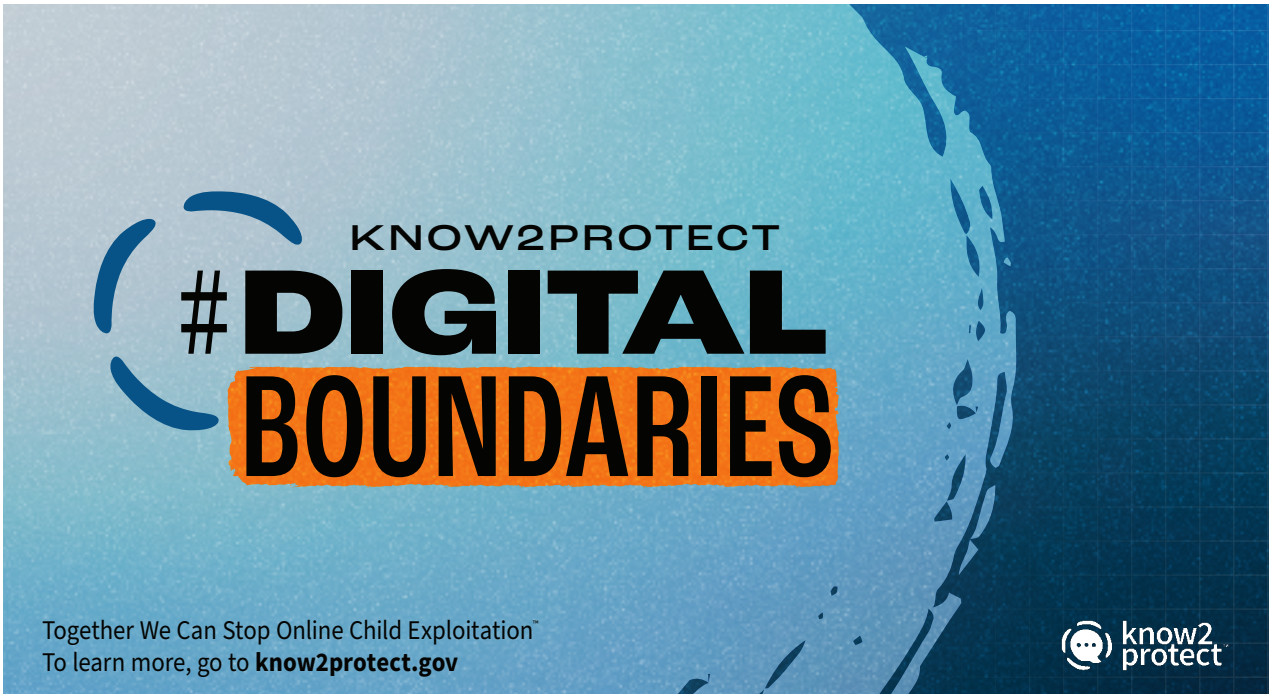
directly engages with vulnerable communities in the maritime domain to increase reporting.[33] Furthermore, FLETC trained more than 3,100 law enforcement officers, representing more than 90 law enforcement agencies, on how to recognize and respond to potential trafficking cases.

In April 2024, DHS launched a first-of-its-kind national public awareness campaign, Know2Protect, to counter the rapidly escalating crisis of online CSEA. The campaign will 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 DHS Cyber Crimes Center as a permanent Department function. This new campaign—which will reach target audiences through strategic public-private partnerships with technology companies, sports leagues, and youth-serving organizations—will build on existing public education efforts currently offered across the Department.[34]

As the threat evolves, DHS continues to refine and develop robust training so the public and our HSE partners will have the information needed to counteract perpetrators' techniques and tactics.

LEAD: CBP, FLETC, ICE, OPE, PLCY, TSA, USCG, USCIS, USSS

STAKEHOLDER: CISA, CRCL, I&A, OSLLE



33 With additional authorities provided in the National Defense Authorization Act of 2023, the Coast Guard is the lead enforcement agency for ensuring workplace safety in the maritime domain, combating crimes of exploitation and sexual misconduct, directly engaging with vulnerable communities to increase reporting, and removing Coast Guard-licensed commercial mariners through the suspension and revocation process.

34 ICE HSI operates Project iGuardian in partnership to educate children, teens, parents, and teachers throughout the country about online safety and how to stay safe from sexual predators. Educated over 186,000 kids, teens, parents, and teachers about internet safety and how to stay safe from sexual predators through the iGuardian program. USSS Childhood Smart Program Ambassadors educated more than 112,000 children, parents, and teachers across 31 states and the District of Columbia about how to prevent online sexual exploitation and child abduction. October 2023 - April 2024". https://www.dhs.gov/news/2024/04/17/fact-sheet-how-dhs-combating-child-exploitation-and-abuse

OBJECTIVE 6.2:
Identify, Protect, and Support Victims

DESIRED OUTCOME:
Increase identification of victims and provide them with the services and support they need to prevent revictimization and protect them from further trauma.

In October 2021, Secretary Mayorkas directed that DHS operations and activities promote a victim-centered approach to minimize additional trauma endured by many victims, mitigate any undue penalization, and provide needed stability and support to victims of trafficking and exploitation.[35, 36] This approach helps survivors begin to rebuild 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 to incorporate a victim-centered approach into all relevant policies and programs in FY 2022.

DHS agencies have already taken important steps in accordance with the Secretary's directive. ICE, for example, issued a new directive, *Using a Victim-Centered Approach with Noncitizen Crime Victims,*[37] 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. In addition, HSI's Child Exploitation Investigations Unit (CEIU), part of the Cyber Crimes Center, a global leader in CSEA law enforcement operations, utilizes state-of-the-art technologies combined with traditional investigative techniques to identify and rescue child victims throughout the world.[38] DHS is committed to expanding the HSI Victim Assistance Program, specifically the number of victim assistance personnel by 40 percent in the first year and subsequently 60 percent in the following year. Through USCIS, DHS significantly increased the protections granted to qualifying victims of human trafficking and other serious crimes, offering victims safety, stability, and a means to become self-sufficient.

DHS provides immigration relief to certain individuals who are victims of crimes of exploitation. For example, 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

35 See https://www.dhs.gov/news/2021/10/20/dhs-takes-victim-centered-approach-first-anniversary-center-countering-human.

36 Institutionalizing a victim-centered approach means providing nonjudgmental assistance with an emphasis on self-determination. *A victim-centered approach prioritizes* assisting victims in making informed choices, restoring victims' feelings of safety and security, and safeguarding against policies and practices that may inadvertently re-traumatize victims. This includes protections against unnecessarily or inappropriately penalizing or subjecting them to enforcement actions. A victim-centered approach should also incorporate a trauma-informed, survivor-informed, and culturally sensitive approach. See https://www.whitehouse.gov/wp-content/uploads/2021/12/National-Action-Plan-to-Combat-Human-Trafficking.pdf.

37 See https://www.ice.gov/doclib/news/releases/2021/11005.3.pdf.

38 In 2023 the Cyber Crimes Center hosted Operation Renewed Hope, a three-week task force resulting in 316 referrals with possible identity or country of origin identifications and 87 victims positively identified, including 35 minor children. Operation Renewed Hope was conducted with the support of 30 HSI special agents, analysts, computer forensic analysts, and task force officers, as well as partners from FBI, USDOJ Child Exploitation and Obscenities Section (CEOS), NCMEC, the Virginia State Police ICAC Task Force, and 14 foreign law enforcement agencies.

may be potential witnesses or have filed federal civil actions – by launching an online application and processing system for law enforcement to expedite access to the Continued Presence system. This will help victims and survivors restore self-sufficiency and seek justice. 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. In April 2024, USCIS announced a *final rule* to strengthen the integrity of the *T nonimmigrant status* (T visa) and ensure eligible victims of human trafficking can access protections and stabilizing benefits on a timely manner. T nonimmigrant status enables certain victims of human trafficking to remain in the United States for an initial period of up to four years.

DHS recognizes that the trauma associated with these crimes extends beyond survivors; it also affects our personnel. Too often individuals underestimate the personal effects of encountering human trafficking and child sexual exploitation in the line of duty. Without support and treatment for the personnel doing this critical work, they may experience trauma or other job-related stressors that may diminish their capacity to contribute to this important mission. DHS will ensure its employees have access to peer support programs and the Employee Assistance Program to protect the health and well-being of its most vital resource, its people. DHS will further require personnel encountering human trafficking and child sexual exploitation to access support on a regular basis, where possible.

Incorporating proven and promising victim-centered practices into DHS policies, programs, and protocols will enhance every aspect of DHS's work to counter crimes of exploitation. Continued improvements focused on identification, protection, and support lead to holding more perpetrators accountable and bringing more victims safety, stability, and available protections.

LEAD: CBP, ICE, USCIS

STAKEHOLDER: CRCL, OHS, PLCY, S&T, TSA, USSS

OBJECTIVE 6.3:
Detect, Apprehend, and Disrupt Perpetrators

DESIRED OUTCOME:
A robust homeland security enterprise works seamlessly to increase the number of perpetrators apprehended and disrupt networks that engage in crimes of exploitation.

As a leader in the fight against crimes of exploitation, DHS works with partners at every level to investigate crimes like human trafficking and bring perpetrators to justice.

Detecting crimes of exploitation is challenging and perpetrators will continue adjusting their techniques to evade our detection methods. We must invest in the latest tools and technologies to combat traffickers' constantly changing tactics to avoid detection, including those who move their internet servers overseas. In addition to identifying and/or rescuing child victims of sexual exploitation, CEIU detects and apprehends producers and distributors of child sexual abuse material 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, livestreams, and other internet-based platforms.

DHS will also modernize and improve our tools to detect and investigate these crimes. The CCHT will implement the authorities and resources identified in the *Countering Human Trafficking Act*[39] to support and advance DHS's unified efforts to combat human trafficking. This includes improving and modernizing systems and processes, increasing DHS efforts to combat forced labor in supply chains by holding accountable manufacturers of goods produced with forced labor worldwide, increasing support for research and data collection efforts to better understand the scope and dynamics of human trafficking, and informing the development of more effective prevention and intervention strategies. These actions will enable DHS to improve its collaborative approach to focus efforts and resources on areas where we have greater impact.

Some emergent technologies, like anonymous browsing, allow human traffickers to evade law enforcement. S&T's research in this area is focused on improving the detection, analysis, and understanding of human trafficking; examining human trafficking as a process and its impacts on individuals, communities, the United States, and the systems within; and conducting gap analyses to identify aspects of human trafficking (for either victims or perpetrators) in greatest need of empirical research. During FY 2022, S&T worked with the Homeland Security Operational Analysis Center to develop a long-term research agenda focused on labor trafficking. The research will fill knowledge gaps and guide future social science research investments related to labor trafficking in the United States. S&T has deployed unique forensic tools for operations using emerging technology and continues to conduct research and development toward additional analytic tools to aid in victim identification and investigations. Using these S&T digital forensic tools has

39 See https://www.dhs.gov/news/2022/12/29/president-biden-signs-legislation-codifies-and-expands-dhs-fight-against-human

reduced processing time for massive amounts of bulk data from weeks to days.[40]

To protect victims, the USSS provides forensic and investigative assistance[41] to the NCMEC and state and local law enforcement agencies in support of investigations involving missing or exploited children. The USSS is committed to the protection of victims via a two-pronged strategy that combats CSEA with advanced investigative and forensic support to state and local law enforcement partners and aggressively investigates sextortion, a predatory fraud scheme which oftentimes results in the illicit sexual exploitation of minors.[42]

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 form of human trafficking. DHS takes enforcement actions on a wide variety of goods made with forced labor, such as diamonds mined in Zimbabwe, tobacco grown in Malawi, and seafood harvested by fishing vessels and fleets that use forced labor. Furthermore, DHS oversees the implementation of the *Uyghur Forced Labor Prevention Act* (UFLPA)[43] and, through CBP, is charged with enforcing this watershed law. As chair of the Forced Labor Enforcement Task Force[44], DHS leads a multi-agency effort to expand the UFLPA Entity List.[45] The 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.

This is a global problem. Our disruption efforts to minimize the risk these perpetrators pose to national security and public safety must go beyond our borders. To be effective we work closely with the whole homeland security enterprise and international partners to achieve the greatest results in apprehending and prosecuting perpetrators.

LEAD: PLCY, CBP, ICE, USSS

STAKEHOLDER: CRCL, OSLLE, PRIV, S&T, TSA, USCIS, USCG

40 The Science & Technology Directorate (S&T) develops forensic tools to support investigations with agile research and development to design, develop, and assess digital forensic prototypes and transition them to operations. S&T currently has unique forensic tools including speech and language tools, livestream triage capabilities and face recognition.

41 Pursuant to 18 U.S.C. Section 3056(f)

42 USSS also supports through forensic assistance via polygraph support, photo/video enhancement, analysis of questioned documents, and GIS assistance on cases related to missing or exploited children.

43 Pub. L. No. 117-78; signed into law by President Biden on December 23, 2021. See https://www.dhs.gov/uflpa.

44 https://www.dhs.gov/forced-labor-enforcement-task-force

45 The UFLPA Entity List is a consolidated register of four lists required to be developed and maintained pursuant to the UFLPA. Goods produced by an entity on the UFLPA Entity List are prohibited from importation into the United States.

Enable Mission Success by Strengthening the Enterprise

DESIRED OUTCOME:
DHS accomplishes its missions efficiently and effectively with a world-class workforce based on national priorities and strategic guidance in furtherance of the national interest.

Over two decades, DHS has evolved into the third-largest Cabinet agency, with over 260,000 dedicated professionals carrying out our mission through more than two dozen offices and agencies. Every day, we interact with the public more than any other federal agency—on land, at sea, in the air, and in cyberspace. The breadth of our mission and the scale of our impact demand support for a world-class workforce, organizational agility, and appropriate resourcing to better meet the increasingly dynamic and rapidly evolving threat landscape.

This will require a workforce that is strengthened and supported; capabilities that are adaptable; technology and data systems that are interoperable; modernized facilities that are safe, secure, and resilient; and operations that draw on science and data. The entire HSE will need to 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.

We seek to strengthen and enhance the enterprise in key areas to guide DHS's strategic focus, to include maturing organizational governance, championing our workforce, and harnessing data and technology to advance mission delivery. Our vision is of a Department that operates efficiently and effectively with a highly skilled, diverse, and engaged workforce capable of accomplishing the homeland security mission.

ENABLING OBJECTIVE 1:
Mature Organizational Governance

DESIRED OUTCOME:
The Department translates leadership vision into action through developing and aligning strategic planning and budget development processes, leveraging partnerships, and respecting our nation's laws and values.

Our policymaking and operational decision-making processes will continue to mature organizational governance by translating leadership vision into actionable policy and strategic guidance. The Department uses strategic planning processes to translate the DHS vision into actionable goals, objectives, and operational activities for resourcing priorities, including those designated in Appendix A. Maturing governance across all organizational frameworks will require the added discipline of aligning strategic guidance to resources and operational outcomes.

Components and offices throughout the Department use different performance management architectures. These architectures should be designed to promote interoperability for enabling decision-making and continuous evaluation and management.

Accomplishing our missions also requires a steadfast commitment to protecting civil rights, civil liberties, and privacy while advancing principles of equity. 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 policy development, program design, operational planning, and assessments, and it must continue throughout the entire lifecycle of these activities. Records containing adequate and proper documentation of the Department's activities must also be protected and preserved as evidence of the Department's commitment to safeguarding the rights and interests of the public, and to hold officials accountable for their actions, memorialize our successes, and document our nation's decision-making history.

Fundamentally, DHS is a department of partnerships. Our success depends on the strength of these partnerships as we cannot accomplish our mission alone. DHS is 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 nation's highest values.

With approximately 80,000 law enforcement officers across nine different agencies and offices, DHS has the largest law enforcement workforce in the federal government. DHS supports this workforce through the Law Enforcement Coordination Council (LECC), the Department's first unified law enforcement coordination body, to facilitate collaboration among the different law enforcement units, comprehensively assess potential policy changes, and promote best practices. The Department's partnerships with the 18,000 state, local, tribal, territorial, and campus (SLTTC) law enforcement agencies in the United States is particularly critical to keeping communities safe. It is likewise important that the interests of our SLTTC law enforcement partners are woven into the fabric of our Department. DHS

must continue to ensure that law enforcement equities are represented throughout the Department during policy, program, and initiative development; that law enforcement and terrorism-focused grants are appropriately centered on terrorism prevention activities; and that DHS provides maximal information, resources, and operational support to our law enforcement partners.

LEAD: CRCL, MGMT, OPE, OSLLE, PLCY, PRIV

STAKEHOLDER: ALL

ENABLING OBJECTIVE 2: Champion the Workforce

DESIRED OUTCOME:
The DHS workforce reflects the diversity of the communities we serve and is equipped and enabled to succeed in their respective roles free from discrimination and harassment.

DHS is able to execute our critical mission because of the extraordinary public servants in our Department. They protect the traveling public, secure our borders, facilitate lawful trade and travel to promote a strong American economy, help protect the cybersecurity of organizations of all sizes, increase nationwide resilience against natural disasters, and so much more. Their dedication makes attaining our noble missions possible.

To champion our workforce, DHS will promote a culture of transparency, fairness, accessibility, and equal employment opportunity, providing avenues of redress and leadership support in addressing and resolving workplace conflict through integrated conflict management and Alternative Dispute Resolution. DHS will also continue to leverage increased employee engagement to drive meaningful change for our employees. We will prioritize maintaining a culture of recognition and empowerment at every level, including with peers, and amplify employee and team successes externally. Our workforce must continue to reflect the diversity of the communities we serve. These priorities will contribute to building and maintaining a world-class workforce.

DHS will continue to invest in its workforce through engagement and continual enhancement of processes and procedures that support both organizational and individual performance. It remains committed to promoting principled practices that ensure equity in career development programs. With a focus on human capital solutions, DHS will identify and develop a continuous pipeline of leaders that is reflective of the people they serve. By improving awareness of training, professional development, and education opportunities, the Department will reduce barriers in accessing career development resources and strengthen employee autonomy in charting their professional paths.

LEAD: CRCL, MGMT

STAKEHOLDER: ALL

ENABLING OBJECTIVE 3:
Harness Data and Technology to Advance Mission Delivery

DESIRED OUTCOME:
DHS leverages data and technology to advance mission delivery and increase openness and transparency while protecting privacy, civil rights, and civil liberties.

DHS can leverage technology and other innovative approaches to modernize the programs we administer and deliver our missions with more efficacy and efficiency. Whether behind-the-scenes or in customer-facing processes and experiences, we will leverage data and technology to transform and optimize our operations and our decision-making across offices and agencies to enhance mission delivery and improve outcomes for the Department and the communities we serve. These efforts will improve the public's customer experience when seeking DHS services. S&T, as the DHS research and development lead, seeks technology solutions for the Department's operational challenges. S&T will leverage the work of other agencies, where possible, and share its work with them to make the most of our resources and grow partnerships in areas of similar missions. DHS will establish S&T as an enterprise resource that can provide technology-enabled capabilities, scientific advice, and additional information to operations across the DHS mission space.

DHS collects and holds significant amounts of identity and operational processing data. It is critical to leverage this data appropriately and improve our technologies, processes, and services to the greatest extent possible to accomplish our missions in accordance with the law, including protecting privacy throughout the data lifecycle. DHS is entrusted to handle the sensitive personal information of Americans, visitors, and businesses for the purposes of homeland security, and it is our duty to handle it responsibly and securely. To do this effectively, we must continue to earn and maintain the public's trust.

DHS has launched a Data Inventory Program[46] to create a catalog of DHS data that is accurate, complete, timely, and useful. This program provides a systematic approach for documenting how and where information is collected, the purposes for which it is being used, how long it is retained, and the information flow within each Component and across the Department and interagency. 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 more easily create accurate predictive models that will allow us to better plan for changing operational dynamics in multiple mission areas.

46 The Data Inventory Program is conducted under DHS Delegation 04004 of May 18, 2021, from Secretary Mayorkas to the Chief Information Officer, as authorized by the *Foundations for Evidence-Based Policymaking Act of 2018* (Pub. L. No. 115-435) and the *Open, Public, Electronic, and Necessary Government Data Act* ("OPEN Government Data Act"; codified at 44 U.S.C. §3511).

Timely, effective, and innovative research, development, test, and evaluation of promising and emerging technologies that can be used by front-line operators is vital for DHS to keep pace and preempt the dynamic and evolving nature of threats to the homeland. The Operational Components, MGMT, and S&T employ the Acquisition Life Cycle Framework (ALF) and other acquisition disciplines to field new and enhanced systems for the Department and the HSE. The ALF balances security capability needs with procurement laws and regulations, oversight, system effectiveness and useability, and overall affordability to optimize the acquisition process from concept to fielding. DHS continues to use and improve the ALF to provide capable and effective equipment more quickly to strengthen the HSE.

LEAD: CRCL, MGMT, PLCY, PRIV, S&T

STAKEHOLDER: ALL

Appendix A: DHS Organizational Performance Management and Measurement

A key component of any strategy is the ability to measure progress against the goals and objectives contained within that strategy. This Appendix outlines the processes by which DHS will measure organization performance and progress. Measurement is a dynamic process that requires a rigorous approach to gauge development, safeguards to ensure the measures are valid and reliable, and the flexibility to adjust as the strategic and operational environments change.

DHS has instituted a robust organizational performance management framework to implement the *Government Performance and Results Act of 1993* (GPRA)[47] and GPRAMA to assess our mission program progress using data and evidence, define success for the organization, ensure measured results are reliable, engage senior leaders, and drive the delivery of value to external stakeholders.

Fig. 3. DHS Performance Management

47 Pub. L. No. 103-62.

Performance Measurement and the Annual Performance Plan

DHS publishes an Annual Performance Plan in the Department's *Annual Performance Report* that describes target and achieved levels of performance on publicly reported performance measures related to DHS's Strategic Goals and Objectives. This performance plan provides the direct linkage between long-term strategic goals outlined in agencies' strategic plans and what programs are expected to accomplish with a given level of resources. Department performance measures include enduring measures of core missions and dynamic measures reflecting changing priorities and initiatives. DHS improves performance measures annually through extensive engagement with Department workforce, leaders, and external stakeholders and accounts for changing Administration priorities and contexts in which DHS missions operate.

DHS publishes performance measures and targets annually in the Department's *Annual Performance Report, Congressional Justifications, and Future Years Homeland Security Program* (FYHSP) reports to Congress. DHS subjects the data collected from performance measures to rigorous verification and validation assessments to ensure their completeness, reliability, quality, and limitations for use in decision-making. Once approved by DHS and OMB, these performance data are reflected in the Department's quarterly and annual Performance and Accountability reporting to the public each FY.

DHS conducts quarterly and annual reviews that bring together people, resources, and performance data to facilitate best practices of a learning organization, including to:

- Assess achievements of programs and capabilities;
- Identify next steps and opportunities for improvement;
- Identify where evaluation or other research or analysis are needed to determine effectiveness; and
- Inform planning, budgeting, and management decisions.

Appendix B: DHS Evaluation and Evidence

The Department implements planning and performance management policies based on best practices and applicable legislation, including GPRAMA, the *Program Management Improvement Accountability Act of 2016,*[48] and the *Foundations for Evidence-Based Policymaking Act of 2018* ("Evidence Act").[49] The Department coordinates strategic planning, performance management, and evidence-building initiatives at the program, Component, and Department levels to promote efficiency and effectiveness in achieving homeland security goals.

The Department's Evaluation Policy[50] provides a key framework for generating evidence through evaluation to inform decisions and policymaking. The Department collects and uses data and evidence from evaluations to support organizational learning, improve program and operations performance, determine resource priorities, and engage stakeholders for transparency and public accountability.

Consistent with the Evidence Act, DHS developed a Learning Agenda[51] and Capacity Assessment as companion reports to the *DHS Strategic Plan: Fiscal Years 2023-2027*. The Department also develops an Annual Evaluation Plan[52] that accompanies the Department's *Annual Performance Report*. The Learning Agenda and Annual Evaluation Plans reflect extensive consultation with the DHS workforce, leadership, and external stakeholders to identify both broad and specific questions about the missions of the Department and how the questions will be addressed by the Department's evidence-building with the goal of improving situational awareness, mission delivery, and homeland security outcomes and impacts.

The Department's Learning Agenda is a multi-year strategic evidence-building plan that aligns with policy priorities of the Department's Strategic Plan and emerging policy priorities, such as COVID-19, climate change, and diversity, equity, inclusion, and accessibility. The Learning Agenda provides an important planning tool that supports the DHS workforce and external stakeholders in planning, building, and using evidence for strategic, operational, programmatic, and policy decision-making. Annually, DHS coordinates updates on Learning Agenda activities to determine progress toward the original priorities, understand shifting learning priorities, and identify emerging evidence needs. The DHS Evaluation Officer uses this process to inform updates to the Learning Agenda, as needed, and develop the Annual Evaluation Plan. The Department's Annual Evaluation Plans include planned significant evaluations that contribute to answering the Department's Learning Agenda questions, fill gaps in evidence, and respond to mandates.

Concurrent to developing the Learning Agenda and Strategic Plan, the Department assessed its capacity to build and use evidence generated through evaluation, statistics, research, and

48 Pub. L. No. 114-264.

49 Pub. L. No. 115-435.

50 See https://www.dhs.gov/sites/default/files/2022-03/Directive 069-03%2C Revision 00 Program%2C Policy%2C and Organizational Evaluations.pdf.

51 See https://www.dhs.gov/sites/default/files/2022-03/DHS FY2022-26 Learning Agenda_508c.pdf.

52 See https://www.dhs.gov/evaluation-and-evidence-plans.

analysis. The capacity assessment[53] highlights the Department's strengths and opportunities to grow capacity through increased investment in, and attention to, the Department's staffing, funding, infrastructure, processes, and culture. The Department uses the capacity assessment to inform collective and concerted efforts to improve DHS and Component capacity critical to achieving the priorities laid out in the Strategic Plan, Learning Agenda, and Annual Evaluation Plans. Led by the Department's Evaluation Officer, DHS Operational and Support Components are actively working to build capacity for evaluating programs, policies, and operations commensurate with the scale of the Component's work, size of their portfolio, and size of their budget.

53 See https://www.dhs.gov/sites/default/files/2022-03/DHS FY2021 Capacity Assessment_508c_0.pdf.

DHS STRATEGIC PLAN:
Fiscal Years 2023-2027