# THE DHS STRATEGIC PLAN Fiscal Years 2020-2024

The DHS Strategic Plan comprehensively reflects the Department's complex mission. Every day, each operator and employee across the Department advances the strategic goals and objectives contained herein to keep Americans safe, secure, and resilient. The DHS Strategic Plan establishes a common framework to analyze and inform the Department's management decisions, including strategic guidance, operational requirements, budget formulation, annual performance reporting, and mission execution.

Along with the DHS Strategic Plan, DHS also conducts the Quadrennial Homeland Security Review, which identifies strategic homeland security priorities based on extensive analysis and stakeholder engagement. Together, these documents inform internal operations and our interactions with Congress, interagency counterparts, and the American public.

## *Contents*

# U.S. Department of Homeland Security (DHS)

## Description:

From the ashes of the September 11th terrorist attacks, Congress established DHS in 2003 as a new Cabinet-level agency to unite the Nation's approach to homeland security. DHS combined functions of 22 different federal departments and agencies with broad responsibilities that collectively prevent attacks, mitigate threats, respond to national emergencies, preserve economic security, and preserve legacy agency functions. In the years since its formation, DHS has matured considerably to improve integration across its Headquarters Offices and Operational Components. As we move forward, it is imperative for DHS to continue strengthening the execution of its Headquarters' responsibilities by centralizing and coordinating the Department's many functions and ensuring that the whole is greater than the sum of its parts.

**Stakeholder(s):**

**Kevin K. McAleenan** :
*Acting Secretary, U.S. Department of Homeland Security*

**Office of the Secretary** :
*Oversees and coordinates the Department's legal affairs, public affairs, external engagements, operational requirements, and legislative affairs.*

**DHS Operational Components**

**U.S. Customs and Border Protection** :
*One of the world's largest law enforcement organizations, charged with safeguarding America's borders by keeping terrorists, their weapons, and all dangerous people and illicit materials out of the United States while facilitating lawful international travel and trade.*

**Cybersecurity and Infrastructure Security Agency** :
*Serves as the Nation's risk advisor to build the national capacity to defend against cyber attacks, coordinate security and resilience efforts across the public and private sectors, and identify and address the most significant risks to the national critical functions provided by our Nation's critical infrastructure.*

**Federal Emergency Management Agency** :
*Leads and supports the Nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation to reduce the loss of life and property while protecting the Nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters.*

**U.S. Immigration and Customs Enforcement** :
*Conducts homeland security investigations and enforces criminal and civil federal laws governing border control, customs, trade, and immigration. Transportation Security Administration: Protects the Nation's transportation systems to secure freedom of movement for people and commerce.*

**U.S. Citizenship and Immigration Services** :
*Administers the Nation's lawful immigration system, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the Homeland, and honoring our values.*

**U.S. Coast Guard** :
*Safeguards the American people and promotes our security in a complex, evolving maritime environment as a law enforcement organization, a regulatory agency, an environmental steward, a first responder, a member of the Intelligence Community, and the only military service within the Department of Homeland Security.*

**U.S. Secret Service** :
*Protects national leaders, visiting heads of state and government, designated sites, and National Special Security Events, and safeguards the Nation's financial infrastructure and payment systems to preserve the integrity of the economy.*

**DHS Support Components**

**Countering Weapons of Mass Destruction Office** :

*Supports Departmental efforts to counter attempts by terrorists or other threat actors to carry out an attack against the United States or its interests using a weapon of mass destruction.*

*— continued next page*

*Stakeholders (continued)*

**Federal Law Enforcement Training Centers** :
*Prepares law enforcement professionals to perform their duties safely and effectively in their operating environments.*

**Management Directorate** :
*Manages the Department's processes for budget formulation, appropriations, expenditure of funds, accounting and finance; procurement; human resources and personnel; information technology systems; identity services; facilities, property, equipment, and other material resources; and identification and tracking of performance measurements relating to the responsibilities of the Department.*

**Office of Intelligence and Analysis** :
*Equips the Homeland Security Enterprise with the timely intelligence and information it needs to keep the Homeland safe, secure, and resilient.*

**Office of Operations Coordination** :
*Provides daily information to the Secretary of Homeland Security, senior leaders, and the homeland security enterprise to enable decision-making; oversees the National Operations Center; and leads the Department's continuity of operations and government programs to enable continuation of primary mission essential functions in the event of a degraded or crisis operating environment.*

**Office of Strategy, Policy, and Plans** :
*Leads development and coordination of Department-wide strategies, policies, and plans to promote and ensure integration across the Department using risk-based analysis, subject-matter expertise, and stakeholder feedback.*

**Science and Technology Directorate** :
*The primary research and development arm of the Department that develops novel and unique technological solutions to protect the Homeland.*

## Vision

A secure Homeland

## Mission

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

## Values

**Principles**: Guiding Principles:

**Resilience**: Champion "Relentless Resilience" for All Threats and Hazards: DHS will remain resolute against today's threats and hazards by keeping pace with our adversaries and preparing for those of tomorrow by identifying and confronting systemic risk, ensuring the Nation's citizens remain resilient, building redundancy and resilience into community lifelines, and raising the baseline of our security across the board—and across the world.

**Risk Mitigation**: Reduce the Nation's Risk to Homeland Security Dangers: DHS will mitigate risks to the Homeland by interdicting threats, hardening assets to eliminate vulnerabilities, and enhancing rapid recovery efforts to reduce potential consequences from physical attacks, natural disasters, and cyber incidents.

**Engagement**: Promote Citizen Engagement and Strengthen and Expand Trusted Partnerships: Homeland security is a whole-of-society endeavor, from every federal department and agency to every American across this Nation. We will work together and empower partners to leverage national capacity and capabilities, improve training exercises, and develop contingency plans that make America safe, secure, and resilient against all threats and all hazards.

**Trust**

**Partnership**

**Privacy**: Uphold Privacy, Transparency, Civil Rights, and Civil Liberties: DHS will continue to implement safeguards for privacy, transparency, civil rights, and civil liberties when developing and adopting policies and throughout the performance of its mission to ensure that homeland security programs uphold privacy, civil rights, and civil liberties.

**Transparency**

**Civil Rights**

**Civil Liberties**

**Integration**: Ensure Mission-Driven Management and Integration: As a unified Department, DHS will leverage the collective capabilities of its operational Components to identify opportunities for jointness and integration. Through a comprehensive and collaborative approach, DHS will ensure its operators and employees have the necessary tools, resources, and authorities to execute its mission.

# 1. Terrorism & Threats

*COUNTER TERRORISM AND HOMELAND SECURITY THREATS*

One of the Department's top priorities is to resolutely protect Americans from terrorism and other homeland security threats by preventing nation-states and their proxies, transnational criminal organizations, and groups or individuals from engaging in terrorist or criminal acts that threaten the Homeland. In recent years, terrorists and criminals have increasingly adopted new techniques and advanced tactics in an effort to circumvent homeland security and threaten the safety, security, and prosperity of the American public and our allies. The rapidly evolving threat environment demands a proactive response by DHS and its partners to identify, detect, and prevent attacks against the United States.

## 1.1. Intelligence

*COLLECT, ANALYZE, AND SHARE ACTIONABLE INTELLIGENCE*

Effective homeland security operations rely on timely and actionable intelligence to accurately assess and prevent threats against the United States. Accordingly, DHS works diligently to enhance intelligence collection, integration, analysis, and information sharing capabilities to ensure partners, stakeholders, and senior leaders receive actionable intelligence and information necessary to inform their decisions and operations. A critical and statutorily charged mission of DHS is to deliver intelligence and information to federal, state, local, and tribal governments and private sector partners. As such, DHS has the broadest customer base for intelligence products of various subjects and classification requirements. This responsibility requires an integrated intelligence network to eliminate redundancies and a mission-focused approach to producing and sharing intelligence. Desired Outcome: Develop intelligence and threat information to identify and mitigate homeland security threats as early as possible and to inform the actions of decision-makers across the Department, interagency partners, public and private sector stakeholders, and international partners.

### 1.1.1. Warnings

*Forecast emerging threats to the homeland and provide early warning*

### 1.1.2. Enablement

*Integrate intelligence and threat information across DHS based on leadership, operator, and partner requirements to enable timely and specific actions*

### 1.1.3. Awareness & Information

*Disseminate intelligence and threat information for domestic and international partners to support continuous threat awareness and inform appropriate threat mitigation and response*

### 1.1.4. Counterintelligence

*Execute counterintelligence activities to protect the homeland security enterprise from espionage, insider threats, and external adversaries*

### 1.1.5. Intelligence

*Provide intelligence support to inform DHS policy, management, and operational leadership*

## 1.2. Threats

*DETECT AND DISRUPT THREATS*

The terrorist threat to the United States has evolved considerably since the September 11th attacks. Despite our success in detecting and preventing multi-actor, complex terrorist attacks, terrorists continue plotting in search of any kind of vulnerability that may permit them to conduct an attack against the United States. While this significant threat looms, decentralized terrorist groups have exploited the Internet and social media to incessantly spread terrorist propaganda and training material that inspire and recruit individuals within the United States to radicalize to violence. Terrorist narratives across the ideological spectrum increasingly encourage the use of simple tactics that target large public gatherings using vehicular attacks, small arms, homemade explosives, or chemical, biological, or radiological materials. These attacks often lack overt warning signs, which limits opportunities for intervention or apprehension. To thwart these attacks, the Department and its partners must engage in a comprehensive counterterrorism approach to prevent both foreign and domestic terrorism and more decisively confronts the terror threat to the Homeland. The Department also requires the tools and capabilities necessary to address targeted violence in all its forms, including threats to our schools, infrastructure, and houses of worship. Meanwhile, nation-states are actively attempting to undermine democratic institutions and the prosperity of the American people. Preventing adversaries from exerting direct or indirect influence on the United States is imperative to homeland security. DHS is collaborating with state, local, and tribal governments and private sector partners to disrupt these activities and raise awareness among our citizens, while continuing to enforce protections against foreign investments into the United States that threaten national security. Transnational criminal organizations and their offshoots also pose serious threats to the American people and the Homeland. Their crimes include trafficking and smuggling of humans, drugs, weapons, and wildlife, as well as money laundering, corruption, cybercrime, fraud, financial crimes, intellectual property theft, and the illicit procurement of export-controlled material and technology. DHS is using its full breadth of law enforcement, border security, immigration, travel security, and trade-based authorities to proactively prevent, identify, investigate, disrupt, and dismantle these organizations. Desired Outcome: Detect and disrupt current and emerging homeland security threats, including from terrorists, nation-states, and other threat actors.

### 1.2.1. Training & Edcuation

*Lead national terrorism and threat prevention efforts through community awareness training and education, counter-radicalization and counter-recruitment, early warning, and counter-recidivism*

### 1.2.2. Plots & Attacks

*Disrupt foreign and domestic terrorist plots and attacks through aviation and surface transportation security, border security, and maritime security, including by investigations, interagency cooperation, and close partnerships with officials, nationwide operators, and international partners*

### 1.2.3. Threat Actors

*Prevent foreign threat actors from exploiting travel, trade, financial, and immigration systems for illicit purposes*

### 1.2.4. Foreign Influence

*Counter malicious foreign influence efforts in the United States, including interference directed at undermining U.S. Government operations and democratic processes, as well as foreign investments that pose national security risks*

### 1.2.5. Trafficking & Exploitation

*Prevent, identify, investigate, disrupt, and dismantle human trafficking, child sexual exploitation, and other exploitation-based crimes through a law enforcement and victim-centered approach*

## 1.3. Leadership, Events & Targets

*PROTECT DESIGNATED LEADERSHIP, EVENTS, AND SOFT TARGETS*

Desired Outcome: Provide protection to designated U.S. leaders, foreign heads of state and government, special events of national significance, and federal facilities to ensure government continuity and enhance overall security of soft targets and crowded places nationwide.

**Stakeholder(s):**

**U.S. Elected Leaders** :
*Ensuring the protection and safety of our Nation's highest elected leaders is a paramount responsibility that demands operational perfection.*

**Designated Leaders** :
*DHS maintains a highly skilled and motivated workforce combined with innovative technologies and advanced countermeasures to protect designated leadership, visiting foreign heads of state and government, and National Special Security Events.*

**Visiting Foreign Leaders**

**Federal Personnel** :
*In addition to its more visible presidential protection responsibilities, DHS also protects federal facilities and personnel across the United States;*

**Tribal Governments** :
*supports tribal, state, and local governments to protect events of national significance; and improves security for soft targets.*

**State Governments**

**Local Governments**

**Homeland Security Stakeholders** :
*In particular, DHS is leading efforts to defend soft targets by sharing intelligence bulletins and analysis with homeland security stakeholders, developing best practices to counter attacks against soft targets, promoting a dynamic process to assess soft targets and address security gaps, and investing in research and development for technological solutions. Together, these initiatives harden and help defend potential targets of terrorist attacks.*

**Federal Coordinators** :
*The Department also assesses risk to local special events occurring across the Nation. This assessment uses the Special Events Assessment Rating (SEAR) methodology to rank events by risk factors. DHS supports the highest risk events with Federal Coordinators to serve as representatives of the Secretary by engaging directly with our state and local partners to coordinate support that helps address safety and security capabilities shortfalls.*

### **1.3.1.** Leaders

*Protect designated U.S. leadership and their families, as well as visiting foreign heads of state or government*

**Stakeholder(s):**

**U.S. Leaders** **Foreign Leaders**

**Families of U.S. Leaders**

### **1.3.2.** Events

*Manage and coordinate federal security operations for National Special Security Events and Special Event Assessment Rating events and provide support to state and local officials for events of national significance*

**Stakeholder(s):**

**State Officials** **Local Officials**

### **1.3.3.** Facilities

*Protect federal facilities, including persons and property in those facilities*

### **1.3.4.** Targets & Places

*Improve security of soft targets and crowded places against the spectrum of nefarious actors who might attempt to target or attack such locations*

## **1.4.** WMD

*COUNTER WEAPONS OF MASS DESTRUCTION AND EMERGING THREATS*

The spread of rapidly evolving and innovative technology, equipment, techniques, and knowledge presents new and emerging dangers for homeland security in the years ahead. Terrorists remain intent on acquiring weapons of mass destruction (WMD) capabilities, and rogue nations and nonstate actors are aggressively working to develop, acquire, and modernize WMDs that they could use against the Homeland. Meanwhile, biological and chemical materials and technologies with dual use capabilities are more accessible throughout the global market. Due to the proliferation of such information and technologies, rogue nations and non-state actors have more opportunities to develop, acquire, and use WMDs than ever before. DHS is strengthening and integrating its detection and counter-measure capabilities to address this profound risk to the United States. Similarly, the proliferation of unmanned aircraft systems, artificial intelligence, and biotechnology increase opportunities for threat actors to acquire and use these capabilities against the United States and its interests. DHS is assessing how these technologies will affect homeland security and developing proactive solutions to limit future risk. Desired Outcome: Guard against evolving homeland security threats, such as weapons of mass destruction, pandemics, sophisticated explosives, and the malicious use of disruptive and emerging technology.

### **1.4.1.** Deterrence, Detection & Disruption

*Deter, detect, and disrupt the use of weapons of mass destruction (WMD) and health security dangers as early in the threat pathway as possible, including through investigations, information sharing, and integrated counter-WMD planning*

### 1.4.2. Partnerships

*Strengthen foreign and domestic partner operational capability to prevent, protect against, and respond to WMD and pandemic threats*

### 1.4.3. Scanning

*Strengthen national horizon-scanning for emerging dangers, including through risk analysis, strategic forecasting, intelligence sharing, and robust research and development*

### 1.4.4. Technological Threats

*Counter malicious threats from disruptive and emerging technologies through development and deployment of counter-measures and partner capacity-building*

### 1.4.5. Terrorists

*Deny terrorists access to WMD materials, agents, equipment, and precursors*

# 3. Borders & Approaches

*SECURE U.S. BORDERS AND APPROACHES*

Secure borders are essential to our national sovereignty. Managing the flow of people and goods into the United States is critical to maintaining our national security. Illegal aliens compromised the security of our Nation by illegally entering the United States or overstaying their authorized period of admission. Illegal aliens who enter the United States and those who overstay their visas disregard our national sovereignty, threaten our national security, compromise our public safety, exploit our social welfare programs, and ignore lawful immigration processes. As a result, DHS is implementing a comprehensive border security approach to secure and maintain our borders, prevent and intercept foreign threats so they do not reach U.S. soil, enforce immigration laws throughout the United States, and properly administer immigration benefits.

## 2.1. Borders

*SECURE AND MANAGE AIR, LAND, AND MARITIME BORDERS*

The security of our Nation depends on operational control over air, land, and maritime borders to prevent terrorists, transnational criminal organizations, and other threat actors from exposing the United States to malicious and illicit activity originating from foreign sources. Sophisticated smuggling enterprises, elaborate border tunnels, go-fast vessels, and other elusive travel methods allow illegal aliens and transnational criminal organizations to evade border enforcement along the United States' nearly 6,000 miles of land border and 95,000 miles of shoreline. To combat these threats, DHS is enhancing border security between designated ports of entry using physical barriers and technological innovations that deny illegal border-crossers unobstructed access to the United States. Additionally, DHS is improving its situational awareness of the land and maritime domains and increasing personnel and assets to stop, interdict, and arrest illegal aliens attempting to enter the United States. Together, these initiatives prevent infiltration of the United States between designated ports of entry and crack down on illegal immigration to the United States. Meanwhile, fraudulent documentation and deceptive travel practices impede our operators from identifying and validating international travelers arriving at designated ports of entry and preclearance facilities. DHS is taking specific measures to positively identify, screen, and vet individuals to prevent potential known or suspected terrorists from traveling to the United States using evasive travel methods. DHS is also combating systemic transnational criminal activity to eliminate the flow of narcotics, crime, and violence into the United States, while intercepting outbound illicit profits. This starts at the land and maritime ports of entry, where DHS is vigilantly inspecting inbound cargo. By reducing the supply of narcotics that enter the United States and preventing human smuggling and trafficking enterprises, DHS is preventing the existence of illicit American markets. Desired Outcome: Defend air, land, and maritime borders against illegal entry and illicit activities.

### 2.1.1. Illegal Trade & Travel

*Deter and impede illegal trade and travel across air, land, and maritime borders, including through deployment of multi-layered defenses, barriers, systems, and personnel*

### 2.1.2. Illicit Activity & Travel

*Detect, interdict, and apprehend illicit activity and travel transiting across air, land, and maritime borders*

### 2.1.3. Individuals

*Positively identify, screen, and vet individuals entering and exiting the United States using law enforcement information, intelligence, and other data to identify potential threat actors*

## 2.2. Reach

*EXTEND THE REACH OF U.S. BORDER SECURITY*

Regional instability and foreign conflicts have endangered the global travel system and significantly increased the prevalence of illegal travel to the United States, posing a significant threat to homeland security from abroad. In particular, foreign terrorist fighters departing conflict zones may attempt to exploit pathways into the United States to continue their terrorist intentions. Additionally, transnational criminal organizations have capitalized on economically depressed regions with limited law enforcement and security capabilities to expand their operations for trafficking and smuggling illegal drugs, contraband, and illegal aliens into the United States. Beyond these threat actors, DHS is confronted with the threat of mass migration movements across land and maritime domains from unstable neighboring regions. DHS is directly addressing these threats by extending the reach of U.S. border security using forward-deployed border security operations, such as cutter patrols, customs and immigration investigations, and travel security assets, combined with international partnerships around the world. In partnership with other federal agencies, DHS is expanding efforts to collect and analyze advance passenger information, strengthen the known and suspected terrorist Watchlist, share information with international partners, and help international partners enhance their screening and vetting capabilities to identify known and suspected terrorists. DHS is also investigating and dismantling transnational criminal organizations to eliminate long-term threats to the Homeland. Together, these initiatives enable the United States to extend the security of its borders, intercepting foreign threats long before they reach U.S. soil. Desired Outcome: Disrupt threats before they reach our territory by working with foreign partners in source and transit zones to disrupt illicit activities and travel pathways.

### 2.2.1. Criminal Organizations

*Investigate, degrade, and dismantle transnational criminal organizations*

### 2.2.2. Smuggling, Trafficking & Illicit Activities

*Detect and disrupt smuggling, trafficking, and illicit activities through land, air, and maritime pathways*

### 2.2.3. Foreign Partners

*Enhance foreign partner capacity to establish impediments to illicit trade and travel and deter illegal entry into the United States*

**Stakeholder(s):**

**Foreign Partners**

### 2.2.4. Partner Nations

*Work with partner nations to help them strengthen their own security capacity*

**Stakeholder(s):**

**Partner Nations**

## 2.3. Immigration Laws

*ENFORCE U.S. IMMIGRATION LAWS*

Enforcement of our Nation's immigration laws is critically important to the national security and public safety of the United States. Illegal aliens who are present in the United States blatantly undermine the integrity of our immigration system and disregard our federal laws. Moreover, many aliens who illegally enter the United States and those who overstay or otherwise violate the terms of their authorized period of admission present a potential threat to national security and public safety. Meanwhile, many aliens who commit crimes within the United States remain in American communities solely because their home countries refuse to accept their repatriation. It is DHS's responsibility to faithfully execute and enforce the immigration laws of the United States in a manner that eliminates these abuses. DHS investigates immigration violators who fraudulently obtain visas to the United States, fail to maintain their authorized status, or otherwise violate the terms of their lawful admission pursuant to federal laws. DHS is improving its ability to maintain positive identification of individuals throughout the immigration and travel process using both biographic and biometric information to identify individuals who overstay their authorized period of admission. In particular, DHS is expanding its screening policies for biometric screening at border entry/exit and evaluations for extensions of status. DHS is also creating a culture of compliance to prevent employers from hiring illegal alien labor that displaces American labor by utilizing a multi-prong approach, including enforcement, compliance, and outreach. Through these initiatives, DHS is exercising all appropriate and lawful means to identify, locate, and detain aliens unlawfully present within the United States and facilitate their timely repatriation. Desired Outcome: Enforce immigration laws throughout the United States in a manner that upholds the rule of law, American values, and national security.

### 2.3.1. Aliens

*Identify, locate, detain, as appropriate, and remove removable aliens*

### 2.3.2. Law Enforcement Partnerships

*Create and foster law enforcement partnerships with federal, state, local, and tribal authorities that enable coordination and information sharing to arrest removable aliens*

**Stakeholder(s):**

**Federal Authorities**

**Local Authorities**

**State Authorities**

**Tribal Authorities**

### 2.3.3. Violations & Workplaces

*Investigate immigration violations and conduct workplace enforcement*

## 2.4. Immigration Benefits

*Administer Immigration Benefits to Advance the Security and Prosperity of the Nation*

Long-standing shortcomings throughout all phases of the visa issuance and travel process have enabled individuals to exploit the Nation's immigration system and gain unlawful access to the United States. In particular, the U.S. immigration system remains vulnerable to fraudulent claims for asylum and refugee status and exploitation of expedited travel programs. Meanwhile, immigration policies have prioritized foreign labor over American workers and the best interests and economic needs of the United States. DHS has aggressively confronted these flaws and is now implementing immigration laws consistent with their original intent. DHS is more thoroughly screening and vetting individuals seeking immigration benefits and seeking entry to the United States, ensuring immigration benefits comport with legislative intent and emphasize American economic needs, and eliminating opportunities for systematic abuse of the U.S. immigration system at the expense of the American people. Pursuant to the Executive Order 13788: "Buy American and Hire American," DHS is also working to ensure that American workers are better protected. Together, these policies will reduce the "pull factors" from years past that encouraged illegal immigration and compel foreign nationals and the businesses that employ foreign nationals on employment-based visas to comply with federal immigration laws and procedures. Desired Outcome: Facilitate lawful immigration while protecting American workers, including ensuring that no one exploits the U.S. immigration system or its benefits.

# 3. Infrastructure & Cyberspace

*SECURE CYBERSPACE AND CRITICAL INFRASTRUCTURE*

Increased connectivity of people and devices to the Internet and to each other has created an ever-expanding attack surface that extends throughout the world and into almost every American home. As a result, cyberspace has become the most active threat domain in the world and the most dynamic threat to the Homeland. Nation-states and their proxies, transnational criminal organizations, and cyber criminals use sophisticated and malicious tactics to undermine critical infrastructure, steal intellectual property and innovation, engage in espionage, and threaten our democratic institutions. By 2021, cybercrime damages are likely to exceed $6 trillion per year. Moreover, the interconnectivity of critical infrastructure systems raises the possibility of cyber attacks that cause devastating kinetic and non-kinetic effects. As innovation, hyper-connectivity, and digital dependencies all outpace cybersecurity defenses, the warning signs are all present for a potential "cyber 9/11" on the horizon. Critical infrastructure provides the services that are the backbone of our national and economic security and the health and well-being of all Americans. Cybersecurity threats to critical infrastructure are one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. In particular, nation-states are targeting critical infrastructure to collect information and gain access to industrial control systems in the energy, nuclear, water, aviation, and critical manufacturing sectors. Additionally, sophisticated nation-state attacks against government and private-sector organizations, critical infrastructure providers, and Internet service providers support espionage, extract intellectual property, maintain persistent access on networks, and potentially lay a foundation for future offensive operations. Meanwhile, the heightened threat from physical terrorism and violent crime remains, increasingly local and often aimed at places like malls and theaters, stadiums, and schools. Moreover, the advent of hybrid attacks, where adversaries use both physical and electronic means to inflict and compound harm, renders the threat landscape more challenging than ever. DHS works to protect critical infrastructure against these and other threats of today, while also focusing on tomorrow's emerging risks. As the national lead for protecting and enhancing the security and resilience of the Nation's civilian cyber systems and critical infrastructure, DHS is adopting a risk management approach that reduces systemic vulnerabilities across the Nation to collectively increase our defensive posture against malicious cyber activity. Simultaneously, DHS law enforcement investigations are focused on prosecuting cyber criminals, disrupting and dismantling criminal organizations, and deterring future malicious activity. These complementary initiatives address both threats and vulnerabilities across the threat spectrum.

## 3.1. Networks

*SECURE FEDERAL CIVILIAN NETWORKS*

The Federal Government depends on reliable and verifiable information technology systems and computer networks for essential operations. DHS and other federal civilian departments and agencies maintain extensive databases with national security information, personal data on American citizens, proprietary information, and other important information. As a result, malicious cyber attackers target government systems to steal information, disrupt and deny access to information, degrade or destroy critical information systems, or operate a persistent presence capable of tracking information or conducting a future attack. Serving as the designated federal lead for cybersecurity across the U.S. Government, DHS promotes the adoption of common policies and best practices that are risk-based and responsive to the ever-changing cyber threat environment. Additionally, DHS collaborates with interagency counterparts to deploy capabilities for intrusion detection, unauthorized access prevention, and near real-time cybersecurity risk reports. In deploying these capabilities, DHS prioritizes assessments, security measures, and remediation for systems that could significantly compromise national security, foreign relations, the economy, public confidence, or public health and safety. Desired Outcome: Secure federal civilian information technology systems from cyber threats and intrusions.

### 3.1.1. Capabilities, Tools & Services

*Deploy protective capabilities, tools, and services across federal civilian government systems*

### 3.1.2. Cybersecurity

*Improve cybersecurity for federal civilian departments and agencies by measuring and enforcing baseline policies and practices and integrating operationally relevant information to inform federal cybersecurity investments*

**Stakeholder(s):**

**Federal Civilian Departments**

**Federal Civilian Agencies**

### 3.1.3. Networks & Data

*Improve security and resilience of DHS networks and sensitive data as part of ongoing information technology modernization efforts*

## 3.2. Infrastructure

*STRENGTHEN THE SECURITY AND RESILIENCE OF CRITICAL INFRASTRUCTURE*

Desired Outcome: Critical infrastructure owners and operators participate as members of the security community, working to ensure a safe and secure nation.

**Stakeholder(s):**

**Infrastructure Owners** :
*Public and private owners and operators manage the vast array of critical infrastructure supporting our economy and communities. These facilities provide national critical functions that are so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on the Nation's security, economy, and public health and safety.*

**Infrastructure Operators** :
*Increasingly, infrastructure owners and operators face new risks and even nation-state adversarial actions. DHS supports owners and operators providing national critical functions by sharing intelligence and information, assisting with incident response, performing vulnerability and risk assessments, investing in the research and development of protective technologies, and providing other technical services to improve the security and resilience of our Nation's critical infrastructure against all threats.*

**Interagency Partners** :
*Along with these important initiatives for stakeholders, DHS collaborates with interagency partners to build a common understanding of strategic cyber threats that can empower private sector network defenders, critical infrastructure owners and operators, and government partners to improve resilience and integrity of national critical functions.*

**Network Defenders**

**Government Partners**

### 3.2.1. Risk Management

*Identify gaps and prioritize solutions for current national risk management efforts*

### **3.2.2.** Tools, Training, Guidelines & Assessments

*Provide tools, training, guidelines, and cyber and physical vulnerability and resilience assessments to critical infrastructure owners and operators*

**Stakeholder(s):**

**Infrastructure Owners** **Infrastructure Operators**

### **3.2.3.** Threats

*Collect and share threat indicators and other cybersecurity intelligence and information*

### **3.2.4.** Interdependencies

*Assess cross-sector critical infrastructure risks and interdependencies and provide expertise and services to critical infrastructure stakeholders*

### **3.2.5.** Security Standards

*Enforce security standards at the Nation's high-risk chemical facilities*

### **3.2.6.** Communications

*Promote and enhance voice, video, and data communications for daily operations and incident response*

## **3.3.** Cybersecurity

*ASSESS AND COUNTER EVOLVING CYBERSECURITY RISKS*

Infrastructure systems are rapidly evolving to capitalize on new technology and opportunities to enhance their services, and adversaries are constantly evolving to outpace stove-piped defenses. As a result, DHS plays a critical role in bringing government, private sector, and international partners together to advance best practices and collective defenses that promote security and resilience across the United States' expansive critical infrastructure and the larger cyber ecosystem. DHS leverages a national risk management approach to jointly assess cyber risks, develop plans for specific threats, and implement tailored solutions to protect our critical networks. As critical infrastructure owners and operators address the challenges of today, DHS will also look to the future and leverage feedback from our partners to plan more strategically to match and surpass the pace and innovation of adversaries. Desired Outcome: Bolster the security of critical infrastructure by understanding evolving risks, prioritizing risk management activities to better secure infrastructure, and taking actions to respond to emerging dangers.

### **3.3.1.** Trends

*Maintain awareness of trends in national and systemic cybersecurity and infrastructure risks, including those impacting global information and communication technology supply chains, and other systemic risks that affect national security, public health and safety, and economic security*

### 3.3.2. Strategies, Collaboration & Solutions

*Develop strategies and actionable solutions to respond to emerging risks in collaboration with relevant stakeholders*

### 3.3.3. Communications

*Promote communications used by emergency responders and government officials to keep America safe, secure, and resilient*

**Stakeholder(s):**

**Emergency Responders** **Government Officials**

### 3.3.4. Internet

*Advance public education and international collaboration to promote cybersecurity best practices and maintain an open, interoperable, secure, reliable, and resilient internet*

## 3.4. Cybercrime

*COMBAT CYBERCRIME*

As cyberspace increasingly pervades every facet of society, it has provided a new and complex domain for traditional criminal actors to engage in illicit activity that threatens U.S. homeland security. This borderless feature allows transnational criminal organizations and foreign criminal actors to commit cyber intrusions, bank fraud, child exploitation, data breaches, and other computer-enabled crimes without ever entering the United States. The speed of innovation further complicates this threat, since cybersecurity measures are implicitly reactionary. As a result, the United States is relying on law enforcement investigations to complement its defensive capabilities that combat this threat. Despite diligent efforts by the collective homeland security enterprise, the United States must do more to deter, detect, and identify cyber criminals and bring them to justice. Accordingly, DHS is applying its extensive cyber capabilities to investigate cyber criminals and take decisive actions to shield the American public from the incessant barrage of cybercrime by disrupting and dismantling criminal organizations. In particular, DHS is working to expand multilateral cooperative agreements with international partners to reach cyber criminals from regions outside the United States. Desired Outcome: Hold cyber criminals accountable and reduce cybercrime through focused law enforcement activity and public-private partnerships.

### 3.4.1. Cybercrimes

*Investigate cybercrimes targeting individuals, private organizations, and public interests consistent with DHS authorities and core homeland security investigative responsibilities*

**Stakeholder(s):**

**Individuals** **Public Agencies**

**Private Organizations**

### **3.4.2.** Investigations

*Engage in joint or collaborative investigations and provide voluntary cyber investigative assistance to law enforcement partners nationwide and globally as appropriate*

**Stakeholder(s):**

**Law Enforcement Partners**

### **3.4.3.** Information & Best Practices

*Share information and best practices with stakeholders to prevent and disrupt criminal schemes involving cyberspace*

# 4. Economy & Prosperity

*PRESERVE AND UPHOLD THE NATION'S PROSPERITY AND ECONOMIC SECURITY*

America's prosperity and economic security are integral to DHS's homeland security operations, which affect international trade, national transportation systems, maritime activities and resources, and financial systems. In many ways, these pre-DHS legacy functions are just as much a part of DHS's culture as its counterterrorism, border security, immigration, cybersecurity, and emergency management responsibilities. Similarly, many DHS activities that advance this important element of homeland security affect the American public just as much as DHS's core security functions. Accordingly, DHS continues to advance these critical operations while exploring new opportunities to better serve the American public.

## 4.1. Trade & Travel

*ENFORCE U.S. TRADE LAWS AND FACILITATE LAWFUL INTERNATIONAL TRADE AND TRAVEL*

International trade law enforcement has an important nexus to homeland security based on the inherent relationship between the U.S. border and cross-border trade. The United States is confronted with anticompetitive trade practices, duty evasion, counterfeited goods, and intellectual property theft, which deprives the United States from substantial lawful revenue and harms American businesses, our economic advantage, and individual consumers. Protecting American trade interests is only becoming more complex as the globalized marketplace flourishes and ecommerce rapidly expands its market share as an ever-increasing percentage of traditional streams of commerce. International trade frequently involves online markets with extensive, worldwide supply chains that require modernized trade enforcement practices to prevent products of forced labor, counterfeit and dangerous goods, and imports linked to anticompetitive practices from entering the United States. Rather than allowing other countries to reap benefits at the cost of the American people, we will protect American fair trade interests and fully enforce international trade agreements and corresponding laws within the United States. DHS is enhancing its trade enforcement, security, and facilitation capabilities to enable legitimate trade, contribute to American economic prosperity, and protect against risks to public health and safety. Additionally, DHS is modernizing existing partnerships with members of the international trade community and expanding existing safeguards and practices that prevent the importation of illicit and dangerous goods, products made with forced labor, and intellectual property law violations. By leveraging partner agency and industry intelligence, DHS is strengthening the global trade network and increasing supply chain security to ensure that goods entering the United States are safe for American consumption and consistent with our values. Desired Outcome: Uphold the law by targeting international trade violators and high-risk shipments and entities while expediting lawful trade.

### 4.1.1. Penalties & Sanctions

*Assess and collect duties, fees, and taxes, and enforce trade laws through penalties and sanctions*

### 4.1.2. Technologies & Collaboration

*Leverage new technologies and interagency collaboration to reduce unlawful trade and secure trade lanes*

### 4.1.3. Merchandise & Travelers

*Facilitate the flow of lawful merchandise and travelers with innovative, 21st century trade and travel processes*

**Stakeholder(s):**

**Shippers**

**Travelers**

### 4.1.4. Fraud & Intellectual Property

*Disrupt and dismantle the organizations, entities, and networks that commit intellectual property violations and trade fraud*

### 4.1.5. Transnational Cybercrime

*Investigate transnational cybercrime that exploits the international trade system*

## 4.2. Transportation

*SAFEGUARD THE U.S. TRANSPORTATION SYSTEM*

The American economy and way of life rely on a robust transportation system with seamless security measures that enable safe travel. For this reason, the transportation system remains a noteworthy target for terrorists intent on inflicting mass casualties. In particular, terrorist organizations remain focused on commercial aviation with new tactics, techniques, and weapons... Desired Outcome: Safeguard the U.S. transportation system by protecting the traveling public and critical assets, closing identified security gaps, and promoting security best practices at home and abroad.

**Stakeholder(s):**

**Travelers** :
*DHS is aggressively pursuing innovative technologies for detection and strengthening identity verification for travelers within the United States through biometric and biographic techniques and technologies.*

**DHS Partners**

**International Partners** :
*Additionally, DHS is collaborating with international partners to increase safety and security standards for international air travel.*

**Seaports** :
*Beyond air transit, DHS continues to strengthen security measures at other transportation hubs, including seaports, railways, other forms of mass transit, as well as pipelines in close coordination with federal, state, local, and tribal governments and private sector partners.*

**Railways,**

**Mass Transit**

**Pipelines**

**Federal Government**

**State Governments**

**Local Governments**

**Tribal Governments**

**Private Sector**

### 4.2.1. Screening & Vetting

*Enhance domestic screening and vetting of passengers, baggage, cargo, and transportation sector workers to deter, identify and interdict threats*

**Stakeholder(s):**

**Passengers**

**Transportation Sector Workers**

### 4.2.2. Conveyances & Hubs

*Protect designated conveyances and transportation hubs through personnel, tools, and technical assistance*

### 4.2.3. Security Technologies

*Invest in more efficient security technologies to reduce burdens on taxpayers and travel stakeholders*

**Stakeholder(s):**

**Taxpayers**

**Travel Stakeholders**

### 4.2.4. Vulnerabilities

*Identify and close security vulnerabilities throughout the transportation sector, including in airports, surface facilities, and maritime conveyances*

**Stakeholder(s):**

**Transportation Sector**

**Surface Facilities**

**Airports**

**Maritime Conveyances**

### 4.2.5. Aviation Security

*Raise the baseline for worldwide aviation security through a combination of foreign partner collaboration, promotion of incentives, and tailored requirements*

**Stakeholder(s):**

**Air Travelers**

**Aviation Industry**

## 4.3. Waterways & Maritime Resources

*MAINTAIN U.S. WATERWAYS AND MARITIME RESOURCES*

The accessibility of U.S. waterways and vitality of marine ecosystems enable economic activities across the United States to flourish. Communities across the United States are heavily dependent on maritime trade routes, marine resources and fisheries, and maritime tourism. DHS's expansive mission supports these economic interests by enforcing regulations to protect the marine environment, managing maritime safety programs and standards, maintaining aids to navigation, conducting maritime search and rescue, providing ice breaking services, and conducting maritime defense operations. These important initiatives keep the U.S. maritime jurisdiction—including the coastal environment, ports, Exclusive Economic Zone, and beyond—clean, safe, and secure against maritime threats. Desired Outcome: Safeguard waterways and maritime resources subject to the jurisdiction of the United States with the goal of facilitating freedom of movement, public safety, commercial activity, and U.S. national security.

### 4.3.1. Regulations

*Establish and enforce regulations for mariners, vessels, and facilities*

**Stakeholder(s):**

**Mariners**

**Maritime Facilities**

**Vessels**

### 4.3.2. Resources & Environment

*Protect marine resources and the environment*

### 4.3.3. Security, Safety & Stewardship

*Maintain maritime security, safety, and stewardship*

### 4.3.4. Defense

*Conduct maritime defense operations*

## 4.4. Financial Systems

*SAFEGUARD U.S. FINANCIAL SYSTEMS*

Economic prosperity depends on global trust in the U.S. dollar and reliable financial institutions and payment systems as critical enablers of global commerce. Although the digitization of financial systems has streamlined commerce and benefited the global economy, it has also exposed financial transactions to new attack vectors. Meanwhile, digital currencies present new challenges for DHS to prevent counterfeiting. These new challenges impose constraints on DHS that require it to either expand its workforce to keep pace with the threat environment or prioritize law enforcement investigations that counter the most significant criminal threats, while partnering with other law enforcement agencies under their related authorities. Desired Outcome: Protect the integrity of the U.S. financial system and reduce counterfeiting, financial crimes, fraud, and other criminal activity in or against any federally-insured financial institution.

**Stakeholder(s):**

**Law Enforcement Agencies**

### 4.4.1. Cybercrimes

*Investigate cybercrimes against the U.S. financial sector and related cyber markets and networks*

**Stakeholder(s):**

**U.S. Financial Sector**

### 4.4.2. Counterfeiting & Fraud

*Investigate currency counterfeiting and banking payment system fraud*

**Stakeholder(s):**

**Banks**

### 4.4.3. Financial Systems

*Share information and promote best practices nationwide to ensure financial systems are secure against attack, theft, or malicious activity*

**Stakeholder(s):**

**Financial Systems**

# 5. Preparedness & Resilience

*STRENGTHEN PREPAREDNESS AND RESILIENCE*

The United States will never be completely impervious to present and emerging threats and hazards across the homeland security mission space. Preparedness is a shared responsibility across federal, state, local, tribal, and territorial governments; the private sector; non-governmental organizations; and the American people. Some incidents will surpass the capabilities of communities, so the Federal Government must remain capable of responding to natural disasters, physical and cyber attacks, weapons of mass destruction attacks, critical infrastructure disruptions, and search and rescue distress signals. Following disasters, the Federal Government must be prepared to support local communities with long-term recovery assistance. The United States can effectively manage emergencies and mitigate the harm to American communities by thoroughly preparing local communities, rapidly responding during crises, and supporting recovery.

## 5.1. Preparedness

*BUILD A NATIONAL CULTURE OF PREPAREDNESS*

The United States must strive for a future where disasters cause fewer disruptions and less destruction throughout our communities. The prevalence of disaster declarations and recovery costs over the last decade demonstrate the need for local communities to improve their preparedness for predictable natural events. Building more resilient communities and investing in mitigation measures are the best ways to reduce risks to local communities arising from the loss of life, economic disruption, and infrastructure restoration. DHS is supporting communities to encourage self-sufficiency long before disasters arise by emphasizing pre-disaster mitigation efforts that strengthen infrastructure and reinforce existing structure, which can save lives and exponentially decrease post-disaster recovery costs. Additionally, DHS will enable communities impacted by natural disasters to rebuild better, stronger, and more resilient infrastructure to protect taxpayer investments and adequately prepare for future disasters. Desired Outcome: Prepare the Nation to be ready for the worst disasters and enhance public safety and property protection.

**Stakeholder(s):**
**Local Communities**

### 5.1.1. Risk, Mitigation & Insurance

*Incentivize investments that reduce risk and increase pre-disaster mitigation, including expanding the use of insurance to manage risk*

### 5.1.2. Awareness & Preparedness

*Improve awareness initiatives to encourage public action to increase preparedness*

### 5.1.3. Lessons & Exercises

*Use lessons from past disasters and exercises to inform community investment decisions and anticipate challenges that may emerge during future disasters*

### 5.1.4. Operational Plans

*Develop and implement pre-disaster operational plans to deliver lifesaving and life-sustaining commodities, equipment, and personnel from all available sources*

### 5.1.5. Continuity of Operations

*Coordinate and guide continuity of operations activities through partnerships with government and non-government stakeholders*

## 5.2. Response

*RESPOND DURING INCIDENTS*

This coordinated approach to emergency response enables DHS to apply its full scope of authority and operational capabilities to support impacted communities. For instance, DHS works with stakeholders across all levels of government to maintain interoperable communication systems that support response and recovery efforts. In the case of biological and chemical incidents, DHS works to identify, monitor, and assess emerging threats to recognize outbreaks and control the spread of health incidents. Where cyber incidents require a national response, DHS limits the immediate consequences and prevents the incident from spreading to other victims. These response capabilities ensure that communities across the United States are resilient against all threats and hazards. Desired Outcome: Respond quickly and decisively during catastrophic incidents to reduce their impact.

**Stakeholder(s):**

**Governments** :
*Natural and man-made disasters and emergencies can overwhelm even the best prepared governments, causing a high number of fatalities, widespread destruction, and economic and social damage.*

**Communities** :
*Communities impacted by incidents require guidance, tools, equipment, and resources to deliver necessary aid and relief to Americans in their time of need.*

**Emergency Response Providers** :
*Working with stakeholders across the country, DHS supports and promotes the ability of emergency response providers and relevant government officials to communicate in the event of natural disasters, acts of terrorism, and other hazards.*

**Government Officials**

**Community Leaders** :
*DHS responds to incidents by engaging directly with community leadership to provide support;*

**Federal Officials** :
*coordinating federal response and recovery efforts; and*

**DHS Surge Capacity Force** :
*providing critical resources such as the DHS Surge Capacity Force, search and rescue assets, communication systems, technical assistance, and other incident response functions.*

### 5.2.1. Response

*Manage and lead the U.S. response to natural and man-made incidents*

### 5.2.2. Search & Rescue

*Conduct mass search and rescue operations in the immediate aftermath of an incident*

### **5.2.3.** Stabilization & Restoration

*Assist with stabilization and restoration of community lifelines, including safety and security, food water and sheltering, health and medical, energy, communications, transportation, and hazardous material, immediately following an incident.*

### **5.2.4.** Health Threats

*Identify, monitor, and assess emerging threats to recognize outbreaks and control the spread of health incidents*

### **5.2.5.** Cyber Incidents

*Enhance cyber incident response capabilities and coordination to minimize the effects of cyber incidents*

### **5.2.6.** Intergovernmental Coordination

*Enhance intergovernmental coordination for emergency management by embedding federal integration teams throughout all levels of government and communities*

### **5.2.7.** Information, Awareness & Resources

*Improve information exchange, situational awareness, and prioritization of resources among emergency managers, first responders, and across the public and private sectors*

**Stakeholder(s):**

**Emergency Managers**

**First Responders**

**Public Sector**

**Private Sector**

## 5.3. Recovery

*SUPPORT OUTCOME-DRIVEN COMMUNITY RECOVERY*

Beyond the immediate response in the aftermath of catastrophic incidents, communities often require long-term national assistance to fully restore infrastructure, economic activity, social services, housing needs, and other critical government functions. DHS is streamlining and integrating existing disaster assistance processes to reduce the complexity of survivor support programs. Additionally, DHS is working with all levels of government to design outcome-driven recovery that enables communities to have greater control over their own recovery. To complement these initiatives, DHS is maturing the National Disaster Recovery Framework to help communities rebuild stronger, reduce future risk, and decrease disaster costs. Desired Outcome: Provide appropriate federal support and assistance to promote resilience and recovery in areas affected by natural and man-made disasters.

**Stakeholder(s):**

**Communities**

### 5.3.1. Collaboration

*Collaborate with impacted communities to restore overall capacity of community lifelines and facilitate a return to normalcy*

**Stakeholder(s):**

**Impacted Communities**

### 5.3.2. Recovery & Resilience

*Provide communities with sustained outcome-driven recovery to reinforce and rebuild damaged infrastructure and strengthen community resilience*

### 5.3.3. Assistance

*Deliver disaster assistance to eligible recipients*

## 5.4. Training & Exercises

*TRAIN AND EXERCISE FIRST RESPONDERS*

Most effective strategies for emergency management are federally supported and executed by the immediate authority of a jurisdiction. As disasters unfold, individuals and local government serve as the first responders to triage the incident and stabilize the situation. DHS promotes community-building initiatives to improve the strength of local networks and reinforce practical skills of first responders until further relief takes effect, such as a basic first aid, home maintenance, and emergency planning methods. Desired Outcome: America's first responders are trained to protect U.S. communities against persistent and emerging threats and hazards.

**Stakeholder(s):**

**First Responders**

### **5.4.1.** Law Enforcement Training

*Provide direct training for law enforcement professionals nationwide to enable them to fulfill their responsibilities safely and proficiently*

**Stakeholder(s):**

**Law Enforcement Professionals**

### **5.4.2.** Disaster Assistance Training & Equipment

*Train and equip first responders and other emergency workers for man-made and natural disasters*

**Stakeholder(s):**

**First Responders** **Emergency Workers**

### **5.4.3.** Exercises & Assessments

*Support and conduct exercises and assessment to increase whole community partner readiness and to identify safety and security gaps*

### **5.4.4.** Awareness

*Develop awareness of regional and local risk to better focus exercises and education on the higher risk threats facing a community*

# 6. Workforce

*CHAMPION THE DHS WORKFORCE AND STRENGTHEN THE DEPARTMENT*

Since the Department's formation, each Secretary has recognized the importance of strengthening the integrated relationships between and among Headquarters Offices and Operational Components to optimize the Department's efficiency and effectiveness. Despite the considerable progress during the last 15 years to establish and strengthen DHS management functions, the Department has much to improve. Over the next four years, DHS will continue to mature as an institution by increasing integration, clarifying roles and responsibilities, championing its workforce, advancing risk-based decision-making, and promoting transparency and accountability before the American people. In an important step forward, DHS is beginning to consolidate Support Components and the Office of the Secretary on the St. Elizabeths Campus, which will further promote integration.

## 6.1. Governance & Management

*STRENGTHEN DEPARTMENTAL GOVERNANCE AND MANAGEMENT*

Increasing responsibilities with limited budgets require clear leadership, effective strategic prioritization, and management by Department's leadership. DHS will continue to mature its Headquarters as an institution, including policymaking, management business processes, and other advisory responsibilities. DHS is further defining and prioritizing its operational needs with a Department-wide view based on input from Component operators and its external stakeholders. Through this approach, DHS is applying thorough and sound analytic studies to identify and implement the best solutions for the Nation's investment in homeland security. Desired Outcome: Enhance organizational management by aligning processes that translate leadership vision into action through strategic planning, operational capabilities and requirements, resourcing, acquisition, performance evaluation, and administrative functions.

### 6.1.1. Headquarters

*Define the role of DHS Headquarters and effectively position Headquarters Offices to enable Operational Components' activities*

**Stakeholder(s):**

**DHS Headquarters**

### 6.1.2. Integration & Coordination

*Promote Department-wide mission support and business support integration to improve coordination*

### 6.1.3. Priorities

*Ensure effective processes to identify and prioritize requirements, develop and implement strategies, policies, integrated plans, and requirements that execute presidential, legislative, and secretarial priorities*

### 6.1.4. Budget & Resources

*Formulate the Department's budget and allocate resources effectively and consistently with the articulated strategies, policies, plans, and operational requirements*

### 6.1.5. R&D

*Optimize research and development of solutions based on strategic, policy, operational requirements, and capability assessments*

## 6.2. Workforce

*DEVELOP AND MAINTAIN A HIGH PERFORMING WORKFORCE*

Maintaining a highly-skilled, diverse, and engaged workforce is critical to accomplishing the homeland security mission, which relies on dedicated personnel who go above and beyond to keep Americans safe from harm. From its beginning, DHS has overcome the challenges of standing up an enormous agency comprised of many moving parts, by staying focused on the core mission at hand. Despite the many advances, DHS continues to identify opportunities to significantly increase the efficiency and effectiveness of management systems that support the workforce while developing and sustaining a leadership cadre at every level that inspires an engaged and proficient workforce. Every day, the operators and employees of DHS perform difficult and often dangerous work that goes unseen by most of the American public. Investing in the ability of our workforce to perform to capacity is one of our highest priorities. DHS leadership continues to emphasize workforce engagement and improve agency-wide satisfaction. DHS is making significant improvement as evidenced by increases in both Employee the Engagement Index and the Inclusion Index. In addition, DHS is implementing agency-wide human capital solutions that identify and develop a continuous pipeline of leaders who are capable of attracting and retaining the best talent, encourage creativity and innovation to maximize employee performance, and invest in building career paths and initiatives that inspire work-life balance in order to incentivize and retain exceptional performers. Through dedicated workplace inclusion and employee engagement, DHS will enhance the current workforce and build the future workforce to accomplish the homeland security mission. Desired Outcome: Maximize mission success by hiring a skilled, diverse, and inclusive workforce, retaining world-class personnel, and empowering frontline operators and enabling personnel to do their jobs, enforce the law, and protect the Homeland.

### 6.2.1. Encouragement & Empowerment

*Encourage leadership and empower employees to execute their missions*

### 6.2.2. Hiring & Diversity

*Enhance recruiting efforts and streamline personnel hiring practices to ensure a diverse workforce*

### 6.2.3. Education & Training

*Improve personnel training, professional development, and education opportunities*

### 6.2.4. Rewards & Retention

*Retain and reward exceptional performers, enhance career paths, develop greater cross-component opportunities for career advancement*

### 6.2.5. Workforce Support

*Foster a resilient and prepared DHS workforce by supporting employees and their families*

### 6.2.6. Communication

*Improve leadership communication with the workforce*

**Stakeholder(s):**
**DHS Leaders**

### 6.2.7. Transparency, Fairness & Opportunity

*Promote a culture of transparency, fairness, and equal employment opportunity throughout the DHS workforce, providing avenues of redress and leadership support in addressing and resolving workplace conflict via integrated conflict management and Alternative Dispute Resolution systems*

### 6.2.8. Mentoring & Coaching

*Encourage the use of mentoring and coaching programs to enhance employee recruitment, engagement, and retention*

## 6.3. Operational Support

*OPTIMIZE SUPPORT TO MISSION OPERATIONS*

DHS Headquarters Offices and their Component-based mission support counterparts are critical elements of the DHS mission, providing operators and personnel with the equipment, training, technology, legal counsel, partnerships, and research to more effectively execute their responsibilities. DHS is increasingly integrating these functions across the Department and leveraging cross-Component capabilities and resources to create efficiencies and streamline processes. DHS mission support requires efficient and effective optimization of operations. Specifically, we should look to collaboration, consolidation, and shared services to improving mission support to operations. DHS is experimenting with solutions that leverage existing technologies to combat immediate and emerging threats; coordinating joint operations; closely monitoring operational needs to identify new statutory needs; identifying joint requirements and acquisition needs; and ensuring that DHS activities comply with civil rights, civil liberties, and privacy requirements. Together, these initiatives advance the Department and its workforce to keep pace with the ever-evolving threat landscape. Desired Outcome: Enhance mission operations by increasing coordination and cooperation with key homeland security partners; providing senior leadership and operators with situational awareness and actionable information; identifying research and development solutions for operational needs; maintaining property and assets; and conducting community engagement and outreach.

### 6.3.1. Partnerships

*Increase partnership engagement to support operational activities and outcomes*

### **6.3.2.** Awareness

*Improve situational awareness of events and incidents and provide actionable information to support senior leadership decisions across the Department*

**Stakeholder(s):**

**Senior DHA Leaders**

### **6.3.3.** Legal Support

*Provide legal support to operations and advocate for legal authorities necessary to accomplish the homeland security mission*

**Stakeholder(s):**

**Legal Authorities**

### **6.3.4.** Rights, Liberties & Privacy

*Preserve civil rights, civil liberties, and privacy in all efforts, activities, and programs aimed at securing the homeland and achieving the Department's goals and objectives*

### **6.3.5.** Property & Assets

*Manage and ensure sustainability and efficiency of Department real property and assets*

### **6.3.6.** Technology

*Enable secure, innovative, and interoperable technology solutions to enable operational success*

### **6.3.7.** Information & Data

*Mature information sharing and data management*

## Administrative Information

**Start Date:** 2019-10-01
**End Date:** 2024-09-30

**Publication Date: 2022-04-21**
**Source:** https://www.dhs.gov/sites/default/files/publications/19_0702_plcy_dhs-strategic-plan-fy20-24.pdf

### Submitter:

**Given Name:** Owen
**Surname:** Ambur
**Email:** Owen.Ambur@verizon.net
**Phone:**

**PDF formatted using TopLeaf XML publisher**
**www.turnkey.com.au**