The 2014 Quadrennial Homeland Security Review

Homeland Security

This page intentionally left blank

LETTER FROM THE SECRETARY

Homeland Security

June 18, 2014

Pursuant to Section 707 of the *Homeland Security Act of 2002* (P.L. 107-296), as amended by the *Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53), I am pleased to present the following report, *The 2014 Quadrennial Homeland Security Review*. This report provides a strong analytic and strategic foundation for one of my highest priorities, which is ensuring that the Department invests and operates in a cohesive, unified fashion and makes decisions that strengthen Departmental unity of effort.

Pursuant to congressional requirements, this report is being provided to the following Member of Congress:

The Honorable Michael McCaul
Chairman, House Committee on Homeland Security

The Honorable Bennie G. Thompson
Ranking Member, House Committee on Homeland Security

The Honorable Thomas R. Carper
Chairman, Senate Homeland Security and Governmental Affairs Committee

The Honorable Tom Coburn
Ranking Member, Senate Homeland Security and Governmental Affairs Committee

The first Quadrennial Homeland Security Review report was issued by DHS on February 1, 2010. DHS began work on this second review two years ago and included consultations with subject matter experts across the Federal Government, as well as state, local, tribal, and territorial governments, the private sector, and academic and other institutions.

Since taking office as Secretary of DHS on December 23, 2013, I have reviewed this report, and I concur with its recommendations. Reflecting deep analysis of the evolving strategic environment and outlining the specific strategic shifts necessary to keep our Nation secure, this report reflects the more focused, collaborative Departmental strategy, planning, and analytic capability that is necessary for achieving Departmental unity.

Sincerely,

Jeh Charles Johnson

This page intentionally left blank


U.S. Coast Guard

EXECUTIVE SUMMARY

In this report, we conclude that we will continue to adhere to the five basic homeland security missions set forth in the first Quadrennial Homeland Security Review report in 2010, but that these missions must be refined to reflect the evolving landscape of homeland security threats and hazards. The Deepwater Horizon oil spill in 2010, Hurricane Sandy in 2012, and the Boston Marathon bombing in 2013 illustrate these evolving threats and hazards. We must constantly learn from them and adapt. The terrorist threat is increasingly decentralized and may be harder to detect. Cyber threats are growing and pose ever-greater concern to our critical infrastructure systems as they become increasingly interdependent. Natural hazards are becoming more costly to address, with increasingly variable consequences due in part to drivers such as climate change and interdependent and aging infrastructure.

Meanwhile, this Nation's homeland security architecture has matured over the past four years, and we are determined that this progress continue. For example, our law enforcement and intelligence communities are becoming increasingly adept at identifying

and disrupting terrorist plotting in this country. Programs such as TSA Pre✓™ and Global Entry demonstrate the effectiveness and efficiency of risk-based security that can be achieved within budget constraints. It is also worth noting that, in late 2013, DHS received its first unqualified or "clean" audit opinion; this occurred just 10 years after the Department's formation, which was the largest realignment and consolidation of Federal Government agencies and functions since the creation of the Department of Defense in 1947.

Here are our five basic homeland security missions, revised to address threats and hazards over the next four years:

Prevent Terrorism and Enhance Security. Preventing terrorist attacks on the Nation is and should remain the cornerstone of homeland security. Since the last quadrennial review in 2010, the terrorist threat to the Nation has evolved, but it remains real and may even be harder to detect. The Boston Marathon bombing illustrates the evolution of the threat. Through the U.S. Government's counterterrorism efforts, we have degraded the ability of al-Qa'ida's senior leadership in Afghanistan and Pakistan to centrally plan and execute sophisticated external attacks. But since 2009, we have seen the rise of al-Qa'ida affiliates, such as al-Qa'ida in the Arabian Peninsula, which has made repeated attempts to export terrorism to our Nation. Additionally, we face the threat of domestic-based "lone offenders" and those who are inspired by extremist ideologies to radicalize to violence and commit acts of terrorism against Americans and the Nation. These threats come in multiple forms and, because of the nature of independent actors, may be hardest to detect. We must remain vigilant in detecting and countering these threats. Given the nature of this threat, engaging the public and private sectors through campaigns, such as "If You See Something, Say Something™" and the Nationwide Suspicious Activity Reporting Initiative, and through partnering across federal, state, local, tribal, and territorial law enforcement will, over the next four years, become even more important.

Secure and Manage Our Borders. We must continue to improve upon border security, to exclude terrorist threats, drug traffickers, and other threats to national security, economic security, and public safety. We will rely on enhanced technology to screen incoming cargo at ports of entry and will work with foreign partners to monitor the international travel of individuals of suspicion who seek to enter this country. We will continue to emphasize risk-based strategies that are smart, cost-effective, and conducted in a manner that is acceptable to the American people. We must remain agile in responding to new trends in illegal migration, from Central America or elsewhere. Meanwhile, we recognize the importance of continuing efforts to promote and expedite lawful travel and trade that will

continue to strengthen our economy.

Enforce and Administer Our Immigration Laws. We will continually work to better enforce our immigration laws and administer our immigration system. We support common-sense immigration reform legislation that enhances border security, prevents and discourages employers from hiring undocumented workers, streamlines our immigration processing system, and provides an earned pathway to citizenship for the estimated 11.5 million undocumented immigrants in this country. It is indeed a matter of homeland security and common sense that we encourage those physically present in this country to come out of the shadows and to be held accountable. Offering the opportunity to these 11.5 million people—most of whom have been here 10 years or more and, in many cases, came here as children—is also consistent with American values and our Nation's heritage. We will take a smart, effective, and efficient risk-based approach to border security and interior enforcement and continually evaluate the best use of resources to prioritize the removal of those who represent threats to public safety and national security.

Safeguard and Secure Cyberspace. We must, over the next four years, continue efforts to address the growing cyber threat, illustrated by the real, pervasive, and ongoing series of attacks on our public and private infrastructure. This infrastructure provides essential services such as energy, telecommunications, water, transportation, and financial services and is increasingly subject to sophisticated cyber intrusions which pose new risks. As the Federal Government's coordinator of efforts to counter cyber threats and other hazards to critical infrastructure, DHS must work with both public and private sector partners to share information, help make sure new infrastructure is designed and built to be more secure and resilient, and continue advocating internationally for openness and security of the Internet and harmony across international laws to combat cybercrime. Further, DHS must secure the Federal Government's information technology systems by approaching federal systems and networks as an integrated whole and by researching, developing, and rapidly deploying cybersecurity solutions and services at the pace that cyber threats evolve. And finally, we must continue to develop cyber law enforcement,

U.S. Department of Homeland Security

incident response, and reporting capabilities by increasing the number and impact of cybercrime investigations, sharing information about tactics and methods of cyber criminals gleaned through investigations, and ensuring that incidents reported to any federal department or agency are shared across the U.S. Government. In addition, the Federal Government must continue to develop good working relationships with the private sector, lower barriers to partnership, develop cybersecurity best practices, promote advanced technology that can exchange information at machine speed, and build the cyber workforce of tomorrow for DHS and the Nation.

Strengthen National Preparedness and Resilience. Acting on the lessons of Hurricane Katrina, we have improved disaster planning with federal, state, local, tribal, and territorial governments, as well as nongovernmental organizations and the private sector; pre-positioned a greater number of resources; and strengthened the Nation's ability to respond to disasters in a quick and robust fashion. Seven years after Katrina, the return on these investments showed in the strong, coordinated response to Hurricane Sandy. We must continue this progress.

This review recognizes the environment in which we must pursue the homeland security missions over the next four years. To support priority security requirements in a sustainable way, a corollary responsibility for DHS is to become more efficient and effective across a large and decentralized structure. As a Department, we must eliminate duplicative processes, develop common platforms, and purchase single solutions, while pursuing important commitments, such as the recapitalization of the aging Coast Guard fleet. DHS must and will also address the low morale that exists within many of its Components.

Finally, we recognize that we operate at a time when the public's confidence in the government's ability to function and work for them is low. DHS is unique among federal agencies for the large, daily engagement it has with the public at airports, seaports, and land ports of entry. Thus, the public's attitude toward the entire Federal Government can be shaped by interactions with DHS. Over the next four years, DHS will find opportunities to promote confidence in its ability to fulfill its mission.

There is no more important function that a government can provide for its people than safety and security. Through the leadership of our President, and in full partnership with other federal departments and agencies; state, local, tribal, and territorial governments; nongovernmental and private sector organizations; our foreign allies; and the American public, we will continue to work hard in pursuit of the homeland security missions; nothing less than the safety and security of the American people depend on this.

TABLE OF CONTENTS

This page intentionally left blank

1. LEGAL REQUIREMENT FOR THE REVIEW AND REPORT

Section 707 of the *Homeland Security Act of 2002* (P.L. 107-296), as amended by the *Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53), includes the following requirement:

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

(a) Requirement

(1) Quadrennial reviews required

In fiscal year 2009, and every 4 years thereafter, the Secretary shall conduct a review of the homeland security of the Nation (in this section referred to as a "quadrennial homeland security review").

(2) Scope of reviews

Each quadrennial homeland security review shall be a comprehensive examination of the homeland security strategy of the Nation, including recommendations regarding the long-term strategy and priorities of the Nation for homeland security and guidance on the programs, assets, capabilities, budget, policies, and authorities of the Department.

(3) Consultation

The Secretary shall conduct each quadrennial homeland security review under this subsection in consultation with--

(A) the heads of other Federal agencies, including the Attorney General, the Secretary of State, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of the Treasury, the Secretary of Agriculture, and the Director of National Intelligence;

(B) key officials of the Department; and

(C) other relevant governmental and nongovernmental entities, including state, local, and tribal government officials, members of Congress, private sector representatives, academics, and other policy experts.

(4) Relationship with future years homeland security program

The Secretary shall ensure that each review conducted under this section is coordinated with the Future Years Homeland Security Program required under section 454 of this title.

(b) Contents of review

In each quadrennial homeland security review, the Secretary shall--

(1) delineate and update, as appropriate, the national homeland security strategy, consistent with appropriate national and Department strategies, strategic plans, and Homeland Security Presidential Directives, including the National Strategy for Homeland Security, the National Response Plan, and the Department Security Strategic Plan;

(2) outline and prioritize the full range of the critical homeland security mission areas of the Nation;

(3) describe the interagency cooperation, preparedness of Federal response assets, infrastructure, budget plan, and other elements of the homeland security program and policies of the Nation associated with the national homeland security strategy, required to execute successfully the full range of missions called for in the national homeland security strategy described in paragraph (1) and the homeland security mission areas outlined under paragraph (2);

(4) identify the budget plan required to provide sufficient resources to successfully execute the full range of missions called for in the national homeland security strategy described in

paragraph (1) and the homeland security mission areas outlined under paragraph (2);

(5) include an assessment of the organizational alignment of the Department with the national homeland security strategy referred to in paragraph (1) and the homeland security mission areas outlined under paragraph (2); and

(6) review and assess the effectiveness of the mechanisms of the Department for executing the process of turning the requirements developed in the quadrennial homeland security review into an acquisition strategy and expenditure plan within the Department.

(c) Reporting

(1) In general

Not later than December 31 of the year in which a quadrennial homeland security review is conducted, the Secretary shall submit to Congress a report regarding that quadrennial homeland security review.

(2) Contents of report

Each report submitted under paragraph (1) shall include--

(A) the results of the quadrennial homeland security review;

(B) a description of the threats to the assumed or defined national homeland security interests of the Nation that were examined for the purposes of that review;

(C) the national homeland security strategy, including a prioritized list of the critical homeland security missions of the Nation;

(D) a description of the interagency cooperation, preparedness of Federal response assets, infrastructure, budget plan, and other elements of the homeland security program and policies of the Nation associated with the national homeland security strategy, required to execute successfully the full range of missions called for in the applicable national homeland security strategy referred to in subsection (b)(1) of this section and the homeland security mission areas outlined under subsection (b)(2) of this section;

(E) an assessment of the organizational alignment of the Department with the applicable national homeland security strategy referred to in subsection (b)(1) of this section and the homeland security mission areas outlined under subsection (b)(2) of this section, including the Department's organizational structure, management systems, budget and accounting systems, human resources systems, procurement systems, and physical and technical infrastructure;

(F) a discussion of the status of cooperation among Federal agencies in the effort to promote national homeland security;

(G) a discussion of the status of cooperation between the Federal Government and state, local, and tribal governments in preventing terrorist attacks and preparing for emergency response to threats to national homeland security;

(H) an explanation of any underlying assumptions used in conducting the review; and

(I) any other matter the Secretary considers appropriate.

(3) Public availability

The Secretary shall, consistent with the protection of national security and other sensitive matters, make each report submitted under paragraph (1) publicly available on the Internet website of the Department.

(d) Authorization of appropriations

There are authorized to be appropriated such sums as may be necessary to carry out this section.

U.S. Coast Guard

2. THE PURPOSE OF THE SECOND QUADRENNIAL HOMELAND SECURITY REVIEW

More than 12 years after the attacks of September 11, 2001, the United States is poised to begin a new era in homeland security. Long-term changes in the security environment and critical advances in homeland security capabilities require us to rethink the work DHS does with our partners—the work of building a safe, secure, and resilient Nation.

This new era is defined by both positive and negative factors: the termination of offensive military operations in Iraq and Afghanistan, two of the longest conflicts in U.S. history; the rise of fiscal challenges at home and in partner states; global economic growth, tempered by increased volatility; growth in domestic energy supplies, contrasted with instability in major energy-producing regions; resource constraints in a more densely populated, urbanized world; and rapid technological change that impacts how we live, work, communicate, travel, and access knowledge.

This Quadrennial Homeland Security Review is consistent with, and supports the enduring national interests of the United States, as articulated in our national security strategy:

- The security of the United States, its citizens, and U.S. allies and partners;
- A strong, innovative, and growing U.S. economy in an open international economic system that promotes opportunity and prosperity;
- Respect for universal values at home and around the world; and
- An international order advanced by U.S. leadership that promotes peace, security, and opportunity through stronger cooperation to meet global challenges.

These national interests are inextricably linked and cannot be pursued in isolation.

THE FIVE HOMELAND SECURITY MISSIONS

The first quadrennial review established the five enduring missions of homeland security. This review reaffirms the five-mission structure and updates the missions (detailed in the Mission Framework In Depth section). The updated missions are:

- Prevent Terrorism and Enhance Security;
- Secure and Manage Our Borders;
- Enforce and Administer Our Immigration Laws;
- Safeguard and Secure Cyberspace; and
- Strengthen National Preparedness and Resilience.

Accomplishing these missions requires unity of effort—both across every area of DHS activity and among the numerous homeland security partners and stakeholders. The five missions advance each of the four enduring national interests articulated in the *National Security Strategy*. Successful accomplishment of

HOMELAND SECURITY VISION

A homeland that is safe, secure, and resilient against terrorism and other hazards, where American interests, aspirations, and way of life can thrive.

Transportation Security Administration

these missions results in a secure homeland, fosters a thriving economy, and protects privacy, civil rights, and civil liberties. We pursue enduring national interests and conduct our missions in service to a single homeland security vision: a homeland that is safe, secure, and resilient against terrorism and other hazards, where American interests, aspirations, and way of life can thrive.

As the threats and hazards we face change, the way we and our partners and stakeholders carry out our missions must change as well. The second Quadrennial Homeland Security Review comprehensively examined the homeland security strategic environment and identified strategic shifts and areas of ongoing priority and renewed emphasis for the Nation's long-term homeland security strategy.

To set homeland security priorities, DHS leads national efforts to assess, analyze, and compare ***risk***—which is a function of the likelihood and potential impacts of different homeland security threats and hazards. However, we recognize that the likelihood and consequence of specific threats and hazards may be influenced over time by interdependent economic, political, social, environmental, and technological factors, as well as trends and future uncertainties. We use systems analysis to create a more dynamic view of how these forces influence threats and hazards and how risk may change over time. This forward-looking understanding of risk allows us to prioritize our actions within the five missions and maximize the use of our limited resources.

Based on a deep examination of the strategic environment, we identified six drivers of change and six challenges that pose the most strategically significant risk over the next five years (described in the Strategic Environment section). From those drivers and challenges, we identified the following strategic priorities that impact all five homeland security missions:

- An updated posture to address the increasingly decentralized terrorist threat;
- A strengthened path forward for cybersecurity that acknowledges the increasing interdependencies among critical systems and networks;
- A homeland security strategy to manage the urgent and growing risk of biological threats and hazards;
- A risk segmentation approach to securing and managing flows of people and goods into and out of the United States; and
- A new framework for improving the efficiency and effectiveness of our mission execution through public-private partnerships.

Beyond these strategic priorities, this second quadrennial review also highlights ongoing areas of priority and renewed areas of emphasis based on risk and other considerations—countering nuclear threats, strengthening our immigration system, and enhancing national resilience. Finally, building upon the first Quadrennial Homeland Security Review, this review provides an updated view of the Nation's homeland security mission goals and objectives.

Federal Law Enforcement Training Center


U.S. Coast Guard

3. THE STRATEGIC ENVIRONMENT

DRIVERS OF CHANGE

This Nation's homeland security architecture has matured over the past four years, as illustrated by the development of a One DHS approach to a range of homeland security challenges, and we are determined that this progress continue. For example, programs such as TSA Pre✓™ and Global Entry demonstrate the effectiveness and efficiency of risk-based security and cross-Departmental integration that can be achieved within budget constraints. In addition, law enforcement is becoming increasingly adept at identifying and disrupting terrorist plotting in this country. It is also worth noting that, in late 2013, DHS received its first unqualified or "clean" audit opinion; this occurred just 10 years after the Department's formation, which was the largest realignment and consolidation of federal government agencies and functions since the creation of the Department of Defense in 1947.

Our charge in the quadrennial review, however, is to identify and describe the threats to the

Nation's homeland security interests. The first step in understanding threats and hazards is identifying key areas of change. These areas of change are detailed below.

THE EVOLVING TERRORISM THREAT

The nature of the terrorist threat to the United States has evolved since the September 11, 2001 attacks—and indeed, since the first Quadrennial Homeland Security Review in 2010. Counterterrorism pressure in the Afghanistan–Pakistan region has degraded the ability of al-Qa'ida's senior leadership to launch sophisticated external attacks, although the leadership that remains continues to aspire to attack the United States. At the same time, other groups affiliated and ideologically aligned with al-Qa'ida have emerged with the intent and, in some cases, the capability to carry out attacks against the United States and American citizens overseas.

Al-Qa'ida in the Arabian Peninsula is currently the al-Qa'ida affiliate of the greatest concern because of its demonstrated and continuing interest in advancing plots to attack the United States, particularly against the aviation industry.

> *"The evolution of the terrorist threat demands a well-informed, highly agile, and well-networked group of partners and stakeholders…"*

Also of concern are militants who support al-Qa'ida's international agenda and have established bases of operation in conflict zones in the Middle East, West Africa, and North Africa, particularly in Syria and neighboring states. These safe havens could allow them to plan and launch external operations and train recruits who have Western passports and who can return home with combat skills and a violent anti-Western agenda.

Al-Qa'ida, its affiliates, and adherents also use propaganda to inspire U.S.- and Western-based supporters who have not traveled to conflict zones to conduct terrorist attacks. Lone offenders—prime targets of English-language messaging by al-Qa'ida affiliates—tend to favor plots involving the use of easily acquired weapons or explosives. Lone offenders and small groups acting on their own initiative and without direction of a terrorist group are among the most persistent and difficult threats to counter. In recent years, there have been several acts of violence against military targets by lone offenders as well as attempted attacks on civilian populations by individuals motivated by al-Qa'ida. In addition, other groups and individuals inspired by a range of religious, political, or other ideological beliefs have promoted and used violence against the United States. While not as

significant as the threat posed by al-Qa'ida, its adherents, and its affiliates, these other groups and individuals remain a persistent threat.

Improvised explosive devices continue to represent a significant threat because they are easy to build and popular among violent extremists. Further, violent extremists have shown an enduring interest in improving improvised explosive device materials and methods to evade security measures. Violent extremists also seek to conduct small arms attacks. While violent extremists' mistakes have sometimes contributed to intelligence and law enforcement successes, plots using improvised explosive devices or small arms present unique challenges as a result of being tactically simple and adaptable in both timing and location of execution, complicating discovery and disruption by authorities.

Chemical, biological, radiological, and nuclear threats are enduring areas of concern; the consequences of these attacks are potentially high even though the likelihood of their occurrence is relatively low. Small scale chemical attacks are expected to remain more likely, because of accessibility to precursor materials and toxic industrial chemicals and the relative lack of specialized skills and knowledge required to conduct such attacks. However, nuclear terrorism and bioterrorism pose the most strategically significant risk, the former because of its potential consequences, and the latter because of potential increases in both likelihood and consequence. While the difficulty of stealing a nuclear weapon or fabricating one from stolen or diverted weapons materials reduces the likelihood of this type of attack, the extremely high consequences of an improvised nuclear device attack make it an ongoing top homeland security risk. Biological terrorism becomes more likely as the capability, knowledge, and resources required to carry out an attack become more widely accessible. While biotechnology has great potential for good, its continued expansion around the world challenges our ability to prevent and detect potential bioterrorist incidents.

INFORMATION AND COMMUNICATIONS TECHNOLOGY

The globally interconnected digital information and communications infrastructure, known as cyberspace, has changed dramatically in recent years. Cyberspace has become an integral part of daily life in America and around the world. An estimated two billion people have at least 12 billion computers and devices, including global positioning systems, mobile phones, satellites, data routers, desktop computers, and industrial control computers that run power plants, water systems, and more. A vast array of interdependent information technology networks, systems, services, and resources enable communication, facilitate travel, power our homes, run our economy, and provide essential government

services. These systems provide enormous benefits to our society and economy, but they also create new risks and vulnerabilities.

Malicious actors continue to become more sophisticated in exploiting these vulnerabilities, increasing the risks to critical infrastructure. These actors seek to steal financial information, intellectual property, trade secrets, and other sensitive information from businesses small and large. They also seek to capture personal and financial information from our citizens. While many corporations make cybersecurity a core aspect of their enterprise risk management, many small businesses and public sector entities face financial and personnel constraints in doing the same.

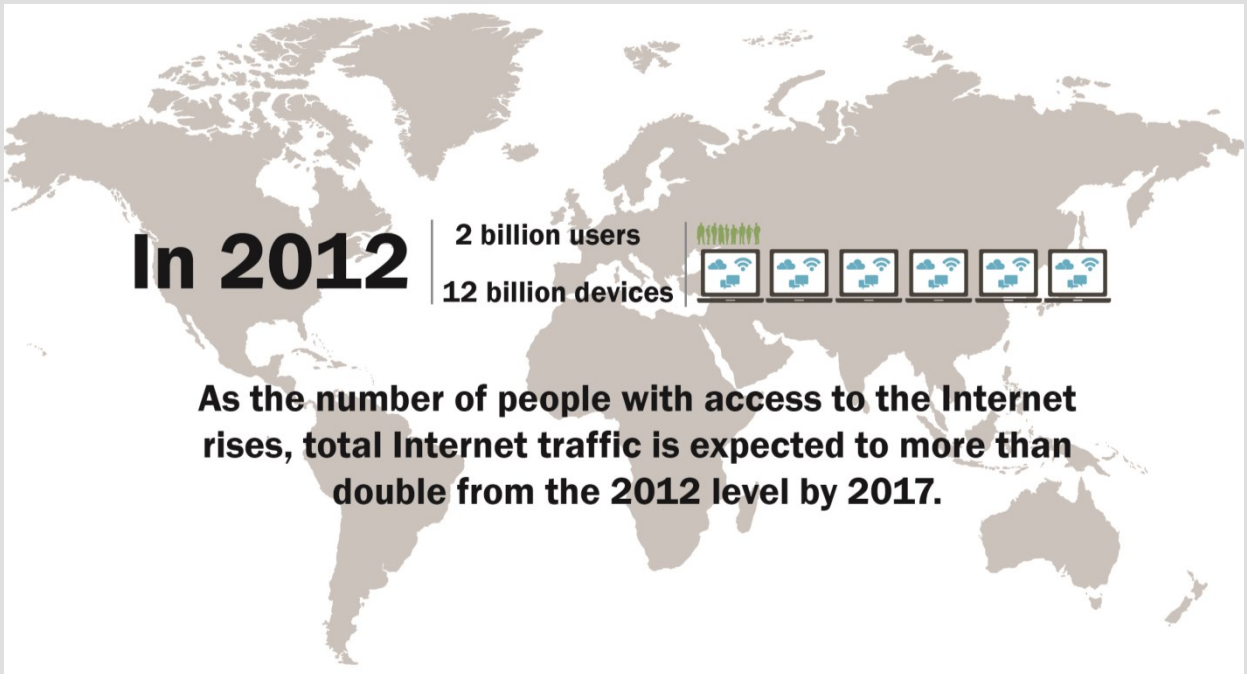


Figure 1: Global Internet use is high and growing.

At the same time, information and communications technology are enabling goods and services to flow through the global supply chain more rapidly than ever before. Moreover, flows of data and information are, in some cases, replacing physical flows of goods. One example of this dynamic is the emerging trend of three-dimensional printing. Of concern, the ongoing development and adoption of electronic payment systems and their increasing use for illicit trafficking and smuggling create substantial new challenges for investigation and interdiction.

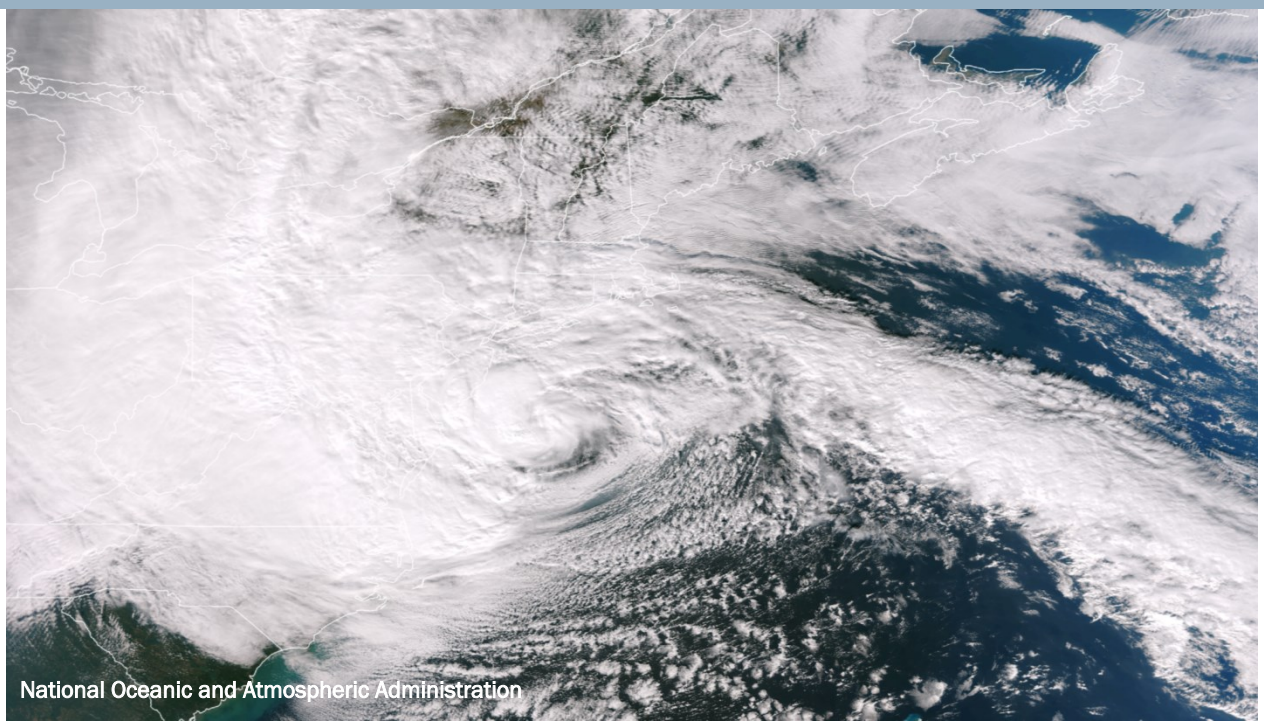
We must not forget that cyberspace provides opportunities for homeland security. With appropriate protections for individual privacy and civil rights and civil liberties, technology can enhance situational awareness, improve investigative capabilities, and support operational integration.

NATURAL DISASTERS, PANDEMICS, AND CLIMATE CHANGE

Natural disasters, pandemics, and the trends associated with climate change continue to present a major area of homeland security risk.

Of the naturally occurring events, a devastating pandemic remains the highest homeland security risk. Both the likelihood and consequences of this low probability, high-impact event are expected to increase, driven in large part by increasing opportunities for novel infectious diseases to emerge and spread quickly around the world. Changes in land use and agriculture, including rising urbanization in countries where disease is endemic or potentially endemic, promote the emergence of potential pandemic-causing diseases. Increasing global trade and travel have the potential to fuel the spread of infectious diseases around the world, challenging the capacity of public health systems at home and abroad to handle pandemics. Rising antiviral and antibacterial resistance have the potential to severely limit the effectiveness of available medical countermeasures, but other disease prevention and treatment techniques are now emerging.

Weather events present a significant and growing challenge, with several multi-billion dollar disasters in recent years. Hurricane Sandy, the largest diameter Atlantic storm on record, is estimated to have killed 117 people in the United States and caused widespread flooding. More than 8.5 million people were left without power, and the storm caused tens of billions of dollars in damage. Other disasters, particularly earthquakes, droughts, and floods, also pose significant risks to the Nation. The risk of these disasters is increased by the vulnerability of aging infrastructure, increasing population density in high-risk areas,


National Oceanic and Atmospheric Administration

and—in the case of droughts, floods, and hurricanes—by trends associated with climate change. Pandemic disease, hurricanes, and other natural disasters not only have the potential to cause severe consequences, including fatalities and economic loss, but also may overwhelm the capacities of critical infrastructure, causing widespread disruption of essential services across the country.

Climate change and associated trends may also indirectly act as "threat multipliers." They aggravate stressors abroad that can enable terrorist activity and violence, such as poverty, environmental degradation, and social tensions. More severe droughts and tropical storms, especially in Mexico, Central America, and the Caribbean, could also increase population movements, both legal and illegal, across the U.S. border. Melting sea ice in the Arctic may lead to new opportunities for shipping, tourism, and legal resource exploration, as well as new routes for smuggling and trafficking, increased risk of environmental disasters, and illicit resource exploitation. Higher temperatures may change patterns of human, animal, and plant diseases, putting the workforce, the general public, and plant and animal health at higher risk of illness. The United States may need to prepare for more frequent, short-term, disaster-driven migration. Higher temperatures and more intense storms may also damage or disrupt telecommunications and power systems, creating challenges for telecommunications infrastructure, emergency communications, and the availability of cyber systems. Finally, the cost of preparing for, responding to, and recovering from such events is anticipated to grow as weather-related events continue to become more severe and damaging.

INTERDEPENDENT AND AGING CRITICAL INFRASTRUCTURE SYSTEMS AND NETWORKS

The Nation's critical infrastructure provides the essential services that underpin the American way of life. The concept of critical infrastructure as discrete, physical assets has become outdated as everything becomes linked to cyberspace. This "cyber-physical convergence" has changed the risks to critical infrastructure in sectors ranging from energy and transportation to agriculture and healthcare. Moreover, this interconnected cyber-physical infrastructure consists of multiple systems that rely on one another to greater degrees for their operations and, at times, operate independent of human direction. One example of this type of interconnected system is the global supply chain, where information and communications technologies are providing real-time location services, traffic updates, emergency notifications, and more.

> *Critical infrastructure are those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*
>
> – Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience" (2013)

Critical infrastructure owners and operators also continue to experience increasingly sophisticated cyber intrusions, which provide malicious actors the ability to disrupt the delivery of essential services, cause physical damage to critical infrastructure assets, and potentially produce severe cascading effects.

The aging or deteriorating condition of significant aspects of critical infrastructure systems weakens our resilience and can affect our Nation's security and prosperity. Infrastructure investment has not kept pace with U.S. population growth or growth in demand. One-third of major roads are in poor or mediocre condition, and approximately one-quarter of the Nation's bridges are either structurally deficient or functionally obsolete. Though growth in demand for electricity has slowed, funding gaps for electric infrastructure could top $100 billion by the end of the decade. Overall, blackouts and other electrical disturbances have increased by more than 140 percent since 2007. Although weather-related events have

been the main cause of major electrical outages in the United States, many outages have been attributed to system operations failures, and reliability issues are emerging due to the complex issues of retiring older infrastructure. Without investment in recapitalization and new technologies, and in light of the potential for increased weather events, the aging electric grid will likely continue to experience disruptions in service. Our country needs an estimated $682 billion in wastewater and drinking water infrastructure improvements over the next 20 years, as well. Hurricane Sandy caused an estimated combined 11 billion gallons of sewer overflows in eight northeast states and the District of Columbia.

Due in large part to financial constraints, the Nation's public health capacity has eroded in recent years, as inadequate funding for infrastructure—from laboratories to community health centers—has been aggravated by increased demand on an already strained system. As a result, public health infrastructure systems are under significant strain on a day-to-day basis, leading to decreased capacity to address large-scale public health emergencies that may emerge.

These challenges present significant obstacles to performing our missions, particularly during times of disaster. However, there are unique opportunities to build our critical infrastructure systems to be more reliable, efficient, and resilient than they were before. For example, as we rebuild aging and failing infrastructure, we can design in cost-effective security and resilience features. By leveraging new tools, such as information and communications technology, building stronger partnerships, and adopting key lessons learned, we are able to update and adapt critical infrastructure systems to better meet future challenges.

FLOWS OF PEOPLE AND GOODS: INCREASING VOLUME AND SPEED

Flows of people and goods around the world have expanded dramatically in recent years. The value of U.S. exports and imports increased substantially between 2005 and 2012; exports increased by 72 percent, and imports increased by 36 percent. Both are expected to grow an average of six percent annually through 2030. Lawful travel to the United States increased 36 percent from 2005 to 2012 and is estimated to increase by more than 25 percent from 2012 to 2018. Air travel has also seen substantial growth internationally, increasing by 47 percent in the same seven-year period.

These trends will be amplified by other factors, including the forthcoming expansion of the Panama Canal, which is likely to substantially increase the volume of trade going through U.S. ports on the East Coast and in the Gulf of Mexico. In addition, the global systems that move goods from one location to another have grown increasingly efficient through

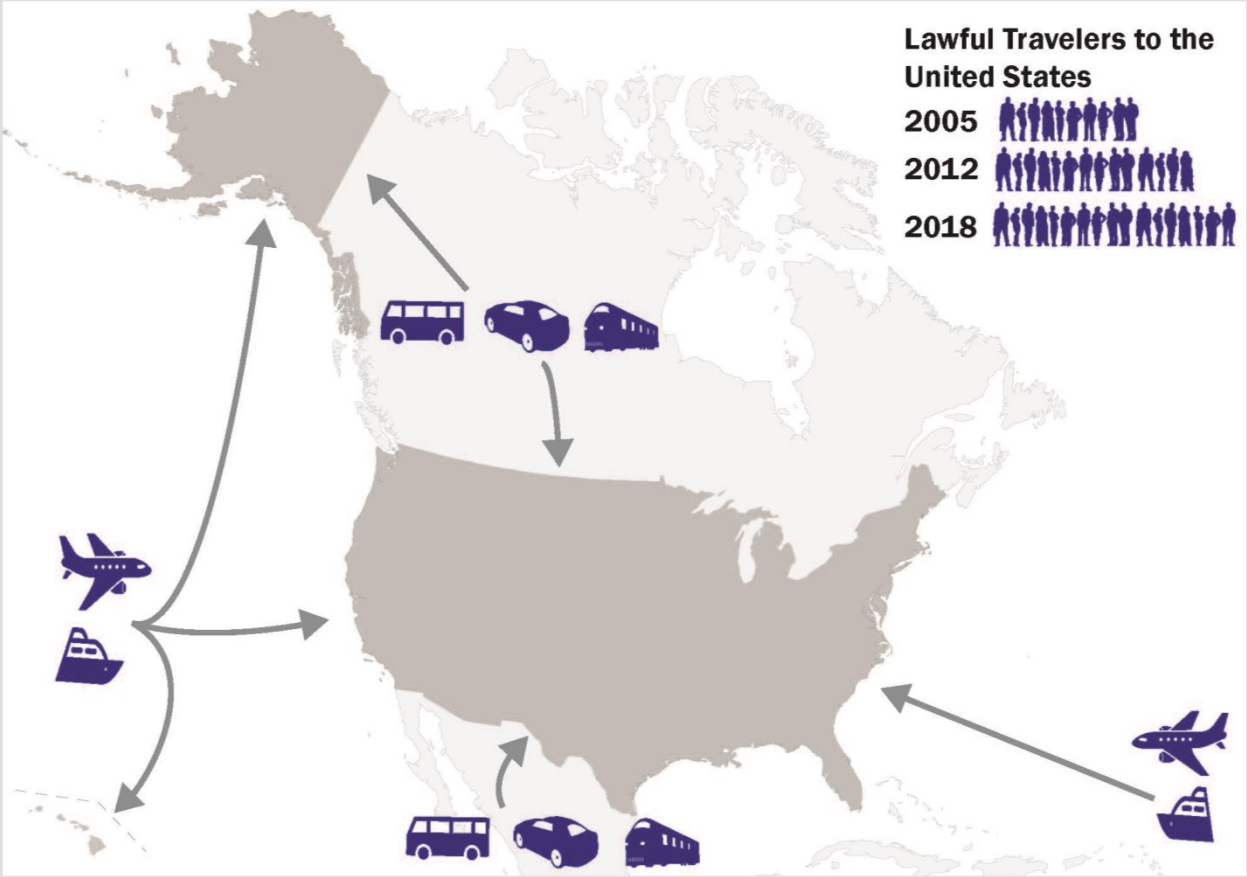


Figure 2: Lawful travel to the United States increased 36 percent from 2005 to 2012 and is estimated to increase by more than 26 percent from 2012 to 2018.

innovations such as intermodal shipping. This has increased trade over our borders. Rail intermodal traffic— transporting shipping containers and truck trailers on railroad flat cars— increased nearly fourfold between 1980 and 2012.

However, the trade and travel system is also susceptible to threats and hazards. When air and maritime travel into and within the United States was halted in the immediate aftermath of the attacks of September 11, 2001, the resulting disruptions had tremendous negative impacts on our economy. Short-term supply chain disruptions due to port strikes and natural disasters have also impacted flows of cargo. Cascading events, such as the 2011 earthquake and tsunami in Japan that led to the Fukushima Daiichi nuclear disaster and the temporary idling of auto plants in the United States, demonstrate the potential for significant disruption to the lawful trade and travel system.

The increased movement of people and goods across our borders provides many opportunities but also provides more places for illegal goods, unauthorized migrants, and

threats to hide. Illicit materials, threats, and hazards may cross at or between our ports of entry deliberately or inadvertently. Illegal shipments, such as intellectual property infringing goods, adversely impact our nation's economy. Unauthorized migration is influenced by many factors, including weak rule of law and violence in sending countries. Violent extremists and criminals can hide within this larger flow of migrants who intend no harm. More travelers moving more efficiently through the lawful trade and travel system also may increase the potential for rapid escalation of biological events across regions, countries, and continents.

Transnational criminal organizations rely on revenues generated through the sale of illegal drugs and counterfeit goods, human trafficking and smuggling, and other criminal activities. These organizations continue to expand in size, scope, and influence and are capitalizing on technological innovation, including new platforms to sell illicit goods, innovative ways of moving money, tools for coordinating operations, and a variety of other criminal and cyber activities. Transnational criminal organizations are gaining strength by taking advantage of the same innovations in management and supply chain structures that are propelling multinational corporations.

As transnational criminal organizations grow stronger and challenge or corrupt governments in many regions, they are moving more freely, expanding their networks, and acquiring and distributing military-grade equipment. Violent extremist networks can also conduct these profitable criminal activities on their own, exploiting the same vulnerabilities in finance, trade and travel, and immigration.

Generally, higher volumes of people and goods will stress current screening and detection capabilities and capacities.

BUDGET DRIVERS

The out year funding assumptions applied for this quadrennial review are based on the economic and policy assumptions underpinning the President's 2015 Budget submission to Congress. Since the last Quadrennial Homeland Security Review, economic conditions have had wide-ranging impacts across homeland security partners and stakeholders, affecting both daily operations and current investments to meet longer-term needs and challenges. For example, more than two-thirds of the nation's 30 largest metro regions have not seen municipal government revenue return to pre-recession levels. While public safety spending is often the last part of the budget to be cut, by 2011, 20 of the 30 largest metro regions had reduced spending on public safety, impacting daily operations and the ability to respond to emergencies.

Going forward, the budgets of many homeland security partners are assumed to maintain parity with inflation or modestly decline in real terms. We also assume that state budgets will be constrained by reductions in federal grants, which are projected to remain below their 2007 historic high (as a percentage of gross domestic product). International partners will likely face similar constraints. Economic pressures on families, nonprofits, and the private sector may also adversely affect local investment in the security and resilience of our communities.


Federal Emergency Management Agency

Partnerships with state, local, tribal, and territorial governments; international partners; nongovernmental organizations; and the private sector are essential to meet mutual safety and security needs and extend services in a time of flat or declining budgets. State, local, tribal, and territorial governments are maintaining services through measures such as sharing resources across jurisdictional lines and privatizing infrastructure. Public-private partnerships are a key focus of this report because the security challenges facing our Nation are too large and complex for either government or the private sector to address alone. Working together to invest in infrastructure projects and to expedite travel and trade benefits both private and public sectors.

PREVAILING CHALLENGES THAT POSE THE MOST STRATEGICALLY SIGNIFICANT RISK

The threats, hazards, trends, and other dynamics reflected in the drivers of change suggest several prevailing strategic challenges that will drive risk over the next five years:

- The **terrorist threat** is evolving and, while changing in shape, remains significant as attack planning and operations become more decentralized. The United States and its interests, particularly in the transportation sector, remain persistent targets.
- Growing **cyber threats** are significantly increasing risk to critical infrastructure and to the greater U.S. economy.
- **Biological concerns** as a whole, including bioterrorism, pandemics, foreign animal diseases, and other agricultural concerns, endure as a top homeland security risk because of both potential likelihood and impacts.
- **Nuclear terrorism** through the introduction and use of an improvised nuclear device, while unlikely, remains an enduring risk because of its potential consequences.
- **Transnational criminal organizations** are increasing in strength and capability, driving risk in counterfeit goods, human trafficking, illicit drugs, and other illegal flows of people and goods.
- **Natural hazards** are becoming more costly to address, with increasingly variable consequences due in part to drivers such as climate change and interdependent and aging infrastructure.

Beyond these specific strategic challenges, factors such as technology and migration present both opportunities and challenges for the homeland security community. Technological advances in communications, big data, manufacturing, and biological sciences provide new and lower cost capabilities that may benefit both the United States and our adversaries. Similarly, while lawful immigration greatly benefits the United States, attempted unauthorized migration poses consistent challenges for the management of our legal immigration system, borders, and ports of entry.

POTENTIAL "BLACK SWANS"

There are potential changes in the world around us that, while highly unlikely, would dramatically impact homeland security were they to occur. Such changes may come from previously unknown aspects of the strategic environment or may be the result of known aspects behaving in an unforeseen and unpredictable manner and have been referred to by economists and sociologists as "black swans."

While not an exhaustive list, there are four potential "black swans" that could materially change our assessment of overall homeland security risk and priorities over the next five years:

- Rapid adoption of technology-driven changes to manufacturing processes, such as three-dimensional printing, fundamentally altering the importance of transnational flows of information in relation to the transnational flows of goods;
- A country unexpectedly becoming a failed state, leading to consequences such as loss of control over sensitive technologies (e.g., chemical, biological, radiological, and nuclear materials) or loss of general border integrity;
- A substantial increase in sophistication of hostile non-state actors, such as a violent extremist group gaining the ability to launch a campaign of well-coordinated and highly organized attacks, conducted by interconnected but autonomous groups or individuals within the United States; and
- Abrupt impacts of climate change, such as drastic alterations in U.S. weather patterns and growing seasons or rapid opening of the Arctic.

These changes are not planned for or expected in the next five years, yet if they were to happen, they would fundamentally alter the homeland security strategic environment described here.

4. GUIDING PRINCIPLES

The following principles form the basis for the specific priorities and areas of emphasis the Department, together with our partners and stakeholders, will adopt in addressing the strategic challenges discussed in the Strategic Environment section.

THE CORNERSTONE OF HOMELAND SECURITY IS PREVENTING TERRORISM, BUT HOMELAND SECURITY MUST BE MULTI-THREAT AND ALL-HAZARD

Events of the past 12 years demonstrate that we must consider the full range of threats and hazards facing the Nation when setting homeland security strategy and priorities. The Department is a multi-mission, multi-function agency, covering long-standing functions such as civil defense, emergency response, customs, border control, law enforcement, and immigration. As one agency, we are able to improve efficiency by identifying the common characteristics among the wide variety of threats and hazards we face and by identifying common ways to address them.

U.S. Customs and Border Protection

HOMELAND SECURITY SUPPORTS ECONOMIC SECURITY


U.S. Customs and Border Protection

As noted previously, lawful trade and travel are expanding rapidly, with great benefit to U.S. prosperity and economic security. DHS and our partners are on the front lines overseas and at our air, land, and sea ports of entry, expediting these flows of people and goods and ensuring their security. As such, and as recognized in successive national security strategies, homeland security is inseparable from economic security.

HOMELAND SECURITY REQUIRES A NETWORKED COMMUNITY

The Department works with other units of government, forms public-private partnerships, and enlists the help of the American people because the homeland security missions cannot be met by one entity alone. Our ability to effectively network ourselves through robust partnerships and operational integration—within DHS, across homeland security partners and stakeholders, and with our international partners—increasingly means the difference between mission success and failure. This is all the more important given the range of adversaries the Nation confronts, many of whom are increasingly networked themselves. The homeland security community can be more flexible, adaptable, and efficient in addressing diverse challenges if it acts as an integrated, mutually supporting network. Our shared efforts will promote security and risk reduction approaches that are responsive to the needs of our partners.

HOMELAND SECURITY RELIES UPON THE USE OF MARKET-DRIVEN SOLUTIONS AND INNOVATION

We must partner with industry in research and development efforts to reduce known vulnerabilities that have proven difficult or expensive to address—particularly in cyberspace

and critical infrastructure—and to mitigate consequences of disruption or intrusion. The Department will continue to adopt market-based solutions and coordinate closely with industry to identify new areas of application for security products and services and will help ensure the public and private sectors have awareness and access to the latest technologies and protections.

HOMELAND SECURITY UPHOLDS PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES

Privacy, civil rights, and civil liberties issues are interwoven into our approach to homeland security across all missions and can arise in any homeland security activity, sometimes in unforeseen ways. In addressing new risks or adopting new and integrated approaches, we must identify early on any risk of infringement of these core values and rights and address that risk accordingly. When issues are identified and resolved earlier, it helps ensure that all eligible persons and communities can participate in homeland security programs and benefit from our operations.

HOMELAND SECURITY IS NATIONAL RISK MANAGEMENT

Absolute security against the threats and hazards we face is neither fiscally nor operationally possible. Instead, homeland security is about managing risk. As described previously, the second quadrennial review makes recommendations for strategic shifts and renewed areas of emphasis for our national homeland security strategy and priorities. National risk management emphasizes focusing on those actions and interventions that reduce the greatest amount of strategic risk to the Nation.

U.S. Coast Guard

U.S. Secret Service

5. STRATEGIC PRIORITIES

DHS will adopt the following strategic shifts or renewed emphases over the next four years to best address the changing strategic environment. These priorities emerge out of a number of cross-cutting Quadrennial Homeland Security Review studies, which lead to shifts and renewed areas of emphasis across the homeland security missions. The tables at the beginning of each subsection below show which missions are impacted by these shifts and renewed areas of emphasis.

SECURING AGAINST THE EVOLVING TERRORISM THREAT

OVERVIEW

As described in the first quadrennial review, homeland security is a concerted national effort that involves actions by a widely distributed and diverse group of federal, state, local, tribal, territorial, non-governmental, and private sector partners as well as individuals, families, and communities. The evolution of the terrorist threat demands a well-informed, highly agile, and well-networked group of partners and stakeholders to anticipate, detect,

target, and disrupt threats that challenge national security, economic prosperity, and public safety. To improve overall unity of effort, we will work with our partners to identify, investigate, and interdict legitimate threats as early as possible; expand risk-based security; focus on countering violent extremism and helping to prevent complex mass casualty attacks; reduce vulnerabilities by denying resources and targets; and uncover patterns and faint signals through enhanced data integration and analysis.

Table 1: The following table shows how priority areas of emphasis for securing against the evolving terrorism threat map to the homeland security missions.

Securing Against the Evolving Terrorism Threat					
Priority Area of Emphasis	Prevent Terrorism and Enhance Security	Secure and Manage Our Borders	Enforce and Administer Our Immigration Laws	Safeguard and Secure Cyberspace	Strengthen National Preparedness and Resilience
Identify, Investigate, and Interdict Threats as Early as Possible	✓	✓		✓	
Shrink the Haystack: Expand Risk-Based Security	✓	✓			
Focus on Countering Violent Extremism and Helping to Prevent Complex Mass Casualty Attacks	✓				✓
Reduce Vulnerabilities: Deny Resources, Deny Targets	✓			✓	✓
Uncover Patterns and Faint Signals: Enhance Data Integration and Analysis	✓	✓		✓	

STRATEGIC APPROACH

IDENTIFY, INVESTIGATE, AND INTERDICT THREATS AS EARLY AS POSSIBLE

Given the current and emerging potential threats, a primary concern is that violent extremists can move undetected across porous borders within conflict zones—such as today's conflicts in Syria, Somalia, and Yemen—where they can train in terrorist tactics, skills, and weapons. At the same time, several countries are on the edge of state failure and are unable to secure their own borders, prevent the illicit movement of people and goods, and collect customs revenues to support governance.

To address these pathway vulnerabilities and enhance the safe and secure movement of people and goods, DHS, in coordination with the Departments of State, Defense, Justice, and other partners, will prioritize support to foreign partners to increase their border

management, customs integrity, and law enforcement capabilities and capacities. In addition, we will continue to expand pre-departure screening and enhance transportation security operations among willing partners to mitigate risks from overseas. To keep dangerous people and goods off aircraft bound for the United States, it is critical that we use information received in advance to screen abroad based on risk, rather than waiting for arrival in the United States.

U.S. Customs and Border Protection/Anthony Bucci

Shrink the Haystack: Expand Risk-Based Security

The decentralized nature of today's threat demands that we continue to move away from one-size-fits-all security approaches and toward risk-informed, intelligence-driven approaches. For this reason, DHS will expand efforts to identify low-risk travelers and cargo to focus security resources on those we know less about or those identified as higher risk. Trusted traveler and shipper programs such as Global Entry, TSA Pre✓™, and the Customs-Trade Partnership Against Terrorism advance these objectives and show that effective security and the expedited flow of goods and people can be achieved together. We will continue to identify lower-risk travelers by a number of means, including using background checks and recognizing foreign partner trusted traveler and shipper programs.

More broadly, risk-informed decision making is becoming the norm among homeland security partners and stakeholders. For example, unmanned aerial surveillance systems

used in securing and managing our borders are deployed based on risk, allowing strategic aerial surveillance of wide areas and better detection and interdiction of illicit flows. Risk and intelligence information also drive the deployments of our security teams who secure mass transit and trains, waterways, and other modes of transportation. In addition, we are continuously improving our approach to addressing insider threats, including how we vet, credential, and educate individuals with access to critical or sensitive homeland security facilities. Finally, state, local, tribal, and territorial governments identify risks and decide how to address their greatest risks through the completion of the Threat and Hazard Identification and Risk Assessment process.

Focus on Countering Violent Extremism and Helping to Prevent Complex Mass Casualty Attacks

Our approach to countering violent extremism in the United States—guided by the White House Strategy, Empowering Local Partners to Prevent Violent Extremism in the United States (2011)—applies to all forms of violent extremism regardless of ideology and does not focus on protected First Amendment activities. The Boston Marathon bombing, the arrests of individuals attempting to travel to conflict zones in support of violent extremist groups, and the shooting at a Sikh temple in Wisconsin in 2012 illustrate the persistent threat in the United States from groups and individuals inspired by a range of religious, political, or other ideological beliefs.

Our efforts to countering violent extremism emphasize the strength of local communities and the premise that well-informed and well-equipped families, communities, and local institutions represent the best defense against violent extremism. We prioritize disrupting and deterring recruitment or individual radicalization to violence by supporting community-based problem solving and local law enforcement programs. Such programs include information-driven, community-oriented policing efforts that for decades have proven effective in preventing other types of violent crime. In addition, our communities and youth must be made aware of the increasing dangers of online radicalization to violence. DHS will continue to work with our partners to share information with frontline law enforcement partners, communities, families, and the private sector about how violent extremists are using the Internet and how to protect themselves and their communities.

Further, substantial research and analysis are helping to identify and illustrate the tactics, behaviors, and indicators potentially associated with violent extremism as well as factors that may influence violent extremism. Based on this analysis, DHS jointly develops with federal, state, local, tribal, and territorial partners training for frontline law enforcement officers on behaviors that may be indicative of violent extremist activity.

Similar research into non-ideologically motivated violence, such as the devastating shootings in Newtown, Connecticut and Aurora, Colorado, provides further insight into pre-incident behavioral indicators associated with mass violence. These insights enhance our efforts to equip partners with the most effective tools to identify and mitigate a range of violent attacks, including briefings to community stakeholders on pre-incident behavioral indicators associated with mass casualty shootings and on community-based multidisciplinary intervention techniques.

Transportation Security Administration

Reduce Vulnerabilities: Deny Resources, Deny Targets

Violent extremists will seek to attack symbolic venues, transportation pathways, mass gatherings, and critical infrastructure. To enhance our ability to protect these "soft" targets, we must adopt approaches that are intelligence-led, analytically driven, and pursued in close cooperation between federal, state, local, tribal, territorial, and private sector partners as well as with the public. The DHS "Security Strategy for Mass Transit and Passenger Rail" illustrates how we have employed this approach to improve the security and resilience of critical surface transportation infrastructure.

Further, to counter the threat posed by improvised explosive devices and small arms attacks, we will work with our partners to expand and promote activities such as suspicious activity reporting and private sector security measures. Internationally, we will continue to support multilateral efforts, such as the World Customs Organization's Program Global

Shield, which shares information on the global movement of precursor chemicals used to manufacture improvised explosive devices and raise security standards. We regulate high-risk chemical facilities to reduce their vulnerabilities. We will also continue researching next-generation technology solutions to stay ahead of advances in wireless technology, given the use of wireless technology in improvised explosive device detonation and control mechanisms.

Across all of these efforts, DHS, working with our government and private sector partners, will be proactive in discouraging terrorist plots. We will place an increased emphasis on deterrence, including enhancing efforts to publicly communicate tailored descriptions of homeland security capabilities to influence the perceptions, risk calculations, and behaviors of adversaries.

Uncover Patterns and Faint Signals: Enhance Data Integration and Analysis

DHS and our partners must continually enhance situational awareness. To that end, DHS is committed to integrating its data sources, including by consolidating or federating screening and vetting operations. Perhaps most importantly, we must continually improve our ability to make sense of vast amounts of intelligence and other information—the so-called "big data" challenge—while rigorously protecting the privacy and civil liberties of Americans. For homeland security, the adoption of big data management solutions will aid investigators and analysts in identifying relationships that were previously difficult to discern. This type of pattern and network analysis allows DHS and our partners to identify harmful activity as early as possible and to take steps to intervene or otherwise stop harmful events from occurring.

One critical data source is Suspicious Activity Reporting from state, local, tribal, territorial, and private sector partners as part of the Nationwide Suspicious Activity Reporting Initiative. Another source is the "If You See Something, Say Something™" campaign, which encourages citizens to report suspicious activity to the proper law enforcement authorities. These efforts ensure the protection of privacy, civil rights, and civil liberties, while also ensuring information is quickly reviewed by the Federal Bureau of Investigation's (FBI's) Joint Terrorism Task Forces for possible investigation and shared with other fusion centers and FBI Field Intelligence Groups for additional analysis. Through the National Network of Fusion Centers and other mechanisms, DHS will prioritize the development and timely distribution of locally or regionally oriented joint products. These joint products, produced collaboratively by federal, state, local, tribal, and territorial partners, support operations and provide detailed insight on emerging community or region-specific threats.

SAFEGUARD AND SECURE CYBERSPACE

OVERVIEW

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes is now being perpetrated through cyberspace. This includes the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud, intellectual property violations, and other crimes, all of which have substantial human and economic consequences.

Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks.

Of growing concern is the cyber threat to critical infrastructure. This infrastructure provides essential services such as energy, telecommunications, water, transportation, and financial services and is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend.

In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission. The Department works to achieve this mission by collaborating with government and private sector partners to strengthen cybersecurity protections, investigate those that engage in cybercrime, and take full advantage of innovations in machine intelligence and communications that work at the speed of cyberspace. The Department will promote security and risk reduction approaches that are driven by the needs of our stakeholders, are cost effective, and do not negatively impact operational performance. When incidents do occur, DHS will continue to provide assistance to potentially impacted entities, analyze the potential impact across critical infrastructure, investigate those responsible in conjunction with other law enforcement partners, and coordinate the national response to significant cyber incidents.

The Department works in close coordination with other agencies with complementary cyber missions, as well as private sector and other nonfederal owners and operators of critical infrastructure, to ensure greater unity of effort and a whole-of-nation response to cyber incidents. DHS coordinates the national protection against, mitigation of, and recovery from cyber incidents; works to prevent and protect against risks to critical infrastructure; disseminates domestic cyber threat and vulnerability analysis across critical infrastructure sectors; secures federal civilian systems; investigates, attributes, and disrupts cybercrimes under its jurisdiction; and coordinates federal government responses to significant incidents, whether cyber or physical, affecting critical infrastructure. The Department of Justice (DOJ) prosecutes cybercrimes; investigates, attributes, and disrupts cybercrimes under its jurisdiction; leads domestic national security operations regarding cyber threats, including disrupting foreign intelligence, terrorist, or other national security threats; and conducts domestic collection, analysis, and dissemination of cyber threat information. The Department of Defense (DOD) defends the nation from attack, secures national security and military systems, and gathers foreign cyber threat information. Working together, we work to foster a secure and resilient cyberspace that protects privacy and other civil liberties by design; supports innovation and economic growth; helps maintain national

security and public health and safety; and supports legitimate commerce.

Table 2: The following table shows how priority areas of emphasis for safeguarding and securing cyberspace map to the homeland security missions.

Safeguard and Secure Cyberspace					
Priority Area of Emphasis	Prevent Terrorism and Enhance Security	Secure and Manage Our Borders	Enforce and Administer Our Immigration Laws	Safeguard and Secure Cyberspace	Strengthen National Preparedness and Resilience
Strengthen the Security and Resilience of Critical Infrastructure	✓	✓		✓	✓
Secure the Federal Civilian Government Information Technology Enterprise	✓			✓	✓
Advance Law Enforcement, Incident Response, and Reporting Capabilities	✓	✓		✓	
Strengthen the Ecosystem				✓	✓

STRATEGIC APPROACH

STRENGTHEN THE SECURITY AND RESILIENCE OF CRITICAL INFRASTRUCTURE

The Department employs a risk-informed approach to safeguarding critical infrastructure in cyberspace. We do this in the context of the overall risk to critical infrastructure under an all-hazards approach. In reducing cyber and physical risks, we will emphasize protections for privacy and civil liberties, transparent and accessible security processes, and domestic and international partnerships that further collective action. The Department will continue to coordinate with sector specific agencies, other federal agencies, and private sector partners to share information on and analysis of cyber threats and vulnerabilities and to understand more fully the interdependency of infrastructure systems nationwide. This collective approach to prevent, protect against, mitigate, respond to, investigate, and recover from cyber incidents prioritizes understanding and meeting the needs of our partners. This approach is also consistent with the growing recognition among corporate leaders that cyber and physical security are interdependent and must be core aspects of their risk management strategies.

The Department will evolve towards dynamic real-time situational awareness capabilities, like “weather maps” for cyberspace. These situational awareness capabilities will support cyber infrastructure that—much like the human immune system—will be smart enough to

detect, adapt to, and defend against new threats with sufficient resilience to continue operating while under attack. Further, this situational awareness will support a common operating picture for cybersecurity that will provide cyber event information, and serve as a resource for all of government and industry. Providing information to machines at machine speed to block threats in milliseconds instead of the hours or days required today will enable better cyber incident response and mitigation.

We must draw on the Nation's full range of expertise and resources—from all levels of government, the private sector, members of the public, and international partners—to secure critical infrastructure from cyber threats. Executive Order 13636, Improving Critical Infrastructure Cybersecurity (2013), and Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience" (2013), establish a risk-informed approach and a framework for critical infrastructure security and resilience collaboration. They also include the Framework for Improving Critical Infrastructure Cybersecurity, which provides an industry-driven risk management approach to strengthen cybersecurity across all critical infrastructure sectors. We will continue to work with our partners to foster development of secure cyber products and services and to encourage the adoption of leading cybersecurity best practices, including the Cybersecurity Framework and the National Infrastructure Protection Plan. The cyber ecosystem will also be strengthened as aging and failing infrastructure is replaced by infrastructure with more secure and resilient design built in.

Secure the Federal Civilian Government Information Technology Enterprise

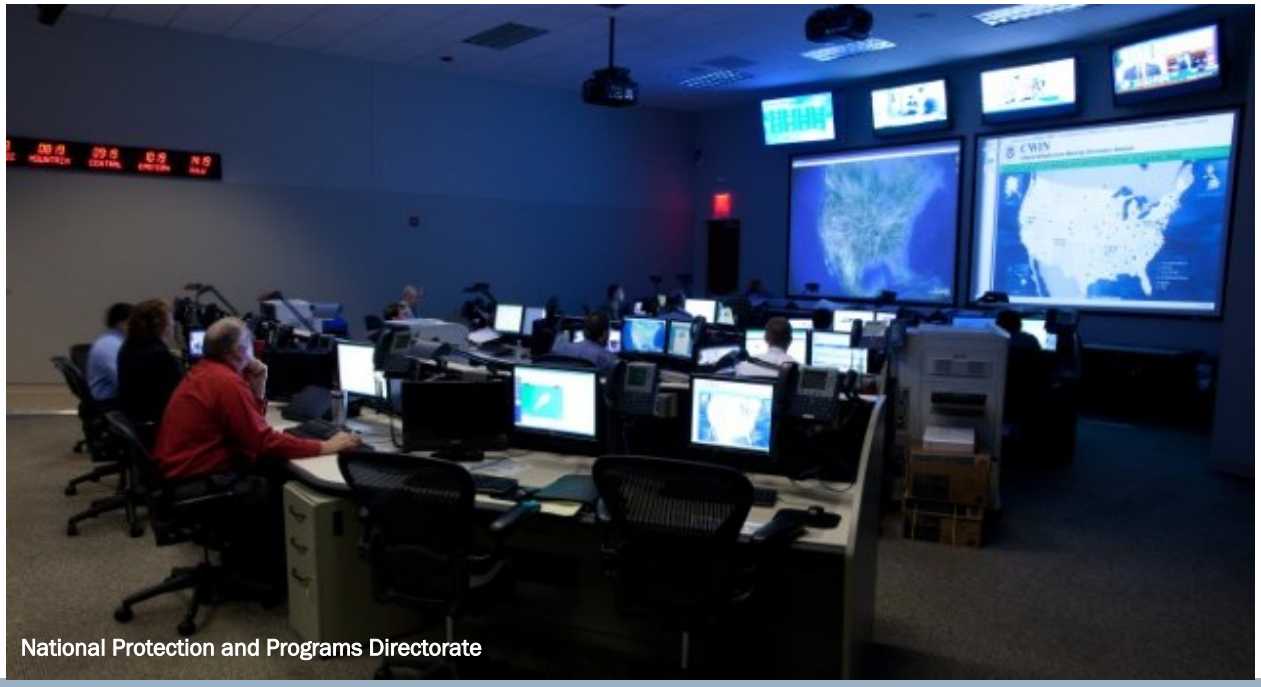
The Federal Government must seek to serve as a model to other organizations in our work to secure our networks with the latest tools, information, and protections. The Department

will continue to work with each federal civilian department and agency to promote the adoption of common policies and best practices that are risk-based and able to effectively respond to the pace of ever changing threats. As systems are protected, alerts can be issued at machine speed when events are detected to help protect networks across the government information technology enterprise and the private sector. This enterprise approach will help transform the way federal civilian agencies manage cyber networks through strategically sourced tools and services that enhance the speed and cost-effectiveness of federal cybersecurity procurements and allow consistent application of best practices.

The Department works with other federal agencies and the private sector to identify emerging requirements and to support research and development projects that keep pace with ever changing threats and vulnerabilities. The Department will target techniques and capabilities that can be deployed over the next decade with the potential to redefine the state of cybersecurity against current and future threats by working to make the innovations from research and development widely available across the public and private sectors.

Advance Law Enforcement, Incident Response, and Reporting Capabilities

Complementary cybersecurity and law enforcement capabilities are critical to safeguarding and securing cyberspace. Law enforcement performs an essential role in achieving our Nation's cybersecurity objectives by investigating a wide range of cybercrimes, from theft

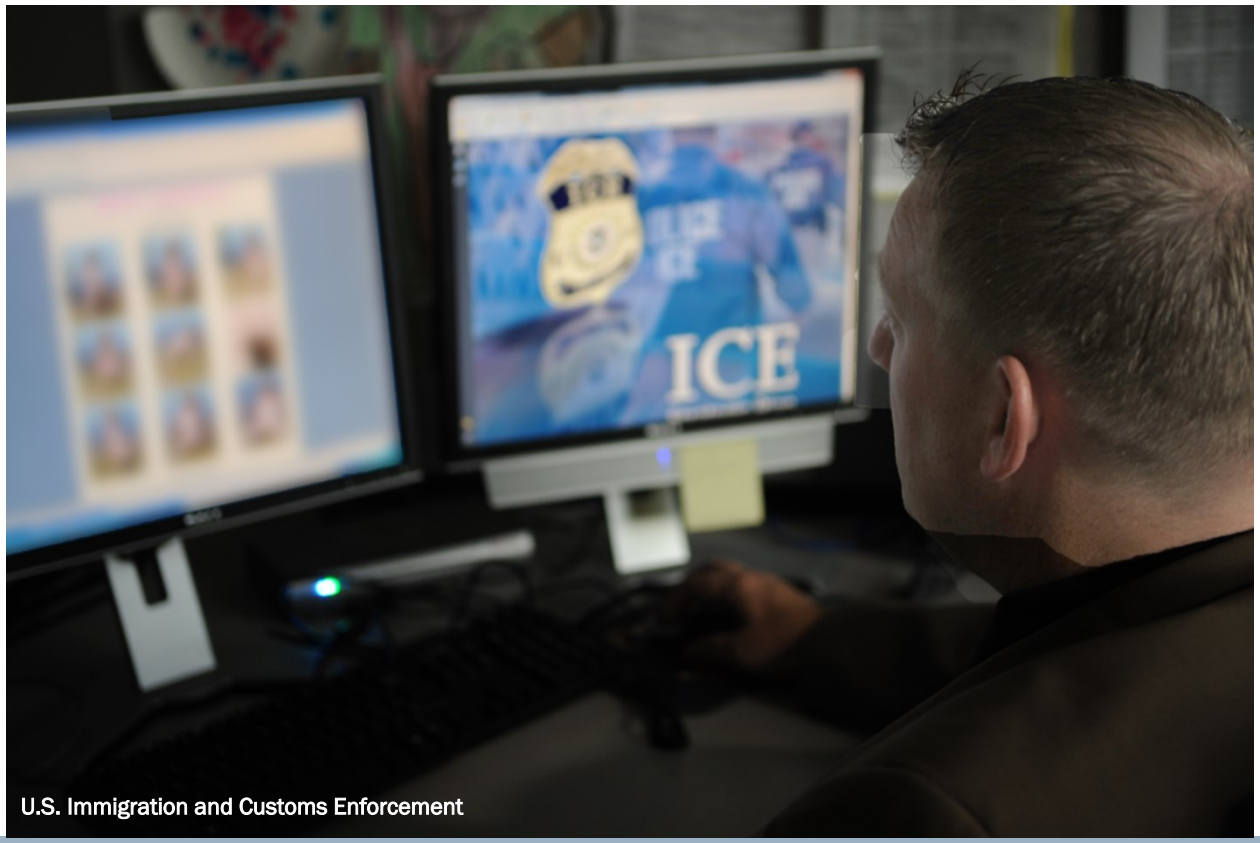


National Protection and Programs Directorate

and fraud to child exploitation, and apprehending and prosecuting those responsible. Cybersecurity and infrastructure protection experts provide assistance to owners and operators of critical systems by responding to incidents and restoring services, and analyzing potentially broader cyber or physical impacts to critical infrastructure.

Law enforcement entities; network security experts; the Intelligence Community; state, local, tribal, and territorial partners; critical infrastructure owners and operators; and others in the private sector, through coordination and planning, will increase the quantity and impact of cybercrime investigations and network security efforts. Together we will continue to identify and respond to malicious actors and continue to grow our national cyber incident response and information sharing capacity. We will also continue sharing lessons learned from these efforts to help prevent the same incidents from happening elsewhere, while protecting victims' privacy and ongoing investigations.

Criminal investigators and network security experts with deep understanding of the technologies malicious actors are using and the specific vulnerabilities they are targeting work to effectively respond to and investigate cyber incidents. DHS will work with other federal agencies to conduct high-impact criminal investigations to disrupt and defeat cyber criminals, prioritize the recruitment and training of technical experts, develop standardized



U.S. Immigration and Customs Enforcement

methods, and broadly share cyber response best practices and tools. The Secretary of Homeland Security will coordinate federal government responses to significant cyber or physical incidents affecting critical infrastructure consistent with statutory authorities.

DHS will continue to work with all partners, government and private sector, to ensure that information provided to any federal agency is appropriately shared. This strengthens the use of established private sector and academia relationships with government partners and leverages these relationships when they are needed most.

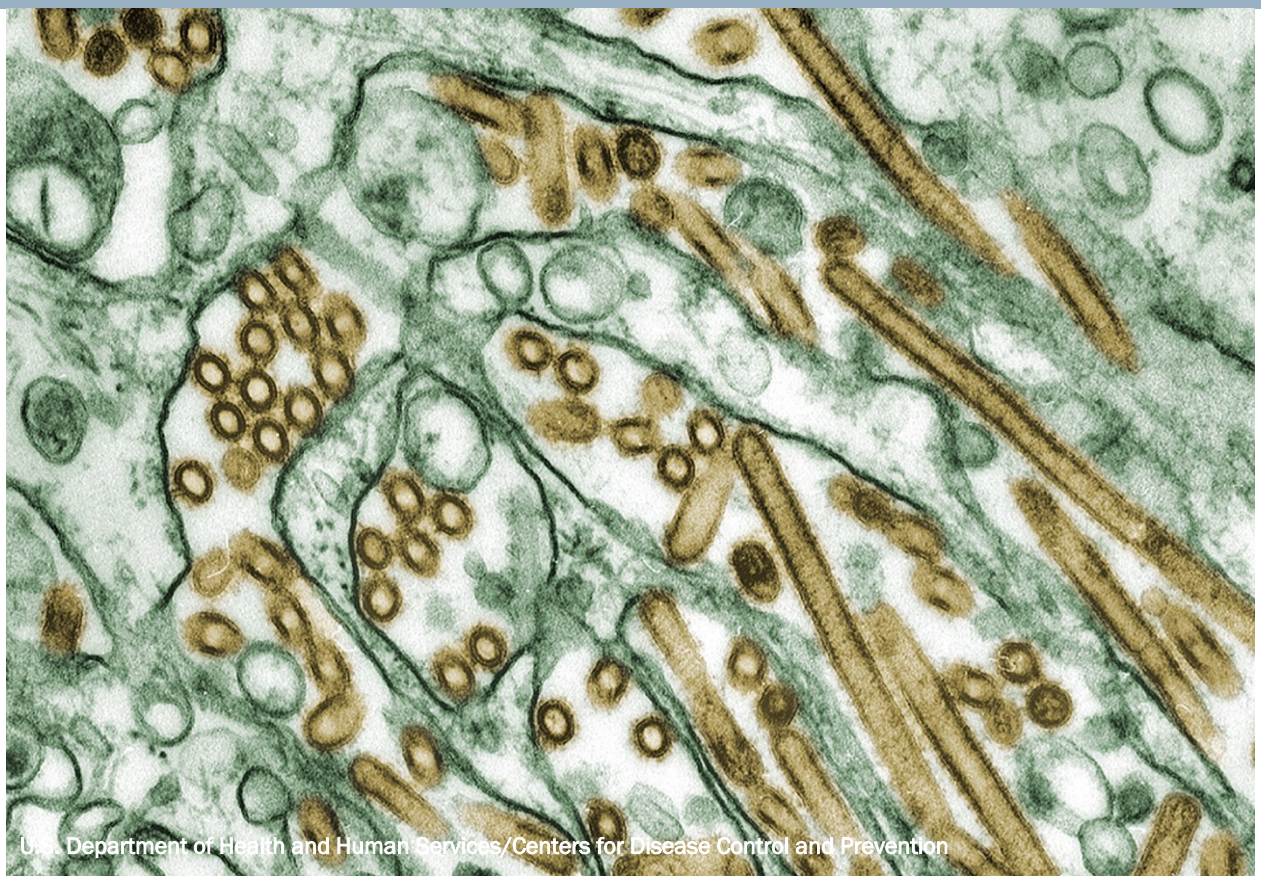
Strengthen the Ecosystem

Cybersecurity is a shared responsibility in which each of us has a role. Ensuring a healthy cyber ecosystem will require collaborative communities, innovative and agile security solutions, standardized and consistent processes to share information and best practices, sound policies and plans, and development of a skilled workforce to ensure those policies and plans are implemented as intended.

DHS will work with our public and private sector partners to help develop innovative security technologies and services that strengthen analytic, response, and remediation capabilities; prevent incidents before they occur; and minimize the consequences of those incidents that occur. To do this, we will develop a strong team of cybersecurity professionals to design, build, and operate robust technology to reduce exploitable weaknesses.

The cyber ecosystem also needs self-mitigating and self-healing systems to address threats at machine speed. Consistent standards are needed for sharing information across organizations and developing interoperable technologies that enable detection of and resilience against threats and hazards. DHS will work with our public and private sector partners and across the science and policy communities to identify promising technologies, policies, and standards that enable trust-based, privacy-centric, automated sharing of cybersecurity information to limit the spread of incidents and minimize consequences.

DHS will continue to advance existing public education programs and promote cybersecurity strategies and awareness campaigns that engage the American people in keeping themselves—and the Nation—secure online. Internationally, DHS will work with the Department of State and other partners to build global networks to share vital cybersecurity information and help enable international response to cyber incidents. DHS, with our partners, will also work to harmonize international laws to effectively combat transnational cybercrime.


U.S. Department of Health and Human Services/Centers for Disease Control and Prevention

A HOMELAND SECURITY STRATEGY FOR COUNTERING BIOLOGICAL THREATS AND HAZARDS

OVERVIEW

Biological threats and hazards—ranging from bioterrorism to naturally occurring pandemics—are a top homeland security risk. They have the potential to significantly impact the health and well-being of the Nation's people, animals, and plants. These threats and hazards may also be highly disruptive to our efforts to pursue the homeland security missions. They may overwhelm our state, local, tribal, and territorial partners and may threaten our ability to maintain essential functions and carry out day-to-day operations.

We generally expect the risk of biological threats and hazards to increase over time, given trends such as increasing trade and travel and the growing accessibility of biotechnology. In the long term, unexpected or dramatic shifts in key areas, including biotechnology, global biosurveillance capability and response capacity, and disease prevention and treatment, may cause the risk to change. As such, these key areas present important opportunities

for managing biological risk into the future, risk that must be addressed in a sustainable way.

The Department performed an in-depth examination of the risk associated with biological threats and hazards in the homeland security mission space. From this analysis, we identified four biological threats and hazards—referred to here as "priority biological threats and hazards"—that pose particularly high risk to the Nation and that an effective homeland security strategy for managing biological risk must address:

- Pathogens posing particular bioterrorism concerns (e.g., anthrax, plague, and smallpox), including enhanced and advanced pathogens;
- Emerging infectious diseases that are highly disruptive (e.g., viruses that could cause human pandemic);
- Animal diseases and plant pathogens or pests that are highly disruptive (e.g., foot-and-mouth disease); and
- Bioterrorist contamination of the food supply chain and water systems.

Incidents involving these priority biological threats and hazards are often difficult to prevent and can cause severe consequences, including mass illnesses, fatalities, and widespread

Table 3: The following table shows how priority areas of emphasis for the homeland security strategy for countering biological threats and hazards map to the homeland security missions.

A Homeland Security Strategy for Countering Biological Threats and Hazards					
Priority Area of Emphasis	Prevent Terrorism and Enhance Security	Secure and Manage Our Borders	Enforce and Administer Our Immigration Laws	Safeguard and Secure Cyberspace	Strengthen National Preparedness and Resilience
Prevent Biological Incidents from Occurring, When Possible	✓	✓			
Improve Risk-Informed Decision Making	✓	✓		✓	✓
Identify Biological Incidents Early	✓	✓			✓
Improve Confidence to Act	✓	✓			✓
Respond and Recover from Biological Incidents					✓
Maintain Vital Services and Functions During and After Biological Incidents	✓	✓	✓	✓	✓

disruption of our society and economy. These types of threats and hazards may evade early detection; may spread quickly across regions, countries, and continents; and may persist for long periods of time. An incident involving a priority biological threat or hazard is referred to here as a "priority biological incident."

A HOMELAND SECURITY STRATEGY FOR MANAGING BIOLOGICAL RISK

Numerous departments and agencies at the federal, state, local, tribal, and territorial levels, as well as the private sector, contribute to the national effort to address these biological threats and hazards. The Department of Health and Human Services (HHS) is the principal federal agency for protecting the Nation's health and providing essential human services. HHS leads the Nation in preparing for, responding to, and recovering from the adverse health effects of public health incidents and develops the National Health Security Strategy. The Departments of Agriculture, Defense, Justice, the Environmental Protection Agency, and various centers within the Office of the Director of National Intelligence also perform central roles. The FBI leads investigations when an act of bioterrorism is suspected, and is the lead law enforcement agency for investigating violations of the biological warfare and terrorism statute. This strategy focuses on those activities and responsibilities assigned to DHS through statute or presidential directive, including information sharing and analysis; threat and risk awareness; biosurveillance integration and detection; technical forensic analysis to support attribution; preparedness coordination; incident management, response, and continuity planning; critical infrastructure security and resilience coordination; and border management. While these varied responsibilities have not changed significantly, this strategy integrates and harmonizes these activities in a manner that best addresses priority biological threats and hazards.

We cannot prevent all biological incidents from occurring, nor can we simply rely on our ability to respond and recover to adequately minimize the risk of catastrophic biological incidents. Therefore, **our strategy is to prevent the occurrence of priority biological incidents, where possible, but, when unable to prevent, to stop priority biological incidents from overwhelming the capacity of our state, local, tribal, and territorial partners to manage and respond.** To do this, we will work to prevent the release of priority biological threat agents, either by an adversary or by accident. We will also prevent, where possible, priority biological threats and hazards from crossing the border into the United States. Understanding that we cannot prevent all biological incidents from occurring, DHS, in close collaboration with HHS, the U.S. Department of Agriculture, and DOJ, will enhance situational awareness and biosurveillance capabilities to recognize faint signals of impending or evolving priority biological incidents, so we can respond to stop escalation

and thus limit potential consequences.

We will continue to help our state, local, tribal, and territorial partners develop the capabilities necessary to manage and respond to priority biological incidents with some federal support, at levels of capacity sufficient to address a "mid-range" incident (see Figure 3). Biological incidents with a "mid-range" level of risk are those that stress state, local, tribal, and territorial capacity without overwhelming it, typically also involving federal assistance. Assuming that state, local, tribal, and territorial partners can directly manage these "mid-range" incidents with some federal assistance, DHS and our federal partners will continue to invest in and develop capabilities as appropriate to support and reinforce these state, local, tribal, and territorial capabilities. Understanding and addressing the state, local, tribal, and territorial regional variability to manage and respond to a priority biological incident will allow us to optimize capability development in accordance with

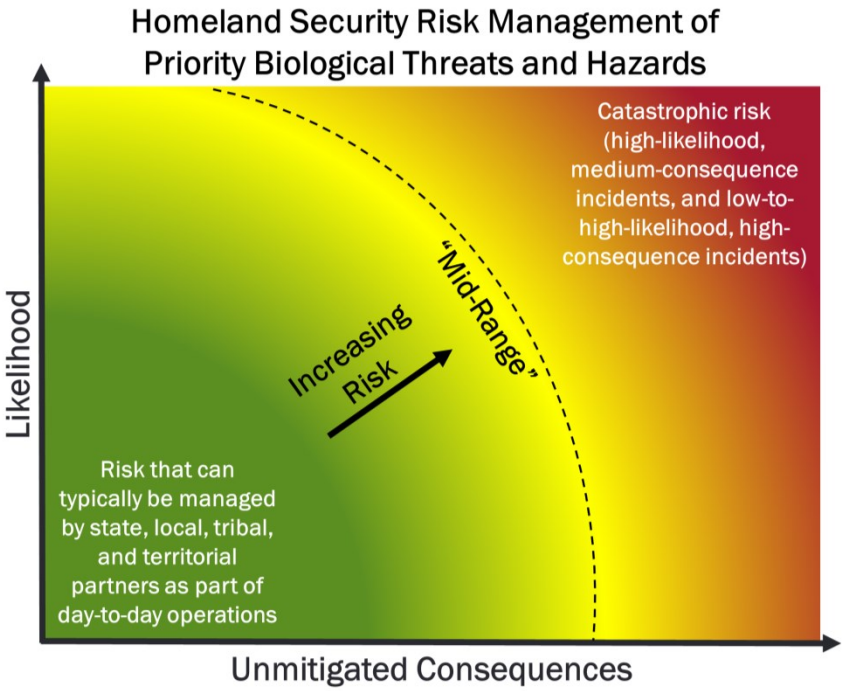


Figure 3: Priority biological incidents with a "mid-range" level of risk, accounting for both likelihood and unmitigated consequences, fall above those incidents that are effectively managed by state, local, tribal, and territorial partners as a part of day-to-day operations but below catastrophic high-risk incidents, including high-likelihood, medium-consequence incidents, and low-to-high-likelihood, high-consequence incidents. The levels of likelihood and consequences that characterize a "mid-range" incident vary by priority biological threat and hazard.

Presidential Policy Directive 8, "National Preparedness" (2011). This strategy is balanced and comprehensive across the different priority biological threats and hazards and across the possible actions the Department can take to reduce likelihood, mitigate vulnerabilities, and reduce consequences.

The Department will focus its resourcing efforts on capabilities necessary to prevent or stop the escalation of priority biological incidents that have the potential to reach or exceed "mid-range" risk, and on supporting response capabilities and capacities for "mid-range" priority biological incidents. What constitutes "mid-range" may vary based on the unique characteristics of different regions, jurisdictions, and localities. While implementing the strategy will result in adjustments to our long-term strategic capability and capacity development, DHS and our partners will continue day-to-day operations using current capabilities to address immediate threats and hazards. **Contingency planning efforts will continue to account for all kinds of biological incidents relevant to homeland security**, including low-likelihood, high-consequence biological incidents that exceed "mid-range" risk.


Science and Technology Directorate

To execute this strategy, we will collaborate with our partners to accomplish the following six goals that involve refinements to our collective homeland security policies, capabilities, and capacities:

- **Prevent or deter the release or introduction, whether intentional or inadvertent, of priority biological threats and hazards in the United States.** To accomplish this goal, we will engage in activities to reduce the potential for priority biological threats and hazards to be misused or introduced into the United States, whether intentionally or inadvertently. These activities include efforts to identify, target, and interdict priority

biological threats and hazards crossing the border into the United States and supporting efforts to ensure an appropriate culture of biosafety and biosecurity in laboratory operations. While preventative in nature, these activities, along with others such as microbial forensics, also contribute to a deterrence regime that will serve to reduce the potential for deliberate or accidental release or introduction of priority biological threats and hazards.

- **Improve risk-informed decision making by ensuring decision makers at all levels across DHS and our partners are appropriately informed by a common understanding of the risk associated with priority biological threats and hazards (e.g., potential likelihood and consequences such as illnesses/injuries, fatalities, economic impacts, and disruption to society).** To accomplish this goal, DHS will work with partners to develop a common, authoritative understanding of biological risk in the homeland security mission (including potential likelihood, and consequences such as illnesses/injuries, fatalities, economic impacts, and disruption to society). DHS will also work with partners to enhance our efforts to anticipate emerging biological threats and hazards, and provide timely, accurate, and actionable information and analysis concerning these priority biological threats and hazards (at the classified/unclassified level as required).

- **Detect and confirm priority biological incidents sufficiently early to ensure incidents do not exceed state, local, tribal, and territorial capacity to manage and respond.** To accomplish this goal, DHS, in close collaboration with our partners, will refine and further integrate this detection and confirmation capability with federal, state, local, tribal, and territorial partners to achieve sufficiently accurate, timely, and trusted detection and confirmation across priority biological threats and hazards. DHS will pursue additional information sharing, integration, and analysis efforts with partners, and will reexamine information sharing policies. DHS will work with partners to pursue technological advances (e.g., information sharing and sensing/ diagnostics capabilities) and translate them into deployed capabilities as they become operationally feasible and affordable.

- **Improve the confidence of our partners to act by ensuring that decision makers at all levels of government have timely, relevant, accurate, and trusted information that supports decision making.** Trusted information that gives decision makers confidence to act includes threat indications and warnings, detection tools, impact assessments, attack or disease emergence notifications, test sensitivity/specificity, and other elements. Early notification maximizes the time available for decision

makers to effectively respond. Accurately confirming and characterizing an incident and rapidly disseminating appropriate information to decision makers at all levels maximizes decision making confidence. Tabletop exercises help decision makers understand how to use information and make rapid decisions during a crisis.

- **Enable effective response to and recovery from priority biological incidents.** DHS and our partners should aim to have the collective capabilities and capacities to address what might be expected from a "mid-range" priority biological incident (see Figure 3) that would exceed the time phase, geographic scope, and casualty levels of most other threats and hazards. To accomplish this goal, we will work to ensure state, local, tribal, and territorial governments and critical infrastructure owners and operators achieve sufficient capabilities and capacities to provide lifesaving medical support and services; stabilize food, agriculture, and other critical sector functions; and minimize economic loss.

- **Maintain mission-essential functions across government and critical infrastructure services and functions during and after incidents involving priority biological threats or hazards.** To accomplish this goal, we will emphasize protection and maintenance of critical infrastructure operations that provide vital services and whose loss of functionality could negatively impact national security, economic vitality, and public health and safety in the face of a biological event. Such emphasis must form part of our risk-informed, all-hazards approach to security and resilience of critical infrastructure so that people are protected and critical facilities continue to operate. We will also encourage collaborative planning and the development and adoption of protocols and standards for protecting critical infrastructure from biological attacks. DHS will maintain our mission-essential functions and protect Department personnel against priority biological threats and hazards. DHS will provide guidance to other Federal departments and agencies and encourage our other partners to take appropriate actions to maintain mission-essential functions in the event of a priority biological incident.

BUILDING FUTURE CAPABILITIES TO ACHIEVE SUCCESS

The success of this strategy relies upon DHS and our partners enhancing coordination efforts and improving the confidence to act. Success also relies on increasing situational awareness by further integrating and coordinating the collection, analysis, and sharing of information, as appropriate, to proactively address priority biological threats and hazards. Before making any substantial new investments, DHS will thoughtfully examine the way our current efforts are being executed in order to identify untapped efficiencies.

U.S. Customs and Border Protection

A RISK SEGMENTATION APPROACH TO SECURING AND MANAGING FLOWS OF PEOPLE AND GOODS

OVERVIEW

DHS and our partners secure and manage the flows of people and goods to enable prosperity and minimize risk. We ensure transit via legal pathways; identify and remove people and goods attempting to travel illegally; and ensure the safety and integrity of these flows of people and goods by safeguarding the conveyances, nodes, and pathways that make up the travel and trade system. This includes our responsibilities in border security, trade law compliance, transportation security, and immigration, among others.

Expediting and safeguarding trade and travel while deterring and interdicting illicit traffic requires understanding how flows of people and goods interact with each other and with external forces. For example, transnational criminal organizations are highly dynamic, and will often respond to pressure on one illicit flow by shifting to another product or route. Similarly, as the volume of global trade and travel increases, the potential for harmful diseases or invasive species to cross our borders also increases.

Table 4: The following table shows how priority areas of emphasis for a risk segmentation approach to securing and managing flows of people and goods map to the homeland security missions.

A Risk Segmentation Approach to Securing and Managing Flows of People and Goods					
Priority Area of Emphasis	Prevent Terrorism and Enhance Security	Secure and Manage Our Borders	Enforce and Administer Our Immigration Laws	Safeguard and Secure Cyberspace	Strengthen National Preparedness and Resilience
Minimize Disruption to and Facilitate Safe and Secure Inbound and Outbound Legal Flows of People and Goods	✓	✓		✓	
Prioritize Efforts to Counter Illicit Finance and Further Increase Transnational Criminal Organization Perception of Risk, While Continuing to Increase Efficiencies in Operations		✓	✓	✓	
Prevent Terrorist Travel into the United States, Terrorism Against International Travel and Trade Systems, and the Export of Sensitive Goods and Technology	✓	✓			✓

SEGMENTING FLOWS OF PEOPLE AND GOODS

We identified three distinct but interrelated types of flows of people and goods based on an in-depth look at legal and illegal flows. Each type requires a different approach by DHS and our partners:

- **Legal Flows of People and Goods.** The vast majority of people and goods entering and exiting the United States represents lawful travel and trade. DHS and our partners work to secure and expedite these flows of people and goods, as they are a main driver of U.S. economic prosperity.

- **Market-Driven Illicit Flows of People and Goods.** These flows of people and goods are characterized by the exploitation of legitimate trade, travel, and financial systems or the creation of alternative, illicit pathways through which people and illegal goods—narcotics, funds, counterfeits, and weaponry—can cross the border. Primarily driven by criminal profits, these flows of people and goods are persistent and enduring. The risk from these activities is difficult to mitigate, especially given the limited role of homeland security activity in addressing the root causes of supply and demand.

- **Terrorism and Other Non-Market Concerns.** These flows of people and goods are driven by social, political, natural, or other non-market forces. These flows of people and goods are illegal, attempt to hide within legal flows or illicit flows that bypass ports of entry, and have the potential to overwhelm the legal trade and travel system or threaten national security. Examples include terrorists; migration driven by displacement or political fears; and the movement of diseases, pests, and invasive species.

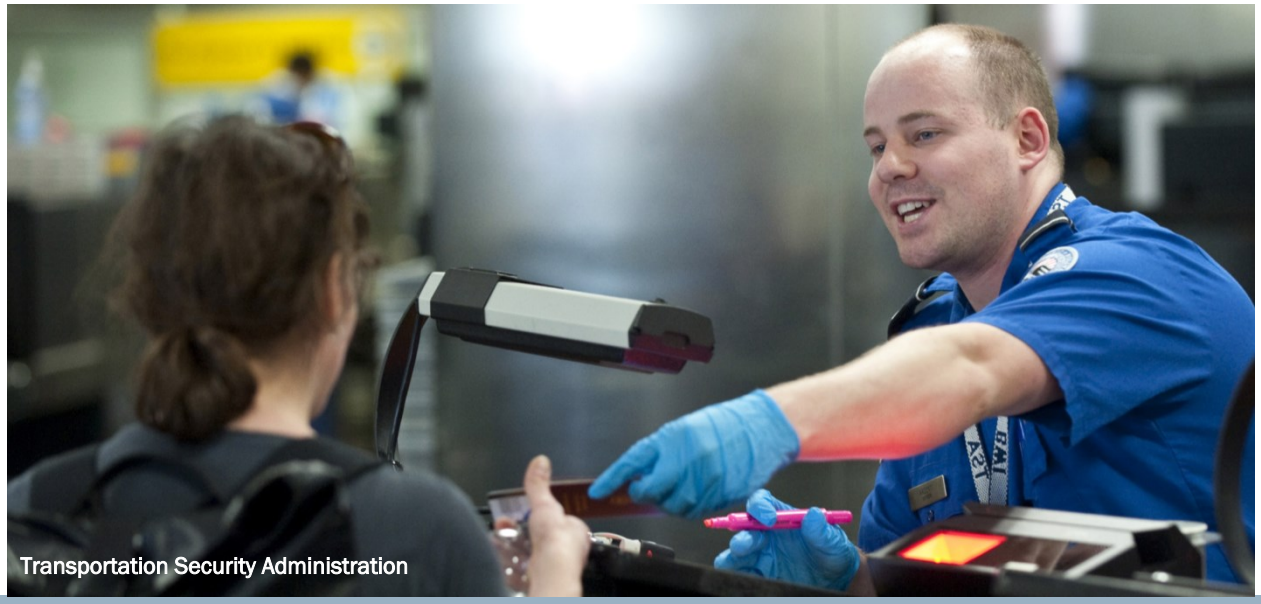
Segmenting flows of people and goods in this way permits more focused strategies and more efficient allocation of resources.

A HOMELAND SECURITY APPROACH TO FLOWS OF PEOPLE AND GOODS

Our approach to flows of people and goods focuses on achieving three strategic objectives: (1) minimize disruption to and facilitate safe and secure inbound and outbound legal flows of people and goods; (2) prioritize efforts to counter illicit finance and further increase transnational criminal organizations' perception of risk through targeted interdiction and other activities, while continuing to increase efficiencies in operations; and (3) prevent terrorist travel into the United States, terrorism against international travel and trade systems, and the export of sensitive goods and technologies.

Minimize Disruption to and Facilitate Safe and Secure Inbound and Outbound Legal Flows of People and Goods

Challenges to flows of people and goods are not limited to illegal activity. Trends indicate higher volumes of trade and travel could overwhelm our port of entry infrastructure and



Transportation Security Administration

strain frontline personnel. Aging infrastructure needs to be upgraded at air, land, and sea ports of entry.

We must also manage those threats and hazards that pose risk to the trade and travel system. We do this by sorting traveler and cargo traffic based on risk and expediting the movement of those found to be low risk. We partner with airlines, cargo carriers, and other relevant organizations to expedite legal flows of people and goods without compromising security. Pre-inspection capabilities, advanced analytics, and mutual recognition agreements with our international partners will further increase the use of traffic segmentation programs. Sorting traffic by risk also helps address terrorism threats, as discussed in the Securing Against the Evolving Terrorism Threat subsection.

Partnerships that leverage the overlapping interests, resources, and authorities of our partners in both the public and private sectors are essential to meet mutual safety and security needs while expediting trade and travel. Public-private partnerships are an important but underutilized resource, and we describe how to improve them in the Strengthening the Execution of Our Missions through Public-Private Partnerships subsection.

Prioritize Efforts to Counter Illicit Finance and Further Increase Transnational Criminal Organization Perception of Risk Through Targeted Interdiction and Other Activities, While Continuing to Increase Efficiencies in Operations

Our analysis identified two areas where DHS intervention can have an especially high impact: (1) targeting the profits of market-driven criminal activity and (2) increasing the perception of risk transnational criminal organizations face in attempting to serve U.S. markets. Our operations directed at market-driven illicit activities also need to become more efficient.

U.S. Customs and Border Protection

Targeting the profits of market-driven criminal activity eliminates the motive to conduct that activity. Illicit finance is the common factor across all illicit market-driven flows of people and goods. Our efforts should target illicit financing activities that transnational criminal organizations depend on, such as money laundering, and increase outbound inspection to deter practices such as cash smuggling or the use of stored-value media.

Transnational criminal organizations remain the primary adversary in market-driven flows of people and goods, and maximizing profit continues to be their major incentive. Although directly targeting the illegal movement of people and goods has resulted in reductions to specific flows, transnational criminal organizations are highly dynamic and will often respond to pressure on one illicit flow by shifting to another product or route. For that reason, it is difficult to assess the long-term effectiveness of specific actions on transnational criminal organization decision making. Homeland security activities must therefore create a deterrent effect, injecting the greatest amount of uncertainty and concern into that decision making. Examples of these types of activities include swiftly shifting assets, presence, technology, and tools, further targeting and focusing interdiction activities, and emphasizing strategic communications that project the effectiveness of homeland security capabilities.

We must also increase efficiencies in how we acquire, govern, and employ our capabilities for managing market-driven illicit activities. This includes (1) integrating capital acquisition and major investments across government; (2) increasing joint governance structures and collaboration to leverage assets, such as the National Targeting Center; and (3) shifting activities that have a lower impact on the overall system to lower-cost solutions.

Prevent Terrorist Travel into the United States, Terrorism Against International Travel and Trade Systems, and the Export of Sensitive Goods and Technology

Countering terrorism within the travel and trade system is a priority because (1) we must prevent violent extremists from exploiting legal and illegal pathways to enter the United States, and (2) attacks against the trade and travel system can cause major system disruption to American life and global commerce.

We must work with our partners in the Departments of Justice, Commerce, Energy, and elsewhere to prevent the export, re-export, or transfer of certain advanced technology and sensitive goods and technologies (e.g., restricted military and dual-use items) that could threaten the security of the United States and our allies if they fell into the wrong hands. Countering terrorism is further discussed in the Securing Against the Evolving Terrorism Threat subsection.

Port of Long Beach

STRENGTHENING THE EXECUTION OF OUR MISSIONS THROUGH PUBLIC-PRIVATE PARTNERSHIPS

OVERVIEW

Homeland security is achieved through a shared effort among all partners, from corporations to nonprofits and American families. Together, we can harness common interests to achieve solutions beyond what any of us could do alone. The first Quadrennial Homeland Security Review highlighted the need to mature and strengthen international partnerships as well as partnerships with state, local, tribal, and territorial governments. Building on that foundation, the second quadrennial review focuses on enhancing the critical relationship between government and the private sector.

Partnerships have always been fundamental to homeland security. Public-private partnerships advance the security and resilience of critical infrastructure under the National Infrastructure Protection Plan. Government relationships and agreements with airlines, shippers, and multi-national corporations facilitate the lawful flows of people and goods while enhancing security and screening capabilities. The Whole Community initiative for national preparedness and resilience supports the creation of critical preparedness

partnerships long before disasters occur. The Captain of the Port relationship, which combines a mix of authorities, regulatory regimes, and proactive collaboration among state and local agencies, industry, and port partners, strikes an important balance between regulation and partnership. This relationship encourages the use and creation of reasonable and fair regulations and fosters industry-led innovations in maritime safety and response technologies. The Air Cargo Advance Screening pilot program was built from the ground up in coordination with industry in response to al-Qa'ida in the Arabian Peninsula's 2010 attempt to attack the international air cargo system by detonating explosive devices hidden in air cargo shipments from Yemen to the United States. The Air Cargo Advance Screening pilot program is widely considered one of the best examples of homeland security partnership within both the public and private sectors.

Still, the Department can go further to advance a consistent, structured approach to partnerships as well as to enhance institutional awareness of public-private partnerships. The following framework outlines that structured approach and can be found in more detail in the Partnerships Toolkit, available at http://www.dhs.gov/qhsr.

Table 5: The following table shows how priority areas of emphasis for strengthening the execution of our missions through public-private partnerships map to the homeland security missions.

Strengthening the Execution of Our Missions through Public-Private Partnerships					
Priority Area of Emphasis	Prevent Terrorism and Enhance Security	Secure and Manage Our Borders	Enforce and Administer Our Immigration Laws	Safeguard and Secure Cyberspace	Strengthen National Preparedness and Resilience
Institutionalize a structured approach to developing public-private partnerships, to include homeland security partnership archetypes linked to specific desired outcomes	✓	✓	✓	✓	✓
Establish a homeland security Community of Practice to identify potential partnership opportunities, develop a repository of partnerships and best practices, and serve as a consultative body to inform the exploration and formation of new partnerships	✓	✓	✓	✓	✓

A STRUCTURED APPROACH TO PUBLIC-PRIVATE SECURITY AND RESILIENCE PARTNERSHIPS

Aligned Interests and Shared Outcomes

At a time when we must do more with less, two guiding principles help public-private partnerships maximize the investment by each partner and the success of the partnership: (1) aligning interests and (2) identifying shared outcomes.

By focusing on how interests align, we can provide alternatives to costly incentives or regulations and help ensure a partnership is based on a solid foundation of mutual interest and benefit. There are many examples of public and private sector interests aligning in homeland security. Common interests include the safety and security of people and property, the protection of sensitive information, effective risk management, the development of new technology, reputation enhancement, and improved business processes. New ways of thinking about corporate social responsibility—in which societal issues are held to be core business interests rather than traditional philanthropy—also present an opportunity to identify shared interests.

Where interests do not directly align, potential partners can often be motivated by shared desired outcomes, such as enhanced resilience; effective disaster response and recovery; and greater certainty in emerging domains, such as cyberspace and the Arctic.

Despite the existence of shared interests and mutual desired outcomes, challenges will exist. Partnerships must often overcome inherent differences in motivations and operational cultures, including risk tolerance, funding, and time horizons. The government must also be mindful to avoid suggesting a preferred relationship, endorsing a partner, or the appearance of privileged access or unfair competition. Being aware of, respecting, and creatively addressing these differences create an essential foundation for public-private partnerships.

Partnership Archetypes for Homeland Security

Successful, well-organized partnership frameworks begin with a set of flexible models for current and future partnerships. For decades, industries, such as construction and international development, have employed public-private partnership models to bring organization and definition to partnerships and provide a basic starting point for developing future partnerships. Flexible models also provide a foundation for thinking about partnership objectives, potential partners, and the resources and capabilities needed to address varying challenges.

Table 6: The five partnership archetypes.

Partnership Archetypes for Homeland Security
Information- and Data-Sharing Archetype ***Engage and Disseminate*** A partnership based on sharing relevant and timely information that may be useful to both parties
Coordination Archetype ***Align Complementary Activities*** A partnership that aligns policies, objectives, messages, and relevant activities among a group of partners to produce clarity and consensus
Operational Linkages Archetype ***Integrate Activities*** A partnership in which systems, procedures, or routines of individual partners are linked to facilitate operations
Co-Investment Archetype ***Consolidate Financing and Resources*** A partnership that consolidates financing for a specific project for a specific goal
Co-Production Archetype ***Create New Products*** A partnership in which the public and private sectors come together to develop and produce new products and processes

Within homeland security, there are five partnership archetypes that encompass the types of relationships we share with the private sector, as shown in Table 6. These archetypes are tied to unique desired outcomes and are arrayed across a spectrum according to depth, investment, and complexity. For well-known challenges, where roles and responsibilities are clearly documented, partnership models can be applied directly. As problems increase in complexity and risk, however, the flexible models can be adapted, scaled, or even combined to achieve desired outcomes.

The Path Forward: A Partnership Culture for Homeland Security

Building on the foundation of the archetypes, we can begin to apply common lessons learned and best practices, spark new and innovative partnerships, and develop crucial relationships long before crises occur. We will build a Department-wide Community of Practice to synchronize the identification of potential partnership opportunities, develop a repository of partnerships and best practices, and serve as a consultative body to inform the exploration and formation of new partnerships, in close collaboration with other federal agencies and the private sector. In addition, we must highlight the importance of partnerships in training and education activities to build the skills needed to identify and negotiate successful partnerships. By developing this shared expertise, we will create, enhance, and sustain our essential relationship with the private sector.

Federal Emergency Management Agency/Tim Burkitt

6. AREAS OF ONGOING PRIORITY AND EMPHASIS

While the Strategic Priorities section of this report describes strategic shifts and new areas of priority, this section reflects certain key ongoing priorities and areas of emphasis for homeland security, driven by risk and long-standing policy imperatives.

NUCLEAR TERRORISM USING AN IMPROVISED NUCLEAR DEVICE

OVERVIEW

Nuclear terrorism remains an enduring risk because of its potential consequences, and as such, preventing nuclear terrorism is a national security priority for the United States. As President Obama stated in his speech at South Korea's Hankuk University in March 2012, "We know that just the smallest amount of plutonium—about the size of an apple—could kill hundreds of thousands and spark a global crisis. The danger of nuclear terrorism remains one of the greatest threats to global security." A terrorist nuclear attack on the Nation would cause severe loss of life, illness, and injury; present challenges to our economy and our free and open society; and damage the national psyche. While the difficulty of stealing

a nuclear weapon or fabricating one from stolen or diverted weapons materials reduces the likelihood of this type of attack, the extremely high consequences of an improvised nuclear device attack make it an ongoing top homeland security risk.

STRATEGIC APPROACH

We prioritize a *sustained, long-term* focus on preventing nuclear terrorism through two foundational capabilities: (1) nuclear detection and (2) nuclear forensics. These capabilities are aimed at preventing our adversaries from developing, possessing, importing, storing, transporting, or using nuclear materials. While we have made significant progress in both detection and forensics over the years, the threat of nuclear terrorism is persistent and requires constant vigilance.

DHS and other departments and agencies have combined their authorities and assets to build the U.S. Government's global nuclear detection capability through the Global Nuclear Detection Architecture, a world-wide network of sensors, people, and information designed to encounter, detect, characterize, and report on nuclear material out of regulatory control. Not only does the Global Nuclear Detection Architecture help reduce the likelihood that radiological or nuclear material can be used as a weapon against the Nation, but by

U.S. Customs and Border Protection

increasing the cost, difficulty, and risk of attempting a nuclear attack, it also acts to deter those who may seek to attack us. The Global Nuclear Detection Architecture presents terrorists with many obstacles to a successful attack, greatly increasing their cost, difficulty, and risk, and thereby deterring terrorists. Through this detection architecture, departments and agencies train personnel, deploy detection systems at home and abroad, and analyze the data these systems generate. Federal, state, local, tribal, territorial, and international partners, as well as many others, are engaged in this effort.

While Global Nuclear Detection Architecture capabilities are focused primarily against terrorists, federal department and agency nuclear forensics capabilities target the decision making of would-be state sponsors. Terrorists can only acquire the special nuclear material necessary for a nuclear weapon by theft, illicit trafficking, or direct support from a state. Thus, nuclear forensics efforts are focused on deterring potential state sponsors of nuclear terrorism by denying them anonymity and ensuring they be held accountable.

As stated in the *Nuclear Posture Review* (2010), the United States is committed to hold fully accountable any state, terrorist group, or other non-state actor that supports or enables terrorist efforts to obtain or use weapons of mass destruction. Our commitment is made possible by our ability to identify perpetrators through information gained from nuclear forensics, intelligence, and law enforcement. Such information serves as a strong deterrent to terrorist accomplices and especially to potential state sponsors of terrorism. Federal agencies work with our National Technical Nuclear Forensics Center to ensure the Nation's nuclear forensics capability is continually advancing and is ready to respond to a nuclear trafficking incident or a terrorist nuclear attack.

We can leverage these nuclear detection and forensics capabilities to influence the decision making of key actors in a potential terrorist nuclear attack or radiological attack, thereby reducing its likelihood.

We complement our operational efforts with extensive analysis aimed at understanding radiological and nuclear terrorism risk. This analysis has matured to a point where we can understand and discern different levels of risk posed by the various pathways and mechanisms for introducing an improvised nuclear device into the United States, not simply the potential consequences of such an introduction. Consequently, we balance our efforts across pathways commensurate with the risk that each one poses.


U.S. Citizenship and Immigration Services

IMMIGRATION

OVERVIEW

Immigration is essential to our identity as a nation of immigrants. Most American families have an immigration story, some recent, some more distant. Many immigrants have taken on great risks to come to our country and seek to work and contribute to America's prosperity or were provided refuge after facing persecution abroad. Americans are extremely proud of this tradition.

Immigration will always be, first and foremost, an opportunity for our country. We reap great economic benefits from receiving the best, brightest, and most hardworking people from across the globe. Immigrants also build bridges to other nations, personally extending our diplomatic reach. They serve in our military and intelligence services with honor, sometimes contributing important language and cultural skills. Immigration enhances how the United States is perceived—as a cosmopolitan nation made up of many cultures and as a champion of humanitarian causes around the world.

Smart and effective enforcement and administration of our immigration laws remains a core homeland security mission. But even though we have already made significant improvements to border security, interior enforcement, and benefits adjudication, our current immigration system remains broken, and it remains an economic, humanitarian, and national security imperative to fix it. Our country needs an immigration system that better supports family reunification, meets the demands of our growing economy, extends humanitarian protections to those in need, and gives undocumented immigrants a path to earned citizenship. Enactment of comprehensive immigration reform thus remains a top homeland security priority.

The President has established four core objectives for strengthening our immigration system through common-sense immigration reform:

- Continuing to strengthen border security;
- Cracking down on employers that hire undocumented workers;
- Creating a path to earned citizenship; and
- Modernizing and streamlining our legal immigration system.

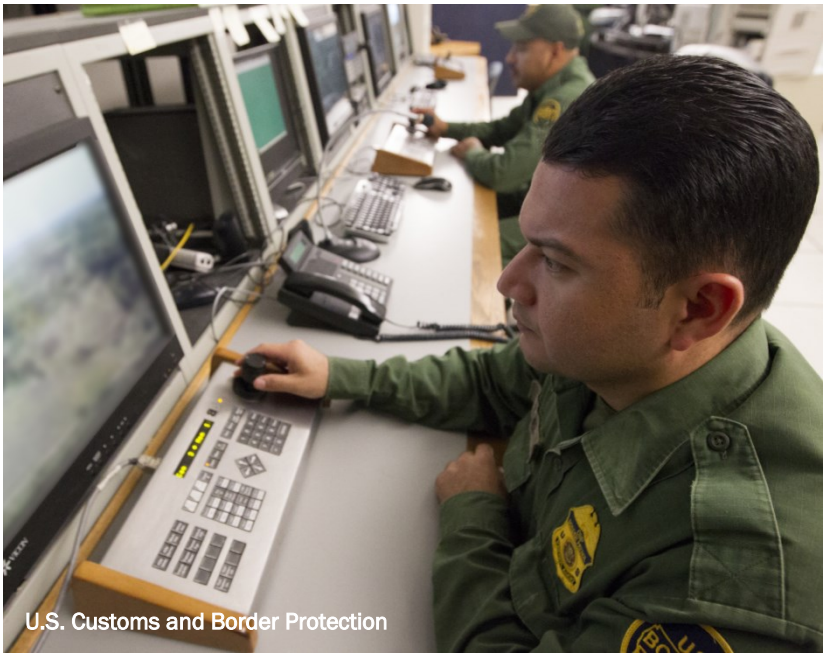
To accomplish these objectives, homeland security partners and stakeholders must function as an interconnected whole. DHS and the Departments of State, Justice, Education, Health and Human Services, and Labor all work to facilitate lawful immigration and to identify and remove threats to our national security and public safety. Further, state and local governments and law enforcement, businesses large and small, and nongovernmental and voluntary organizations also play important roles in our immigration system. For example, government and voluntary organizations together support new refugee arrivals, and government and employers cooperate to ensure that employees are working legally and to prevent employers from discriminating against employees when verifying their authorization to work in the United States. The Federal Government and state and local law enforcement agencies coordinate as appropriate to identify those who pose a national security or public safety risk, so the Federal Government can pursue appropriate enforcement action.

As the President stated in his 2014 State of the Union address, Congress must enact common-sense, comprehensive immigration reform.

STRATEGIC SHIFTS IN IMMIGRATION

BUILDING A STRONGER, SMARTER BORDER ENFORCEMENT SYSTEM

Our immigration system continues to prioritize the security of our border and its arrival zones. As with other flows of people and goods (described in the A Risk Segmentation Approach to Securing and Managing Flows of People and Goods subsection), we take a risk-informed, intelligence-driven, and networked approach to enforcing immigration laws. We have built a border security system that is stronger than ever before; the Border Patrol has doubled from approximately 10,000 agents in 2004 to 21,370 in 2014. Investigative resources have also expanded. The Federal Government works closely with state, local, tribal, and territorial partners to identify concerns at our borders, whether they occur on land, via air routes, or at sea.


U.S. Customs and Border Protection

Securing the border is not just about adding more resources; it is about using the resources we have in a smarter way. We have deployed a vast array of new technologies at and between points of entry. For example, unmanned aerial surveillance tools now can cover the southwest border from California to Texas. More traditional border security tools also remain available to enhance border security. We continue to deploy fixed and mobile surveillance capabilities on the ground, allowing more agents to shift from detection duties to increase our capacity to respond, interdict, and resolve illegal activities. We will continue to operate in a manner that protects privacy and civil liberties and respects humanitarian interests.

The security of the U.S. immigration system can only be ensured by cooperating with foreign states. Through the U.S.-Canada Beyond the Border initiative and the U.S.-Mexico Declaration on 21st-Century Border Management, we are working to harmonize processing inspection and data-sharing efforts with the Governments of Mexico and Canada. We have also concluded agreements with Caribbean countries lending support to U.S. Coast Guard rescue and interdiction operations at sea. In Central America, in collaboration with our

partners, we are focusing public messaging and diplomatic engagement efforts, in conjunction with the Department of State, on countries that have been increasing sources of illegal migration. In other countries, U.S. visa security program officers continue to prevent travel by those who pose a threat. We will continue to secure the border by cooperating with foreign allies.

Together, these efforts are making concrete improvements in our homeland security. We will continue to build on this progress, enhancing infrastructure and deploying technology to strengthen our ability to keep out criminals and national security threats. Comprehensive immigration reform, including enhanced penalties against criminals, would facilitate this effort.

Achieving Smart and Effective Interior Enforcement

DHS and our partners are taking a more effective approach to interior enforcement. In particular, we prioritize removing those posing threats to national security, border security, or public safety—aliens engaged in or suspected of terrorism or espionage and aliens convicted of crimes—while protecting victims of crime and human trafficking. We also prioritize prosecuting priority cases, such as against unscrupulous employers and transnational criminal organizations involved in document fraud, trafficking, and human smuggling, while using prosecutorial discretion on a case-by-case basis and as appropriate.

U.S. Immigration and Customs Enforcement

Our worksite enforcement strategy uses other tools, such as audits and civil fines, to penalize employers who knowingly hire illegal workers. We also promote compliance through E-Verify, a web-based service that allows employers to verify whether their employees are eligible to work in the United States. Approximately 520,000 employers representing more than 1.4 million worksites are enrolled in the E-Verify program, including employers with federal contract positions.

While we use many means to effectively secure the Nation's interior, these efforts can only go so far. Comprehensive immigration reform is needed to enable businesses to employ a legal workforce through programs, such as mandatory employment verification, and more stringent penalties for those who violate the law.

Creating a 21st-Century Legal Immigration System

We are also committed to creating an immigration system that better meets our diverse economic needs. Such a system requires comprehensive immigration reform. Existing numerical limits within our immigration system ignore the needs of today's economy and constrain the benefits immigrants bring to our country. Further, workers need better mobility and additional protections to reduce the risk that they will be exploited. Comprehensive immigration reform is needed to reorient our immigration system to meet the needs of the marketplace.

In the meantime, we are working to better assist high-skilled immigrants. Entrepreneurs and government officials leveraged knowledge from our best and brightest through the Entrepreneurs-in-Residence initiative, streamlining DHS policies and practices to better reflect the realities faced by foreign entrepreneurs and start-up businesses. We have continued to use industry-specific Executives in Residence to ensure consistency in adjudications within the performing arts, entertainment, and nursing industries. We are also streamlining the processing of immigrant visas to encourage businesses to grow in the United States. For students, the Study in the States program provides concrete immigration guidance to those who want to study here. We will continue to develop innovative programs to enable immigrants to reach their potential in the United States.

Addressing Lengthy Visa Backlogs

Perhaps nowhere is there greater evidence of a broken immigration system than in the burdensome backlogs for family-based immigrants waiting for visa numbers to become available. Many family members face a wait time of a decade or more just for the chance to reunite with family members in the United States. While we already work to identify solutions on a case-by-case basis, more can and should be done.

Comprehensive reform of our family-based immigration system is needed to reunite families in a timely manner consistent with our values. One important reform would change numerical limits on family-sponsored immigration, significantly reducing the years of separation these families now endure.

Earned Path to Citizenship

Today, we have an estimated 11.5 million immigrants living in America without documentation. The overwhelming majority does not pose a threat; these individuals seek only to be fully contributing members of their communities. We support comprehensive immigration reform that would provide an earned pathway to citizenship for these persons. Qualified applicants would be required to register and undergo national security and

criminal background checks, pay taxes and a fine, and fully integrate into the United States by learning English.

Our country is stronger and more secure when everyone has a stake, fulfills his or her responsibilities, and is equally invested in our common future. Comprehensive immigration reform would represent a unique opportunity to improve homeland security.

Enhancing Management and Organization to Develop a Responsive Immigration System

At the center of any good immigration system must be an administrative structure able to rapidly respond to changes in demand while safeguarding security. We are constantly seeking ways to better administer benefits, clarify what is required of applicants, and use technology to make information more accessible. Based on feedback from our partners, DHS has implemented programs to support naturalization applicants and to help the public as the Department transforms from paper-based to electronic processing.

It is well understood that comprehensive immigration legislation will significantly increase pressures on our administrative system. We will work hard to ensure we have the capacity, staff, and resources to successfully implement any changes in the law. Following DHS's decision in June 2012 to extend consideration of deferred action for childhood arrivals —a process to allow undocumented young people who meet certain guidelines to remain and work in the United States—the Department received and processed more than a half-million deferred action requests in less than a year. We can and will build upon these successes.

U.S. Citizenship and Immigration Services

Federal Emergency Management Agency

NATIONAL PREPAREDNESS AND THE WHOLE COMMUNITY APPROACH

OVERVIEW

National preparedness is a top Administration priority and an enduring homeland security focus. Indeed, national preparedness underpins all efforts to safeguard and secure the Nation against those threats and hazards that pose the greatest risk. Given the evolving terrorism threat; the growing risk of cyber disruptions; enduring hazards, such as biological challenges and nuclear terrorism; and the increasing number of natural disasters with more costly and variable consequences—driven by trends, such as climate change, aging infrastructure, and shifts in population density to higher-risk areas—it is imperative to build and sustain core capabilities to prevent, protect against, mitigate, respond to, and recover from the most high-risk threats and hazards. Continued integration and increased coordination provide a mechanism for achieving greater national preparedness among homeland security partners within resource limits.

STRATEGIC APPROACH

Presidential Policy Directive 8 calls for a National Preparedness Goal (the Goal) that identifies the core capabilities necessary to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk; a National Preparedness System composed of guidance, programs, and processes to guide activities to achieve the Goal; and a comprehensive Campaign to Build and Sustain Preparedness to unify efforts across the Whole Community to build and sustain national preparedness. Presidential Policy Directive 8 reinforces and complements the authorities set forth in the Post-Katrina Emergency Management Reform Act of 2006. These key national preparedness elements include the following:

- **The National Preparedness Goal:** The Goal defines what it means for the Nation to be prepared for the threats and hazards that pose the greatest risk, including acts of terrorism, cyberattacks, pandemics, and catastrophic natural disasters. The Goal is "[a] secure and resilient Nation with the capabilities required across the Whole Community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."

- **The National Preparedness System:** The National Preparedness System provides a consistent approach that supports decision making, resource allocation, and the measurement of progress toward achieving the Goal. The National Preparedness System includes but is not limited to the following:

    - **National Planning Frameworks and the Federal Interagency Operational Plans:** The Federal Emergency Management Agency (FEMA) and its partners completed first editions of the National Prevention Framework, National Protection Framework, National Mitigation Framework, and National Disaster Recovery Framework, as well as the second edition of the National Response Framework. Together, these National Planning Frameworks describe how the Whole Community works together to prevent, protect against, mitigate, respond to, and recover from threats and hazards. Each framework is supported by a Federal Interagency Operational Plan, which explains how federal departments and agencies work together to deliver the core capabilities through the coordinating mechanisms outlined in the framework. The Protection Federal Interagency Operational Plan is under development. The frameworks are built upon scalable, flexible, and adaptable coordinating

structures that align key roles and responsibilities to deliver necessary capabilities.

- ◊ **Catastrophic Planning:** Catastrophic planning is performed both at FEMA Headquarters and the FEMA regional offices in collaboration with the Whole Community and includes planning for National Special Security Events.

- ◊ **National Exercise Program:** The National Exercise Program serves as the cornerstone of a collective effort to test, improve, and assess national preparedness. The program seeks to enhance resilience at all levels of government, within nonprofit, faith-based, and nongovernmental organizations and throughout the private sector. It employs a finite series of progressive exercises that test the ability to prevent, protect against, mitigate, respond to, and recover from all hazards.

- ◊ **National Preparedness Report:** The annual National Preparedness Report summarizes national progress in building, sustaining, and delivering the 31 core capabilities outlined in the Goal, based on analysis from ongoing national preparedness assessments.

- **Campaign to Build and Sustain Preparedness:** The Campaign has four key elements: (1) a comprehensive campaign, including public outreach and community-based and private sector programs; (2) federal preparedness efforts; (3) grants, technical assistance, and other federal preparedness support; and (4) research and development. This initiative provides a structure for integrating new and existing community-based, nonprofit, and private sector preparedness programs, research and development activities, and preparedness assistance. Further, the Campaign is designed to provide consistent and constant outreach to the public to help ensure the basic tenets of the Goal are understood and met.

Recognizing that preparedness is a shared responsibility, the Whole Community approach calls for the involvement of everyone—not just the government—in preparedness efforts. By working together, everyone can keep the Nation safe from harm and resilient when struck by hazards. The Whole Community approach is based on three core principles: (1) understanding and meeting the actual needs of the Whole Community; (2) engaging and empowering all parts of the community; and (3) strengthening what works well in communities on a daily basis. Whole Community is a means by which residents, emergency managers, organizational and community leaders, government officials, private and nonprofit sectors, faith-based and disability organizations, and the general public can

collectively understand and assess the needs of their respective communities as well as determine the best ways to organize and strengthen their assets, capacities, and interests. A Whole Community approach to planning and implementing disaster strategies helps build a more effective path to societal security and resilience.

Whole Community includes the following:

- Individuals and families, including those with access and functional needs;
- Businesses;
- Faith-based and community organizations;
- Nonprofit groups;
- Schools and academia;
- Media outlets; and
- All levels of government, including federal, state, local, tribal, and territorial partners.

The Whole Community approach helps each community make smart decisions about how to manage those segments of the community. This includes accounting for the composition of the community, the individual needs of community members of every age and income level, and all accessibility requirements. It also helps residents, emergency managers, organizational and community leaders, government officials, private and nonprofit sectors, faith-based and disability organizations, and the general public to collectively understand community needs and how to organize resources to meet those needs. Supporting this process, state, local, tribal, and territorial governments identify their risks and make decisions for addressing their greatest risks through the completion of the Threat and Hazard Identification and Risk Assessment process.

In this manner, national preparedness increases security and resilience by helping our Nation systematically prepare for the threats and hazards that pose the greatest risk.

7. MISSION FRAMEWORK IN DEPTH

The first quadrennial review developed an enduring framework of missions and associated goals that tell us in detail what it means to ensure a safe, secure, and resilient Nation, as well as how to go about the business of conducting homeland security. These missions are not limited to DHS—hundreds of thousands of people from across the Federal Government; state, local, tribal, and territorial governments; the private sector; and other nongovernmental organizations are responsible for executing these missions. These homeland security professionals are responsible for public safety and security. They regularly interact with the public; facilitate and expedite legal trade and travel; own and operate our Nation's critical infrastructure and services; perform research and develop technology; and keep watch for, prepare for, deter, anticipate, and respond to emerging threats and hazards. As our partners carry out their homeland security responsibilities, the homeland security mission framework serves as a guidepost and provides clarity and unity of purpose.

The updated missions and goals set forth in this second Quadrennial Homeland Security Review report reflect changes in the strategic environment and areas where homeland security partners and stakeholders have matured, evolved, and enhanced their capabilities and understanding of the homeland security mission space:

MISSION 1: PREVENT TERRORISM AND ENHANCE SECURITY

Goal 1.1: Prevent Terrorist Attacks

- Analyze, fuse, and disseminate terrorism information;
- Deter and disrupt operations;
- Strengthen transportation security; and
- Counter violent extremism.

Goal 1.2: Prevent and Protect Against the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities

- Anticipate chemical, biological, radiological, and nuclear emerging threats;
- Identify and interdict unlawful acquisition and movement of chemical, biological, radiological, and nuclear precursors and materials; and
- Detect, locate, and prevent the hostile use of chemical, biological, radiological, and nuclear materials and weapons.

Goal 1.3: Reduce Risk to the Nation's Critical Infrastructure, Key Leadership, and Events

- Enhance security for the Nation's critical infrastructure from terrorism and criminal activity; and
- Protect key leaders, facilities, and national special security events.

MISSION 2: SECURE AND MANAGE OUR BORDERS

Goal 2.1: Secure U.S. Air, Land, and Sea Borders and Approaches

- Prevent illegal import and entry; and
- Prevent illegal export and exit.

Goal 2.2: Safeguard and Expedite Lawful Trade and Travel

- Safeguard key nodes, conveyances, and pathways;
- Manage the risk of people and goods in transit; and
- Maximize compliance with U.S. trade laws and promote U.S. economic security and competitiveness.

Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations and Other Illicit Actors

- Identify, investigate, disrupt, and dismantle transnational criminal organizations; and
- Disrupt illicit actors, activities, and pathways.

MISSION 3: ENFORCE AND ADMINISTER OUR IMMIGRATION LAWS

Goal 3.1: Strengthen and Effectively Administer the Immigration System

- Promote lawful immigration;
- Effectively administer the immigration services system; and
- Promote the integration of lawful immigrants into American society.

Goal 3.2: Prevent Unlawful Immigration

- Prevent unlawful entry, strengthen enforcement, and reduce drivers of unlawful immigration; and
- Arrest, detain, and remove priority individuals, including public safety, national security, and border security threats.

MISSION 4: SAFEGUARD AND SECURE CYBERSPACE

Goal 4.1: Strengthen the Security and Resilience of Critical Infrastructure

- Enhance the exchange of information and intelligence on risks to critical infrastructure and develop real-time situational awareness capabilities that ensure machine and human interpretation and visualization;
- Partner with critical infrastructure owners and operators to ensure the delivery of essential services and functions;
- Identify and understand interdependencies and cascading impacts among critical infrastructure systems;
- Collaborate with agencies and the private sector to identify and develop effective cybersecurity policies and best practices; and
- Reduce vulnerabilities and promote resilient critical infrastructure design.

Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise

- Coordinate government purchasing of cyber technology to enhance cost-effectiveness;
- Equip civilian government networks with innovative cybersecurity tools and protections; and
- Ensure government-wide policies and standards are consistently and effectively implemented and measured.

Goal 4.3: Advance Law Enforcement, Incident Response, and Reporting Capabilities

- Respond to and assist in the recovery from cyber incidents; and
- Deter, disrupt, and investigate cybercrime.

Goal 4.4: Strengthen the Ecosystem

- Drive innovative and cost effective security products, services, and solutions throughout the cyber ecosystem;
- Conduct and transition research and development, enabling trustworthy cyber infrastructure;
- Develop skilled cybersecurity professionals;
- Enhance public awareness and promote cybersecurity best practices; and
- Advance international engagement to promote capacity building, international standards, and cooperation.

MISSION 5: STRENGTHEN NATIONAL PREPAREDNESS AND RESILIENCE

Goal 5.1: Enhance National Preparedness

- Empower individuals and communities to strengthen and sustain their own preparedness;
- Build and sustain core capabilities nationally to prevent, protect against, mitigate, respond to, and recover from all hazards; and
- Assist federal entities in the establishment of effective continuity programs that are regularly updated, exercised, and improved.

Goal 5.2: Mitigate Hazards and Vulnerabilities

- Promote public and private sector awareness and understanding of community-specific risks;
- Reduce vulnerability through standards, regulation, resilient design, effective mitigation, and disaster risk reduction measures; and
- Prevent incidents by establishing, and ensuring compliance with, standards and regulations.

Goal 5.3: Ensure Effective Emergency Response

- Provide timely and accurate information;
- Conduct effective, unified incident response operations;
- Provide timely and appropriate disaster assistance; and
- Ensure effective emergency communications.

Goal 5.4: Enable Rapid Recovery

- Ensure continuity and restoration of essential services and functions; and
- Support and enable communities to rebuild stronger, smarter, and safer.

MATURE AND STRENGTHEN HOMELAND SECURITY

The strategic aims and objectives for Maturing and Strengthening Homeland Security are drawn from the common themes that emerge from each of the homeland security mission areas.

Integrate Intelligence, Information Sharing, and Operations

- Enhance unity of regional operations coordination and planning;
- Share homeland security information and analysis, threats, and risks;
- Integrate counterintelligence;
- Establish a common security mindset; and
- Preserve civil liberties, privacy, oversight, and transparency in the execution of homeland security activities.

Enhance Partnerships and Outreach

- Promote regional response capacity and civil support;
- Strengthen the ability of federal agencies to support homeland security missions;
- Expand and extend governmental, nongovernmental, domestic, and international partnerships; and
- Further enhance the military-homeland security relationship.

Conduct Homeland Security Research and Development

- Scientifically study threats and vulnerabilities;
- Develop innovative approaches and effective solutions; and
- Leverage the depth of capacity in national labs, universities, and research centers.

Train and Exercise Frontline Operators and First Responders

- Enhance systems for training, exercising, and evaluating capabilities; and
- Support law enforcement, first responder, and risk management training.

Strengthen Service Delivery and Manage DHS Resources

- Recruit, hire, retain, and develop a highly qualified, diverse, effective, mission-focused, and resilient workforce; and
- Manage the integrated investment life cycle to ensure that strategic and analytically-based decisions optimize mission performance.


U.S. Customs and Border Protection

8. CONCLUSION

Four years ago, the first quadrennial review defined homeland security for America in the 21st century as a concerted national effort to ensure a Nation that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.

Since then, we have developed capabilities and processes to become more risk based, more integrated, and more efficient. This second quadrennial review describes how those capabilities and processes inform us of what challenges lie ahead and how to strategically posture ourselves to address those challenges.

Based on the strategic environment, the drivers of the most significant risk, and our guiding principles, the second Quadrennial Homeland Security Review identifies the following strategic priorities, which cut across the five homeland security missions:

- An updated posture to address the increasingly decentralized terrorist threat;
- A strengthened path forward for cybersecurity that acknowledges the increasing interdependencies among critical systems and networks;
- A homeland security strategy to manage the urgent and growing risk of biological threats and hazards;
- A risk segmentation approach to securing and managing flows of people and goods; and
- A new framework for strengthening mission execution through public-private partnerships.

Beyond these strategic priorities, this review also highlights ongoing areas of priority and emphasis—countering nuclear threats, strengthening our national immigration system, and enhancing national resilience—based on key aspects of the security environment and policy priorities for homeland security.

Together, the strategic shifts and areas of renewed emphasis position DHS and our partners to address those threats and hazards that pose the most strategically significant risk to the Nation. Much work remains to be done to translate these strategies and priorities into action, including a DHS Strategic Plan that specifies necessary capabilities and associated investments, as well as focused efforts to enhance departmental management and improve workforce morale. We must all play a role—and through the commitment of each, we will secure the Nation for all.


U.S. Customs and Border Protection

APPENDIX A: HOMELAND SECURITY ROLES AND RESPONSIBILITIES

Homeland security spans the authorities and responsibilities of federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and private citizens and communities. For this reason, coordination and cooperation are essential to successfully carrying out and accomplishing the homeland security missions. This Appendix highlights key roles and responsibilities of the many homeland security partners and stakeholders. Nothing in this report alters, or impedes the ability to carry out, the authorities or missions of federal departments and agencies to perform their responsibilities or priorities under law.

- The **President of the United States** is the Commander in Chief and the leader of the Executive Branch of the Federal Government. The President, through the Homeland Security and National Security Councils and the National Security Council staff, provides overall homeland security policy direction and coordination.

- The **Department of Homeland Security (DHS)** is the federal agency defined by statute as charged with homeland security: preventing terrorism and enhancing security; securing and managing our borders; enforcing and administering our immigration laws; strengthening cyberspace and critical infrastructure; and strengthening national preparedness and resilience to disasters. The Secretary of Homeland Security is responsible for coordinating the domestic all-hazards preparedness efforts of all executive departments and agencies, in consultation with state, local, tribal, and territorial governments, nongovernmental organizations, private-sector partners, and the general public. Preparedness efforts include those actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats and hazards that pose the greatest risk to the security and resilience of the Nation. DHS includes U.S. Customs & Border Protection, U.S. Citizenship & Immigration Services, U.S. Coast Guard, Federal Emergency Management Agency, U.S. Immigration & Customs Enforcement, U.S. Secret Service, and Transportation Security Administration. DHS is the coordinating agency for multiple Emergency Support Functions under the National Response Framework (see Figure A-1). In particular, with respect to its responsibilities regarding safeguarding and security cyberspace:

    - ◊ To better manage and facilitate cybersecurity information sharing efforts, analysis, and incident response activities, the Department operates the

National Cybersecurity and Communications Integration Center, an around-the-clock center where key government, private sector, and international partners all work together. The National Cybersecurity and Communications Integration Center serves as a focal point for coordinating cybersecurity information sharing with the private sector; provides technical assistance, onsite analysis, mitigation support, and assessment assistance to cyber-attack victims, as well as situational awareness capability that includes integrated, actionable information about emerging trends, imminent threats, and the status of incidents that may impact critical infrastructure; and coordinates the national response to significant cyber incidents affecting critical infrastructure.

- ◊ DHS, through U.S. Immigration and Customs Enforcement Homeland Security Investigations, operates the Cyber Crime Center, which is responsible for providing domestic and international training; and the support, coordination and de-confliction of cyber investigations related to online economic crime, digital theft of export controlled data, digital theft of intellectual property and online child exploitation investigations. The U.S. Secret Service leads a network of Electronic Crimes Task Forces to bring together federal, state, and local law enforcement, prosecutors, private industry, and academia for the common purpose of preventing, detecting, mitigating, and investigating various forms of malicious cyber activity.

The **Department of Justice (DOJ)**, led by the Attorney General, is responsible for prosecution of federal crimes. The Attorney General has lead responsibility for criminal investigation of terrorist acts or threats within the United States and its territories, as well as for related intelligence collection activities within the United States. The Attorney General, generally acting through the Director of the Federal Bureau of Investigation (FBI), in cooperation with other departments and agencies engaged in activities to protect national security, coordinates the activities of the law enforcement community to detect, prevent, preempt, and disrupt terrorist threats or incidents against the United States. DOJ approves state governor requests for personnel and other federal law enforcement support under the Emergency Federal Law Enforcement Assistance Act. DOJ supports the National Health Security Strategy and it is a member of the Mitigation Framework Leadership Group established under the National Mitigation Framework. In addition, DOJ is responsible for Emergency Support Function #13 (Public Safety and Security). In particular:

- ◊ The mission of the FBI is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners; and to perform these responsibilities in a manner that is responsive to the needs of the public and is faithful to the Constitution of the United States. The FBI, primarily through Joint Terrorism Task Forces, has lead responsibility for the receipt and resolution of suspicious activity reporting of terrorist activities or acts in preparation of terrorist activities. The Attorney General, acting through the FBI Director, has primary responsibility for searching for, finding, and neutralizing weapons of mass destruction within the United States and its territories. As part of its efforts to investigate and disrupt cyber crime and national security cyber threats, the FBI is also responsible for operating the National Cyber Investigative Joint Task Force, a multi-agency national focal point with representation from intelligence, law enforcement, and military agencies to coordinate, integrate, and share information related to cyber threat investigations.

- ◊ DOJ deconflicts federal criminal investigations through several organizations, including the International Organized Crime Intelligence and Operations Center, the Organized Crime Drug Enforcement Task Force Fusion Center. The International Organized Crime Intelligence and Operations Center is a multi-agency intelligence center whose mission is to significantly disrupt and dismantle those international criminal organizations posing the greatest threat to the United States, and to coordinate the resulting multi-jurisdictional investigations and prosecutions. The Organized Crime Drug Enforcement Task Force Fusion Center is a multi-agency intelligence center designed to produce actionable intelligence products to support the field. The Center's unique capability includes cross-agency integration and analysis of data to develop products that are disseminated through the multi-agency Special Operations Division for further de-confliction before transmission to the field. All Organized Crime Drug Enforcement Task Force Fusion Center member agencies receive products, including the Task Force's Co-Located Strike Forces.

- The **Department of State** is the lead U.S. foreign affairs agency, and the Secretary of State is the President's principal foreign policy advisor. The Department develops and

implements policies to advance U.S. objectives and interests in shaping a freer, more secure, and more prosperous world. The Department also supports the foreign affairs activities of other U.S. Government entities and works with international partner nations and regional and multilateral organizations to protect the U.S. homeland and U.S. interests and citizens abroad. The Department also provides an array of important services to U.S. citizens and to foreigners seeking to visit or immigrate to the United States. The Department supports the National Health Security Strategy and is the coordinating agency for the International Coordination Support Annex under the National Response Framework.

- The **Department of Defense's (DOD)** military services, defense agencies, and geographic and functional commands protect the population of the United States and its territories, as well as the critical defense infrastructure, against external threats and aggression. DOD defends the Nation from attack; gathers foreign cyber threat intelligence and determines attribution; secures national security and military systems; supports national cyber incident protection, prevention, mitigation, and recovery; and investigates cybercrimes under military jurisdictions. DOD also provides support to civil authorities at the direction of the Secretary of Defense or the President when the capabilities of state, local, tribal, and territorial authorities to respond effectively to an event are overwhelmed. DOD is the lead coordinator for Emergency Support Function #3 (Public Works and Engineering) through the U.S. Army Corps of Engineers and provides support to the other Emergency Support Functions as directed.

    - ◊ DOD accomplishes its cybersecurity operational roles and responsibilities as part of the Federal Cybersecurity Operations Team through the CYBERCOM Joint Operations Center, the National Security Agency/Central Security Service Threat Operations Center, the Defense Cyber Crime Center, and the Defense Information Systems Agency Command Center, in coordination with the cybersecurity operations centers operated by DHS and DOJ.

- The **Department of Health and Human Services (HHS)** leads the coordination of all functions relevant to Public Health Emergency Preparedness and Disaster Medical Response. HHS incorporates steady-state and incident-specific activities as described in the National Health Security Strategy. HHS serves as a member of the Mitigation Framework Leadership Group, the coordinating and primary agency for the Public Health and Medical Services Emergency Support Function, the coordinating agency for

the Health and Social Services Recovery Support Function, and a primary agency for the Community Planning and Capacity Building Recovery Support Function.

- The **Department of the Treasury** works to safeguard the U.S. financial system, combat financial crimes, and cut off financial support to terrorists, weapons of mass destruction proliferators, drug traffickers, and other threats to the national security, foreign policy, or economy of the United States. Treasury is a primary agency for the Economic Recovery Support Function.

- The **Department of Agriculture (USDA)** provides leadership on food, agriculture, natural resources, rural development, and related issues based on sound public policy, the best available science, and efficient management. The Department works with private land owners to build more resilient agricultural systems and healthier forest to reduce the risk of wildfire, insects, and disease. The USDA is a member of the Emergency Support Function Leadership Group, Recovery Support Function Leadership Group, and Mitigation Framework Leadership Group, the coordinator and primary agency for the Firefighting Emergency Support Function and Agriculture and Natural Resources Emergency Support Function, and primary or support agency for all six Recovery Support Functions.

- **Office of the Director of National Intelligence (ODNI).** The Director of National Intelligence serves as the head of the Intelligence Community, acts as the principal advisor to the President for intelligence matters relating to national security, and oversees and directs implementation of the National Intelligence Program. In addition to intelligence community elements with specific homeland security missions, ODNI maintains a number of mission and support centers that provide unique capabilities for homeland security partners, including the National Counterterrorism Center and National Counterproliferation Center.

- The **Department of Commerce** promotes job creation, economic growth, sustainable development, and improved standards of living for all Americans. The Department of Commerce is a member of the Mitigation Framework Leadership Group and the coordinating agency and a primary agency for the Economic Recovery Support Function.

- The **Department of Education** oversees discretionary grants and technical assistance to help schools plan for and respond to emergencies that disrupt teaching and

learning. The Department of Education supports the National Health Security Strategy and is a primary agency for the Health and Social Services Recovery Support Function.

- The **Department of Energy (DOE)** maintains stewardship of vital national security capabilities, from nuclear weapons to leading-edge research and development programs. DOE is the coordinating and primary agency for the Energy Emergency Support Function, is a member of the Mitigation Framework Leadership Group, and a primary agency for the Infrastructure Systems Recovery Support Function.

- The **Environmental Protection Agency (EPA)** is charged with protecting human health and the environment. EPA is a member of the Mitigation Framework Leadership Group, a primary agency for the Oil and Hazardous Materials Response Emergency Support Function, and a primary agency for the Natural and Cultural Resources and Health and Social Services Recovery Support Functions. EPA also carries out critical activities, as directed by Homeland Security Presidential Directive 10 and the National Response Framework, as it relates to decontamination.

- The **Department of Housing and Urban Development** is the coordinator and primary agency for the Housing Recovery Support Function and a member of the Mitigation Framework Leadership Group.

- The **Department of the Interior (DOI)** develops policies and procedures for all types of hazards and emergencies that impact Federal lands, facilities, infrastructure, and resources; tribal lands; and insular areas. DOI is also a member of the Mitigation Framework Leadership Group, a primary agency for the Search and Rescue Emergency Support Function, the coordinating agency and a primary agency for the Natural and Cultural Resources Recovery Support Function, and a primary agency for the Health and Social Services Recovery Support Function.

- The **Department of Transportation (DOT)** collaborates with DHS on all matters relating to transportation security and the security and resilience of transportation infrastructure and in regulating the transportation of hazardous materials by all modes (including pipelines). DOT supports the National Health Security Strategy and serves as a member of the Mitigation Framework Leadership Group, the coordinating agency for the Transportation Emergency Support Function, and a primary agency for the Infrastructure Systems Recovery Support Function.

- The **General Services Administration** is a member of the Mitigation Framework Leadership Group.

- The **Department of Labor** supports the National Health Security Strategy and is a primary agency for the Economic and Health and Social Services Recovery Support Functions. The Department of Labor/Occupational Safety and Health Administration is the Coordinating Agency for the Worker Safety and Health Support Annex under the National Response Framework.

- The **Department of Veteran's Affairs** is a primary agency for the Health and Social Services Recovery Support Function.

- The **Small Business Administration** is a member of the Mitigation Framework Leadership Group and a primary agency for the Economic Recovery Support Function.

- **Other Federal Agencies** contribute to the homeland security mission in a variety of ways. This includes agencies responsible for either supporting efforts to assure a resilient homeland or collaborating with the departments and agencies noted above in their efforts to secure the homeland.

- The **American Red Cross** is chartered by Congress to provide relief to survivors of disasters and help people prevent, prepare for, and respond to emergencies.

In addition to the roles and responsibilities specified above, Table A-1 identifies the coordinating and primary agencies for each of the Emergency Support Functions under the National Response Framework. The Emergency Support Functions are the primary federal coordinating structures for delivering response core capabilities established in the National Preparedness Goal.

APPENDIX A

Table A-1: ESFs and ESF Coordinators (Source: NRF)

ESFs and ESF Coordinators			
ESF #	ESF	ESF Coordinator	Primary Agency
1	Transportation	Department of Transportation	Department of Transportation
2	Communications	DHS/National Protection and Programs/Cybersecurity and Communications/National Communications System	DHS/National Communications System DHS/FEMA
3	Public Works and Engineering	Department of Defense/U.S. Army Corps of Engineers	Department of Defense/U.S. Army Corps of Engineers
4	Firefighting	Department of Agriculture/Forest Service, DHS/FEMA	Department of Agriculture/Forest Service
5	Information and Planning	DHS/FEMA	DHS/FEMA
6	Mass Care, Emergency Assistance, Temporary Housing, and Human Services	DHS/FEMA	DHS/FEMA, American Red Cross
7	Logistics	General Services Administration, DHS/FEMA	General Services Administration, DHS/FEMA
8	Public Health and Medical Services	Department of Health and Human Services	Department of Health and Human Services
9	Search and Rescue	DHS/FEMA	DHS/FEMA, DHS/U.S. Coast Guard, DHS/Customs and Border Protection, Department of the Interior/National Park Service, Department of Defense
10	Oil and Hazardous Materials Response	Environmental Protection Agency	Environmental Protection Agency, DHS/ U.S. Coast Guard
11	Agriculture and Natural Resources	Department of Agriculture	Department of Agriculture, Department of the Interior
12	Energy	Department of Energy	Department of Energy
13	Public Safety and Security	Department of Justice/ Bureau of Alcohol, Tobacco, Firearms, and Explosives	Department of Justice/Bureau of Alcohol, Tobacco, Firearms, and Explosives
14	Superseded by National Disaster Recovery Framework		
15	External Affairs	DHS	DHS/FEMA

In addition to the roles and responsibilities of federal departments and agencies, other homeland security participants include the following:

- **Private Sector Entities**, including businesses, industries, private schools and universities are integral parts of the community, and they play a wide range of critical roles. The majority of the Nation's infrastructure is owned and operated by private sector entities. They take action to align relevant planning, training, exercising, risk management and investments in security as a necessary component of prudent business planning and operations. During times of disaster, private sector partners provide response resources—including specialized teams, essential services, equipment, and advanced technologies—through public-private emergency plans/partnerships, or mutual aid and assistance agreements, or in response to requests from government and from nongovernmental-volunteer initiatives. In addition, the private sector has a role in building community resiliency by preparing for, responding to, and recovering from emergencies affecting their businesses.

- **Governors** are responsible for overseeing their state's threat prevention activities as well the state's response to any emergency or disaster, and take an active role in ensuring that other state officials and agencies address the range of homeland security threats, hazards, and challenges. During an emergency, governors will play a number of roles, to include serving as the state's chief communicator and primary source of information on the scope of the disaster, the need for evacuations, and the availability of assistance. Governors are commanders of their National Guards and are able to activate them to assist under state active duty during a disaster, and also retain command over their National Guard under Title 32 status. During a disaster, governors also will need to make decisions regarding the declaration of emergencies or disasters, requests for mutual aid, and calls for federal assistance.

- **State and Territorial Governments** supplement the activities of cities, counties, and intrastate regions. States administer federal homeland security grants (in certain grant programs) to local and tribal governments, allocating key resources to bolster their prevention and preparedness capabilities. State agencies conduct law enforcement and security activities, protect the governor and other executive leadership, and administer state programs that address the range of homeland security threats, hazards, and challenges. State government officials lead statewide disaster and mitigation planning. During response, states coordinate resources and capabilities throughout the state and are responsible for requesting and obtaining resources and capabilities from surrounding states. States often mobilize these

substantive resources and capabilities to supplement the local efforts before, during, and after incidents.

- **Tribal Leaders** are responsible for the public safety and welfare of their membership. They can serve as both key decision makers and trusted sources of public information during incidents.

- **Tribal Governments**, which have a special status under federal laws and treaties, ensure the provision of essential services to members within their communities, and are responsible for developing emergency response and mitigation plans. Tribal governments may coordinate resources and seek assistance from neighboring jurisdictions, states, and the Federal Government. Depending on location, land base, and resources, tribal governments provide law enforcement, fire, and emergency services as well as public safety to their members. During a disaster, tribal governments make decisions regarding whether to request a Presidential emergency or major disaster declaration independent of the state within which the tribal lands are located.

- **Mayors and Other Local Elected and Appointed Officials** are responsible for ensuring the public safety and welfare of their residents, serving as their jurisdiction's chief communicator and a primary source of information for homeland security-related information, and are responsible for ensuring their governments are able to carry out emergency response activities. Officials serve as key decision makers and trusted sources of public information during incidents. In some states, elected officials such as sheriffs or judges also serve as emergency managers, search and rescue officials, and chief law enforcement officers.

- **Local Governments** are responsible for the public safety, security, health, and welfare of the people who live in their jurisdictions. Local governments promote the coordination of ongoing protection plans and the implementation of core capabilities, as well as engagement and information sharing with private sector entities, infrastructure owners and operators, and other jurisdictions and regional entities. Local governments also address unique geographical issues, dependencies and interdependencies among agencies and enterprises and, as necessary, the establishment of agreements for cross-jurisdictional and public-private coordination. Local governments provide front-line leadership for local law enforcement, fire, public safety, environmental response, public health, and emergency medical services for preventing, protecting, mitigating, and responding to all manner of hazards and

emergencies. They are also responsible for ensuring all citizens receive timely information in a variety of accessible formats and coordinate resources and capabilities during disasters with neighboring jurisdictions, nongovernmental organizations, the state, and the private sector.

- Nongovernmental Organizations provide sheltering, emergency food supplies, counseling services, and other vital services to support response and promote the recovery of disaster survivors. They often provide specialized services and advocacy that help individuals with special needs, including those with disabilities, and provide resettlement assistance and services to arriving refugees. They also provide for evacuation, rescue, shelter, and care of animals, including household pets and service animals. Nongovernmental organizations are key partners in preparedness activities to include response and recovery operations.

- Communities are unified groups that share goals, values, or purposes rather than geographic boundaries or jurisdictions. These groups may possess the knowledge and understanding of the threats and hazards, local response capabilities, and requirements within their jurisdictions and have the capacity to alert authorities of those emergencies, capabilities, or needs. During an incident these groups may be critical in passing along vital communications to individuals and families, and to supporting response activities in the initial stages of a crisis.

- Individuals, Families, and Households take protective actions and the basic steps to prepare themselves for emergencies, including understanding the threats and hazards that they may face, reducing hazards in and around their homes, preparing an emergency supply kit and household emergency plans (that include care for animals, including household pets and service animals), monitoring emergency communications, volunteering with established organizations, enrolling in training courses, and practicing what to do in an emergency. These preparedness activities help to strengthen community resilience and mitigate the impact of disasters. In addition, individual vigilance and awareness can help communities remain safer and bolster prevention efforts by contacting local law enforcement and sharing information within their communities.

APPENDIX B: PROCESS AND STAKEHOLDER ENGAGEMENT ACTIVITIES

Section 2401 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, Pub. L. 110-53, amends Title VII of the *Homeland Security Act of 2002* to require the Secretary of Homeland Security to conduct a Quadrennial Homeland Security Review every four years beginning in 2009. In conducting the review, DHS is directed to consult with (1) the heads of other federal agencies, including the Attorney General, the Secretary of State, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of the Treasury, the Secretary of Agriculture, and the Director of National Intelligence; (2) key officials of the Department; and (3) other relevant governmental and nongovernmental entities, including state, local, tribal and territorial government officials, Members of Congress, private-sector representatives, academics, and other policy experts.

By articulating an enduring vision for and definition of homeland security, and establishing five homeland security missions, the first quadrennial review in 2010 answered the question, "What is homeland security?" Building on this foundation, the second quadrennial review identifies the necessary strategic shifts and areas of ongoing priority and renewed emphasis that will position DHS to successfully counter evolving threats and hazards, and keep our Nation safe. Pursuant to the legislative direction, the second review included two years of deliberate, rigorous analysis and substantive collaboration with partners at all levels of government and across the public and private sector.

REVIEW APPROACH: STRATEGY THROUGH ANALYSIS

The second Quadrennial Homeland Security Review included four phases: (1) preparation; (2) study and analysis; (3) writing and decision; and (4) rollout. The ***preparation phase***, which took place in 2012 and early 2013, included a review of homeland security risks and the dynamic security environment, as well as preliminary updates to the goals within the homeland security missions. The ***study and analysis*** phase, which took place during the spring and summer of 2013, focused on deep dive studies and targeted analyses. The ***writing and decision*** phase, which took place in fall 2013 and early 2014, interrupted by the partial government shutdown in October 2013, aimed at reaching decisions on high-priority questions with interagency partners and external stakeholders. As with the first Quadrennial Homeland Security Review, substantive engagement and outreach across a wide variety of stakeholders were critical across all stages of the review. ***Roll-out*** culminates the engagement with the release of the second quadrennial review. As with the

first review, the Office of Policy (PLCY), through its Office of Strategy, Planning, Analysis & Risk, served as the executive agent for the second review.

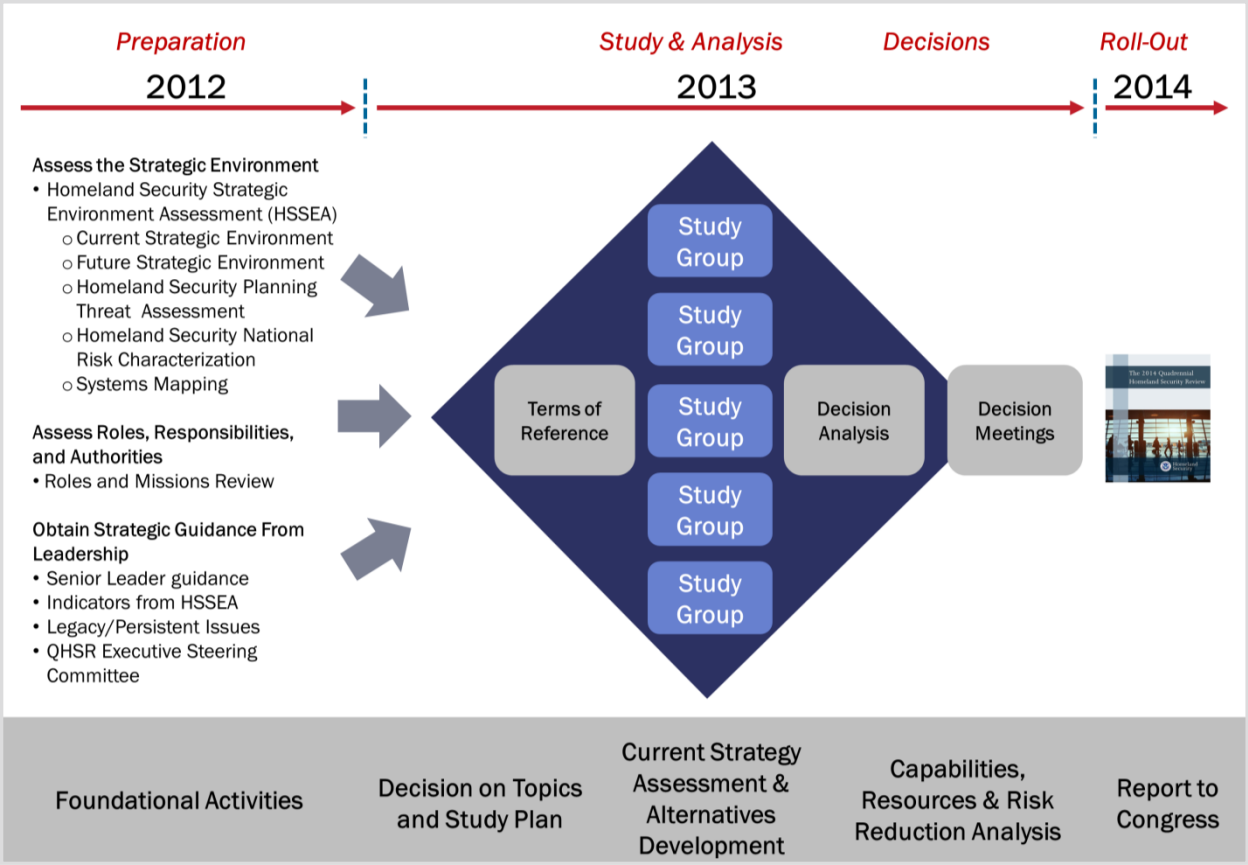


Figure B-1: The four phases of the second quadrennial review

PREPARATION PHASE

The Quadrennial Homeland Security Review preparation phase began in 2012 and focused on two primary efforts to prepare the Department to successfully execute the second review: (1) deeply examining the strategic environment, including threats and hazards, trends, future uncertainties, and strategic risk; and (2) reviewing, affirming, and where necessary updating the DHS missions and goals based on changes since the first quadrennial review. During this process, DHS developed a Homeland Security Strategic Environmental Assessment, which combined cross-cutting threat and hazard analysis with an examination of the changing risk environment through analysis of system relationships, trends, and future uncertainties. The result was insight into how strategic homeland security risk will likely evolve over time, and a clear sense of the threats and hazards that pose the most strategically significant risk to the Nation over the next five years. The Department also conducted a roles and missions review that affirmed the enduring nature

of the five core missions and the cross-cutting imperative to Mature and Strengthen Homeland Security.

STUDY AND ANALYSIS PHASE

Based on the preparation phase analyses and informed by conclusions about the areas that pose the most strategic significant risk, DHS leadership directed the following Quadrennial Homeland Security Review studies: (1) The Evolving Terrorism Threat; (2) Cybersecurity; (3) A Homeland Security Strategy for Countering Biological Threats and Hazards; (4) Securing and Expediting Flows of People and Goods; and (5) Governance in the Homeland Security Enterprise: The Public-Private Relationship. Several key areas of ongoing emphasis—Nuclear Terrorism Using an Improvised Nuclear Device, Immigration; and the National Preparedness System and the Whole Community Approach—were the subject of ongoing efforts pursuant to Congressional and Presidential direction and therefore were not explicitly studied in the quadrennial review process.

Each Quadrennial Homeland Security Review study involved a strategic review of the topic area, with on-going guidance and in-progress decisions from Departmental leadership. Each study group included a leader from PLCY's Office of Strategy, Planning, Analysis, and Risk, and a dedicated group of senior managers and subject matter experts from across DHS. Each study followed a tailored analytic plan based on a common approach to strategy development and analysis. This common approach includes four sequential elements with associated analytic milestones and deliverables:

- **Lay the Foundations**—Departmental leadership provided guidance, defined priorities, and set expectations for each study, while study groups developed plans for engaging partners and stakeholders inside and outside DHS;

- **Define the Context**—each study framed the challenge, including understanding threat and risk today and making assumptions about the future given key trends and uncertainties, and specified desired end-states;

- **Develop Solutions**—each study defined key priorities or areas of emphasis to best address the challenge and meet desired outcomes; where applicable, studies considered alternatives that traded off cost, risk reduction, executability, and robustness against future uncertainty; and

- **Decide on an Approach**—each study worked through relevant criteria and results from analysis to reach conclusions and recommendations for leadership on strategic posture shifts and areas of ongoing or renewed emphasis.

WRITING AND DECISION PHASE

Study group recommendations were provided to DHS leadership through the Quadrennial Homeland Security Review Executive Steering Committee, a body of senior executives from all DHS directorates, Components, and offices, and a series of Deputy Component head meetings chaired by the Deputy Secretary. The Department initiated drafting of the Quadrennial Homeland Security Review Report once decisions were reached across all studies. Decisions were informed by input from interagency partners and homeland security communities of interest, as described in "Stakeholder Engagement," below.

ROLL-OUT PHASE

The roll-out phase focuses on generating substantive dialogue with our partners and stakeholders, to include the public, on the future of the Nation's homeland security. The ultimate goal for the second review is to foster discussion about Quadrennial Homeland Security Review conclusions across the broad range of homeland security partners and stakeholders, and to drive review conclusions into programs and budgets, major investments, and operations.

STAKEHOLDER ENGAGEMENT

Throughout the Quadrennial Homeland Security Review study process, DHS conducted extensive engagement with federal executive branch partners and Congress; state, local, tribal and territorial partners; the private sector; academics; and others. The primary goal of stakeholder engagement was to solicit stakeholder perspectives on studies and supporting analysis, and to incorporate that input into the second quadrennial review. Since the Quadrennial Homeland Security Review Terms of Reference directed that the second review be an enterprise-wide review, a thorough and accurate picture of the homeland security landscape, and robust participation from stakeholders across all aspects of the enterprise was required. Acquiring this input involved engaging a group of stakeholders that was broad enough to present perspectives from across the enterprise and possessed the subject matter expertise needed to inform the analytic studies. Our analytical efforts focused on reviewing, researching, and synthesizing existing literature and academic work on the study topics, in-person discussions with experts in the field, and

the participation of homeland security stakeholders.

Pursuant to the Quadrennial Homeland Security Review legislative mandate, the review engagement strategy sought input from three groups of stakeholders (see Figure B-2):

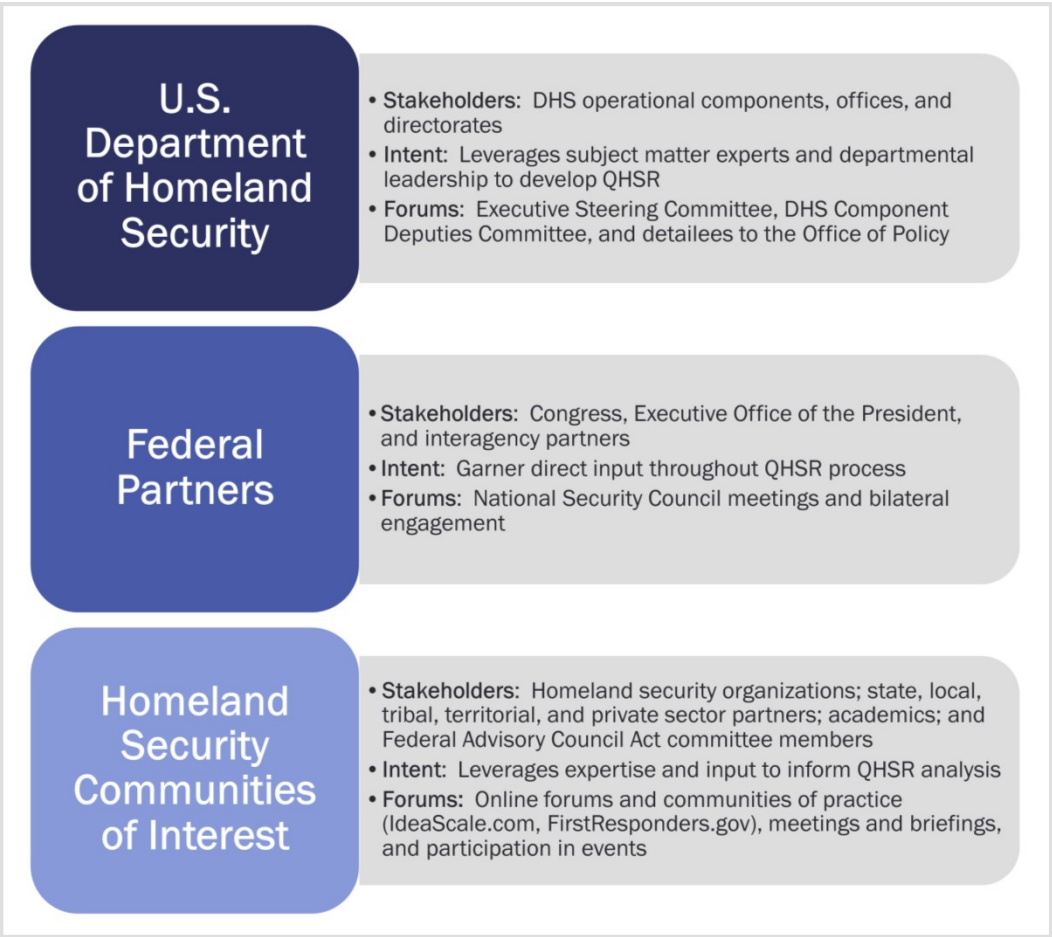


Figure B-2: DHS engaged three distinct stakeholder communities

DEPARTMENT OF HOMELAND SECURITY

Throughout the review, DHS employees at all levels were consulted and provided input. Each study lead convened a group of subject matter experts to shape and inform the analysis. An Executive Steering Committee of DHS Senior Executives guided the overarching narrative and presented decisions to DHS senior leadership through a series of Component Deputy Meetings:

Study Groups: In keeping with the inclusive approach of the review, more than 200 participants from across DHS Components and offices conducted each of the studies through standing working groups, led by a core group of analysts from PLCY's Office of Strategy, Planning, Analysis, and Risk. The work of the DHS study group participants was supported by a team of subject-matter experts and research analysts from the Homeland Security Studies and Analysis Institute, one of the Department's federally funded research and development centers. The study groups conducted their analysis over a 12-month period, with work products consistently shared using the online portals described in "Homeland Security Communities of Interest," below.

Executive Steering Committee: A Steering Committee, chaired by the Assistant Secretary for Strategy, Planning, Analysis & Risk and made up of senior executive-level representatives of all DHS Components, met more than 25 times for coordination and consultation through the course of the review. The Steering Committee provided insight and suggestions, and shaped study group material for decision.

DHS Senior Leadership Meetings: The DHS Deputy Secretary hosted leadership meetings more than a dozen times throughout the review process, in order to shape the preferred approach of each study topic and to review final results. Final decisions on the recommendations reflected departmental acknowledgement of major themes around which the Quadrennial Homeland Security Review Report was written.

FEDERAL PARTNERS

Stakeholders across the Federal Government were consulted throughout the review process, culminating in a series of decisions that informed both policy and budget priorities. Federal partners received regular briefings and participated in discussions at key decision points during the review.

Legislative Branch: Staff-level briefings on Quadrennial Homeland Security Review progress were offered to all relevant committees on a variety of occasions, and provided to the House Committee on Homeland Security, the Senate Homeland Security and Governmental Affairs Committee, and the Senate Appropriations Committee. Additionally, key members and staff of relevant committees were invited to participate on the online engagement venues; several joined to monitor and participate in quadrennial review discussions. In discussions with congressional staff, their access to the ongoing online discussion was invaluable in understanding the process and results of the review. Chairman Michael McCaul (R-TX) and Ranking Member Bennie Thompson (D-MS) of the House Committee on Homeland Security also provided consolidated input to the process in

a joint letter sent to the Department in December 2013.

Executive Branch: The Quadrennial Homeland Security Review team held regular synchronization briefings with executive branch staff to remain aligned with evolving presidential policy decisions, budget priorities, and national security concerns, and to enable mutual awareness of the progress and direction of the review.

- *Interagency Policy Process:* Input from federal partners was coordinated through meetings under the National Security Council (NSC)[1] structure. Sub-Interagency Policy Committees were convened for interagency engagement and a series of Interagency Policy Committee-level briefings were used to socialize quadrennial review progress and decisions. Sub-Interagency Policy Committees were set up specifically for the Quadrennial Homeland Security Review studies on a Homeland Security Strategy for Countering Biological Threats and Hazards, Securing and Managing Flows of People and Goods, and Governance in the Homeland Security Enterprise: The Public-Private Relationship.

- *Direct Engagement with other Agencies:* In order to fulfill the requirement of consulting with other federal agencies, DHS engaged in interagency coordination through the NSC staff as well as direct bilateral meetings with interagency partners to receive interdepartmental expertise and coordinate strategy. These direct departmental meetings included discussions with the Departments of Defense, Justice, State, Health and Human Services, Veterans Affairs, Agriculture, and Treasury, as well as the Environmental Protection Agency, and the Internal Revenue Service.

- *Direct Engagement with the Executive Office of the President:* DHS engaged directly with various offices and policy council staff of the Executive Office of the President, including the NSC staff, staff from the Office of Management and Budget (OMB), and the Office of National Drug Control Policy. DHS held nearly two dozen meetings with senior NSC staff to help drive consensus throughout the strategic review process and ensured interagency coordination on key issues. DHS met monthly with OMB staff to update them on progress of the Quadrennial Homeland Security Review and the FY14-18 DHS Strategic Plan. DHS also consulted with the Office of National Drug Control Policy to confirm data related to securing and expediting flows of people and goods, and the Domestic Policy Council staff for insight on topics related to immigration.

HOMELAND SECURITY COMMUNITIES OF INTEREST

Outreach efforts focused on a cross-section of homeland security stakeholders. In order to reach the widest swath of homeland security practitioners and experts using available resources, pre-existing online venues were used as a primary mechanism for engagement. Two sites—the Quadrennial Homeland Security Review Community of Practice hosted through DHS Science and Technology's FirstResponder.gov Communities of Practice and the IdeaScale site managed by the DHS Office of Public Affairs—served as the primary interface between quadrennial review study teams and homeland security stakeholders.

Figure B-3: Stakeholder participation in IdeaScale

Stakeholder Participation in IdeaScale	
Stakeholder Group	Percentage of Users
State, Local, Tribal, Territorial Employee	27%
Private Sector	25%
Nongovernmental Organization/Non-profit	6%
Academia	9%
Federal Government	32%

In June 2013 the Secretary invited more than 200 organizations and their members, representing all facets of homeland security, to join the Quadrennial Homeland Security Review Community of Practice, which was linked to the Quadrennial Homeland Security Review IdeaScale site. This invitation garnered dynamic and enthusiastic participation throughout the entire review process from subject matter experts in the field. Their essential insights strengthened and supported the review, providing a holistic understanding of the realities of homeland security.

While the engagement process aimed to receive extensive stakeholder input, it also sought informed expertise that could be used for quadrennial review studies and analysis. To that end, the Quadrennial Homeland Security Review team reached out to:

- Hundreds of key organizations representing state, local, tribal, and territorial elected and appointed officials, and the national associations, organizations, and affiliates that represent them, the private sector, and non-profit organizations;

- Tens of thousands of practitioners through homeland security listservs managed by FEMA, DHS Intergovernmental Affairs, the Naval Postgraduate School, and the First Responder Community of Practice, among others;

- Hundreds of Federal Advisory Committee Act Committee members;
- Several international partners with interest in homeland security topics; and
- Individual organizations and experts closely related to quadrennial review study topics.

These stakeholders were targeted for extensive involvement throughout the Quadrennial Homeland Security Review study process. Study groups developed IdeaScale and Community of Practice engagement topics directly related to their analysis and stakeholders were invited to provide their thoughts and ideas. Between the two online venues, more than 2,000 unique stakeholders registered to provide their perspectives and insights, yielding thousands of comments, more than 100 source documents, and more than 10,000 votes. Stakeholders from across disciplines and from every state and several territories and tribal nations participated in these engagements. This focused and substantive input was used to inform study group analysis and helped shape the final Quadrennial Homeland Security Review Report.

To supplement this online engagement, study groups held a series of briefings and forums to solicit input and socialize the quadrennial review process with members of DHS Advisory Committees Following the 2010 review, the Government Accountability Office (GAO) noted that the review did not fully utilize Federal Advisory Committee Act groups due to a number of limitations. Specifically, it was suggested by GAO that as the limitations of Federal Advisory Committee Act "significantly reduced the role that nonfederal stakeholders played in the [Quadrennial Homeland Security Review]…addressing the [Federal Advisory Committee Act] requirements and including appropriate [Federal Advisory Committee Act]-compliant groups with a broader range of academics and others could have affected the outcome of the study group's deliberations."[2] In order to remediate this issue, PLCY's Office of Strategy, Planning, Analysis, and Risk held eight Quadrennial Homeland Security Review Forums to engage with members of DHS Federal Advisory Committee Act committees between April and December 2013. The forums allowed the Department to engage DHS's advisory committee members as individual stakeholders with relevant expertise in focused briefings. These forums did not function as Advisory Committee meetings, as the members who attended were not solicited for consensus advice or recommendations, did not speak on behalf of the Committees, and each forum consisted of different members from across the Department's Advisory Committees. When individual DHS Advisory Committees requested specific quadrennial review briefings, staff from PLCY's Office of Strategy, Planning, Analysis, and Risk provided those briefings at the

committees' regularly-scheduled and publicly-noticed meetings. DHS also engaged with specific organizations to host review-related activities, including a forum on public-private partnerships hosted by the U.S. Chamber of Commerce and a public-private partnerships tabletop exercise held in conjunction with Business Executives for National Security.

[1] In January 2014, the Assistant to the President for National Security Affairs changed the name of the integrated National Security Council and Homeland Security Council staff from the National Security Staff (NSS) to the National Security Council (NSC) staff. This appendix refers to the NSC staff, although during the conduct of the review the staff was referred to in QHSR preparatory documents as the NSS.

[2] "Quadrennial Homeland Security Review: Enhanced Stakeholder Consultation and Use of Risk Information Could Strengthen Future Reviews," GAO-11-873, September 2011, pg. 23.