Quadrennial Homeland Security Review Report:

A Strategic Framework for a Secure Homeland

February 2010

Homeland Security

TABLE OF CONTENTS

TABLE OF CONTENTS

Pursuant to the *Implementing Recommendations of the 9/11 Commission Act of 2007*, I am pleased to submit the first Quadrennial Homeland Security Review (QHSR).

Since the terrorist attacks of September 11, 2001, this Nation has recognized how remote threats and distant trouble can pose near and present dangers to our shores. We have learned as a Nation that we must maintain a constant, capable, and vigilant posture to protect ourselves against new threats and evolving hazards. But we have also learned that vigilance and protection are not ends in and of themselves, but rather necessary tools in the service of our national purpose.

Just as today's threats to our national security and strategic interests are evolving and interdependent, so too must our efforts to ensure the security of our homeland reflect these same characteristics. As we develop new capabilities and technologies, our adversaries will seek to evade them, as was shown by the attempted terrorist attack on Flight 253 on December 25, 2009. We must constantly work to stay ahead of our adversaries.

This homeland security review addresses both the threats presented and the framework for our strategic response. The QHSR identifies the importance of what we refer to as the homeland security enterprise— that is, the Federal, State, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of America and the American population. The Department of Homeland Security (DHS) is one among many components of this national enterprise. In some areas, like securing our borders or managing our immigration system, the Department possesses unique capabilities and, hence, responsibilities. In other areas, such as critical infrastructure protection or emergency management, the Department's role is largely one of leadership and stewardship on behalf of those who have the capabilities to get the job done. In still other areas, such as counterterrorism, defense, and diplomacy, other Federal departments and agencies have critical roles and responsibilities, including the Departments of Justice, Defense, and State, the Federal Bureau of Investigation, and the National Counterterrorism Center. Homeland security will only be optimized when we fully leverage the distributed and decentralized nature of the entire enterprise in the pursuit of our common goals.

The purpose of this QHSR is to outline the strategic framework to guide the activities of participants in homeland security toward a common end. With respect to DHS specifically, the QHSR has led directly to

an examination of DHS's own activities from the bottom up in order to make recommendations regarding programs, assets, and capabilities, as well as policies, authorities, and organizational effectiveness, in its fiscal year 2012 budget submission. Thus, the QHSR will be followed by subsequent submissions to Congress that address programmatic, budgetary, and organizational alignment as called for by statute. The QHSR sets the stage by describing the breadth and depth of an enterprise-wide approach to homeland security.

In preparing the QHSR, the Department has benefited from the constructive engagement of thousands of dedicated individuals from across the country and, indeed, around the globe. Although numbers alone cannot capture the depth and vibrancy of the debates and discussions that occurred throughout the process of preparing the QHSR, more than 100 stakeholder associations and more than 500 experts from government at all levels, as well as academia and the private sector, have been engaged in this process. Our online National Dialogues had more than 20,000 visits, with over 3,000 comments submitted.

The QHSR reflects the most comprehensive assessment and analysis of homeland security to date. DHS worked closely with the White House, National Security Staff, and other Federal departments and agencies to refine the QHSR and ensure consistency with the President's 2010 National Security Strategy and other major security reviews, including the Quadrennial Defense Review and the Quadrennial Diplomacy and Development Review. This interagency engagement, at the leadership and staff levels, has helped to ensure that the QHSR represents the whole-of-government approach to national security envisioned by the Obama Administration.

Indeed, every day, ensuring the security of the homeland requires the interaction of multiple Federal departments and agencies, as well as operational collaboration across Federal, State, local, tribal, and territorial governments, nongovernmental organizations, and the private sector. This collaboration and cooperation undergirds our security posture at our borders and ports, our preparedness in our communities, and our ability to effectively react to crises. The QHSR makes specific recommendations on how to strengthen and mature the homeland security enterprise, including mechanisms to enhance unity of effort across multiple homeland security partners and stakeholders.

Finally, in presenting this first-ever QHSR, I believe it is important to acknowledge the efforts and commitment of my predecessors in this office, the men and women of the Department of Homeland Security, and the many thousands of law enforcement personnel, first responders, emergency managers, and other homeland security professionals across the country who have worked tirelessly to make this Nation secure. On their behalf, and on behalf of those who continue to serve, I am pleased to deliver this first Quadrennial Homeland Security Review.

Secretary Janet Napolitano

PREFACE

The first-ever Quadrennial Homeland Security Review (QHSR) comes amid much expectation and interest. Homeland security encompasses the most sweeping reform in government in nearly half a century, and makes explicit the realization that the evolving international security landscape bears directly on our domestic security. But we have also learned that security is not an end in itself; rather, it is an important means to a vital end: preserving the values, principles, and way of life we pursue as Americans.

A review of homeland security could take many forms—from a retrospective and assessment of the past, to an analysis of current programs and activities, to a view of what the future might bring. Nonetheless, Congress made clear in its direction to the Department of Homeland Security (DHS), the principal author of this report, that the QHSR should delineate a homeland security strategy, including an outline of priority mission areas, not simply for DHS, but for the homeland security enterprise as a whole—embracing Federal, State, local, tribal, and territorial governments, nongovernmental organizations, the private sector, as well as individuals, families and communities. Such a strategic analysis would then serve as a basis for a deeper review of the many programs and budgets required to execute the full range of homeland security missions.

Congress also sought to better understand the resource and organizational implications of an evolving strategic view of homeland security. What was clear from the start, however, is that any articulation of strategy or analysis of specific programmatic or resource tradeoffs—either within DHS or across the broader homeland security enterprise—had to be firmly rooted within a comprehensive strategic understanding of homeland security. For example, "What is homeland security?" "How is the homeland best made secure?" "What does it mean to be prepared?" Eight years after 9/11, these questions still echo widely among the many homeland security stakeholders.

The QHSR marks the beginning of a multi-step process to answer these questions. It offers a vision for a secure homeland, specifies key mission priorities, outlines goals for each of those mission areas, and lays the necessary groundwork for subsequent analysis and recommendations. As an immediate follow-on and complement to the QHSR, an important "bottom-up" review of DHS was begun in November 2009 that will look to align the Department's programmatic activities and organizational structure with the mission sets and goals identified in the QHSR. That review is scheduled to be completed in the first calendar quarter of 2010.

PREFACE

While the primary purpose for the QHSR is to outline the strategic framework to guide the activities of participants in homeland security toward a common end, it is equally important to note what the QHSR is _not_. The report is not a resource prioritization document, although in identifying key mission areas for priority focus, it is highly indicative of where those priorities should lie. Nor does the QHSR detail the roles and responsibilities of Federal or other institutions for each mission area. Instead, the QHSR functions as a strategic document that seeks to answer the most fundamental questions that many Americans still ask about homeland security. By describing a forward-looking homeland security vision for the Nation and the requisite set of key mission areas, goals, objectives, and outcomes, integrated across the breadth of the homeland security landscape, it also will serve as a roadmap to keep America safe, secure, and resilient in the years ahead.

EXECUTIVE SUMMARY

The purpose of the first-ever Quadrennial Homeland Security Review (QHSR) is to outline the strategic framework to guide the activities of participants in homeland security toward a common end. A safe and secure homeland must mean more than preventing terrorist attacks from being carried out. It must also ensure that the liberties of all Americans are assured, privacy is protected, and the means by which we interchange with the world—through travel, lawful immigration, trade, commerce, and exchange—are secured.

In addition, while the importance of preventing another terrorist attack in the United States remains undiminished, much has been learned since September 11, 2001, about the range of challenges we face. Hurricane Katrina, widespread international cyber attacks, the expansion of transnational criminal activities, and H1N1 influenza are examples of threats and hazards that are central to homeland security, requiring an equally wide variety of capabilities to address them.

The QHSR is not simply a discussion of the roles and responsibilities of the Department of Homeland Security (DHS).[1] The QHSR acknowledges existing relationships, roles, and responsibilities, and seeks to set forth a shared vision of homeland security in order to achieve unity of purpose. The Nation's first QHSR takes as its aim a vision for our homeland as safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.

Today's Security Environment

The accelerated flow of ideas, goods, and people around the world, while vital to supporting and advancing America's interests, also creates security challenges that are increasingly borderless and unconventional. To a greater degree than at any point in history, individuals and small groups—from nongovernmental organizations (NGOs) on the one hand to criminal networks and terrorist organizations on the other—have the ability to engage the world with far-reaching effects, including those that are disruptive and destructive.

Among the forces that threaten the United States and its interests are those that blend the lethality and high-tech capabilities of modern weaponry with the power and opportunity of asymmetric tactics such as terrorism and cyber warfare. We are

---

[1] Section 707 of the Homeland Security Act of 2002, as amended, requires the Secretary of Homeland Security, in each quadrennial review, to "delineate and update, as appropriate, the national homeland security strategy," and to "outline and prioritize the full range of the critical homeland security mission areas of the Nation."

challenged not only by novel employment of conventional weaponry, but also by the hybrid nature of these threats. We have seen their effects on the American homeland. Moreover, we must remember that we face a determined and constantly adapting adversary. The attempted terrorist attack on Flight 253 on December 25, 2009, is a powerful illustration that terrorists will go to great lengths to try to defeat the security measures that have been put in place since 9/11.

Figure ES-1. Threats, Hazards, and Long-Term Global Challenges and Trends

Threats and Hazards	Global Challenges and Trends
• **High-consequence weapons of mass destruction** • **Al-Qaeda and global violent extremism** • **High-consequence and/or wide-scale cyber attacks, intrusions, disruptions, and exploitations** • **Pandemics, major accidents, and natural hazards** • **Illicit trafficking and related transnational crime** • **Smaller scale terrorism**	• **Economic and financial instability** • **Dependence on fossil fuels and the threats of global climate change** • **Nations unwilling to abide by international norms** • **Sophisticated and broadly available technology** • **Other drivers of illicit, dangerous, or uncontrolled movement of people and goods**

Defining and Framing Homeland Security

Homeland security describes the intersection of evolving threats and hazards with traditional governmental and civic responsibilities for civil defense, emergency response, law enforcement, customs, border control, and immigration. In combining these responsibilities under one overarching concept, homeland security breaks down longstanding stovepipes of activity that have been and could still be exploited by those seeking to harm America. Homeland security also creates a greater emphasis on the need for joint actions and efforts across previously discrete elements of government and society.

Homeland security is a widely distributed and diverse—but unmistakable—national enterprise. The term "enterprise" refers to the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities. The use of the term connotes a broad-based community with a common interest in the public safety and well-being of America and American society that is composed of multiple actors and stakeholders

EXECUTIVE SUMMARY

whose roles and responsibilities are distributed and shared. As the Commander-in-Chief and the leader of the Executive Branch, the President of the United States is uniquely responsible for the safety, security, and resilience of the Nation. The White House leads overall homeland security policy direction and coordination. Individual Federal agencies, in turn, are empowered by law and policy to fulfill various aspects of the homeland security mission. The Secretary of Homeland Security leads the Federal agency as defined by statute charged with homeland security: preventing terrorism and managing risks to critical infrastructure; securing and managing the border; enforcing and administering immigration laws; safeguarding and securing cyberspace; and ensuring resilience to disasters. However, as a distributed system, no single entity is responsible for or directly manages all aspects of the enterprise.

There are three key concepts that are essential to, and form the foundation for, a comprehensive approach to homeland security:

- **Security:** Protect the United States and its people, vital interests, and way of life;

- **Resilience:** Foster individual, community, and system robustness, adaptability, and capacity for rapid recovery; and

- **Customs and Exchange:** Expedite and enforce lawful trade, travel, and immigration.

All homeland security activities must be built upon a foundation of ensuring security and resilience, as well as facilitating the normal, daily activities of society and interchange with the world.

The Homeland Security Missions

The QHSR outlines the Nation's homeland security missions, or broad areas of activity around which the homeland security enterprise is oriented. *These missions are underlined enterprise-wide, and not limited to the Department of Homeland Security.* 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 must have a clear sense of what it takes to achieve the overarching vision.

EXECUTIVE SUMMARY

There are five homeland security missions. The missions and associated goals are as follows:

Mission 1: Preventing Terrorism and Enhancing Security

- Goal 1.1: Prevent Terrorist Attacks
- Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities
- Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events

Mission 2: Securing and Managing Our Borders

- Goal 2.1: Effectively Control U.S. Air, Land, and Sea Borders
- Goal 2.2: Safeguard Lawful Trade and Travel
- Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations

Mission 3: Enforcing and Administering Our Immigration Laws

- Goal 3.1: Strengthen and Effectively Administer the Immigration System
- Goal 3.2: Prevent Unlawful Immigration

Mission 4: Safeguarding and Securing Cyberspace

- Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment
- Goal 4.2: Promote Cybersecurity Knowledge and Innovation

Mission 5: Ensuring Resilience to Disasters

- Goal 5.1: Mitigate Hazards
- Goal 5.2: Enhance Preparedness
- Goal 5.3: Ensure Effective Emergency Response
- Goal 5.4: Rapidly Recover

In addition, we must specifically focus on maturing the homeland security enterprise itself. Maturing and strengthening the homeland security enterprise includes enhancing shared awareness of risks and threats, building capable communities, fostering unity of effort, and fostering innovative approaches and solutions through leading-edge science and technology.

By defining the homeland security missions and setting prioritized goals, objectives, and strategic outcome statements for each mission, we chart a course for action over the next 4 years.

I. INTRODUCTION

The story of homeland security is inextricably linked to the story of 9/11. The vivid images of the World Trade Center, the Pentagon, and smoldering fields in Shanksville, Pennsylvania, portrayed a Nation obviously shaken by the catastrophic surprise attacks that had occurred on its soil. Yet on that same day there were other images—of firefighters racing up the stairs of the Twin Towers, of police and first responders rushing aid to those in need at the Pentagon, and of ordinary Americans, indeed total strangers, coming together to help each other cope with challenges large and small. These images of American resilience portrayed a Nation determined to do whatever it might take to recover from this disaster and to prevent such attacks from occurring again.

In the closing days of 2001, the first narrative describing homeland security began to take shape: that despite the dramatic changes since the end of the Cold War, the world was still very much a dangerous place. The terrorists that had targeted this country clearly were determined to attack Americans at home, American interests anywhere, and our friends and allies everywhere. As the central part of this first narrative, our Nation believed that it needed to improve its vigilance, increase its preparedness, reduce its vulnerabilities, and strengthen its guard against any future attack in order to confront this threat.

The Federal Government began to institutionalize these priorities with a series of initiatives under the banner of *homeland security*: a Presidential advisor and advisory council were appointed, a series of national-level policies were issued, new statutory authorities were enacted by Congress, and in 2003, a new Federal agency was established—the Department of Homeland Security (DHS). These initiatives—in particular, the newly established DHS—linked the imperative of safeguarding the Nation to key operational responsibilities that were principally focused on securing the Nation's borders and air transportation system, while enhancing the Nation's preparedness to confront terrorism.

In the years since 9/11, homeland security has become commonly and broadly known as both a term and as a Federal department. Less well understood, however, has been its ongoing purpose and function. What is homeland security? Is it more than preventing terrorism? If so, what else does it take to achieve a safe and secure homeland? What risks are we willing to accept? Who has the responsibility, authority, capabilities, and resources to do all that needs doing?

The attempted terrorist attack on Flight 253 on December 25, 2009, demonstrates that al-Qaeda continues to plot against us, and thus, the importance of preventing another

I. INTRODUCTION

terrorist attack in the United States remains undiminished. However, much has been learned since 9/11 about the range of additional challenges we face. Hurricane Katrina powerfully illustrated the overall impact of weak preparedness and response in the face of extreme natural disasters. Widespread international cyber attacks—from some of the most sophisticated denial-of-service efforts to persistent and rising attacks on U.S. Government cyber systems—reflect the increasing importance of securing the information systems that are the very lifeblood of so much of our critical energy, financial, health, commerce, and transportation infrastructure. Transnational criminal organizations that have expanded efforts to cross our borders with illicit goods, currency, and trafficked persons represent a growing threat to the prosperity, security, and quality of life of U.S. citizens at home and abroad. As we have seen with H1N1 influenza, the rapid global spread of infectious diseases can cause great disruptions at home. Preventing these and other dangers from threatening our Nation has also become central to homeland security.

At the same time, we have learned that it is not possible to secure the American homeland simply with physical protections or through strategies that reinforce fear or isolation. Nor is this country made safe by substantially curtailing the very rights and liberties that define the free and diverse society we seek to protect, or by excluding visitors and lawful immigrants. Indeed, homeland security is as much about protecting the American way of life as it is about protecting this country from future attacks.

Thus, a safe and secure homeland must mean more than preventing terrorist attacks from being carried out. It must also ensure that the liberties of all Americans are assured, privacy is protected, and the means by which we interchange with the world—through travel, lawful immigration, trade, commerce, and exchange—are secured. Ultimately, homeland security is about effectively managing risks to the Nation's security. As such, an effective strategy for homeland security forms an important component of our overarching national security strategy.

> **"We reject as false the choice between our safety and our ideals.** Our Founding Fathers, faced with perils we can scarcely imagine, drafted a charter to assure the rule of law and the rights of man, a charter expanded by the blood of generations. Those ideals still light the world, and we will not give them up for expedience's sake."
>
> **– President Barack Obama**

I. INTRODUCTION

The purpose of this first-ever Quadrennial Homeland Security Review (QHSR) is to elaborate upon this broader vision by outlining the strategic framework to guide the activities of participants in homeland security toward a common end. And in this regard, it is important to note that this is not a review confined to the roles and responsibilities of DHS.[2] Homeland security encompasses a much broader scope, with vital contributions from all Federal agencies, State, local, tribal, and territorial governments, businesses, and nongovernmental organizations, as well as individuals, families, and communities. International partnerships are also essential to success.

Thus, this QHSR will describe more comprehensively the Nation's homeland security interests, identify more clearly the critical homeland security missions, and define more completely a strategic approach to those missions by laying out the principal goals, essential objectives, and key strategic outcomes necessary for that strategic approach to succeed. The QHSR acknowledges existing relationships and roles and responsibilities, and seeks to set forth a shared vision of homeland security in order to achieve unity of purpose going forward.

When we recall the events of 9/11, we are reminded of the destruction of those attacks to be sure. However, as we look forward from this vantage point, it is essential that we elevate the importance of the extraordinary acts that also took place when New York firefighters marched up tower stairs, when passengers of United Flight 93 stormed the cockpit and sacrificed their lives, and when countless fellow citizens across the country volunteered their time for days and months on end to help others heal. These stories of the bravery, courage, and resolve of the American people tell the story of homeland security.

These acts of courage also demonstrate the simple yet profound truth: that homeland security is not simply about government action alone, but rather about the collective strength of this entire country. The Nation's first QHSR builds on the conviction that this country can protect itself and takes as its aim a vision for our homeland as safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.

---

[2] Section 707 of the Homeland Security Act of 2002, as amended, requires the Secretary of Homeland Security, in each quadrennial review, to "delineate and update, as appropriate, the national homeland security strategy," and to "outline and prioritize the full range of the critical homeland security mission areas of the Nation."

I. INTRODUCTION

The Vision for Homeland Security

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

II. TODAY'S SECURITY ENVIRONMENT

The interconnected nature of people, economies, and international infrastructure around the world can infuse seemingly isolated or remote events with global consequences. Events at home and abroad generate rapid effects, often in an interconnected fashion, driven by breathtaking technological change and speed-of-light international communications. This accelerated flow of ideas, goods, and people around the world, while vital to supporting and advancing America's interests, also creates security challenges that are increasingly borderless and unconventional.

In many parts of the world, states no longer have a monopoly on the use of force, although they continue to hold a large majority of power. Globally, natural hazards have increased in scale and impact, and emerging diseases move effortlessly across borders and expansively through global movement systems. To a greater degree than at any point in history, individuals and small groups—from nongovernmental organizations (NGOs) on the one hand, to criminal networks and terrorist organizations on the other—have the ability to engage the world with far-reaching effects, including those that are disruptive and destructive.

Homeland security, as an essential element of our Nation's security, must be firmly embedded in and linked to broader national security concerns. Against this backdrop, we must pursue a homeland security agenda linked to America's national security interests. Such interests reflect the Nation's highest order priorities.

America's interests are inextricably linked to the integrity and resilience of the international system. Chief among these interests are security, prosperity, broad respect for universal values, and an international order that promotes cooperative action. Consistent with the President's vision, the United States will advance these interests by strengthening our domestic foundation and integrating all elements of national power, engaging abroad on the basis of mutual interest and mutual respect, and promoting an international order that reinforces the rights and responsibilities of all nations.

II. TODAY'S SECURITY ENVIRONMENT

Among the forces that threaten the United States and its interests are those that blend the lethality and high-tech capabilities of modern weaponry with the power and opportunity of asymmetric tactics such as terrorism and cyber warfare. We are challenged not only by novel employment of conventional weaponry, but also by the

> **Hybrid threats** refer to the ability of adversaries—lone attackers, criminals, transnational terrorist organizations, even nation-states—to employ combinations of tactics, technologies, and capabilities to gain an asymmetric advantage.

hybrid nature of these threats. Countering such threats requires us to adapt traditional roles and responsibilities across the national security spectrum and craft solutions that leverage the capabilities that exist both inside and outside of government. The attempted terrorist attack on Flight 253 on December 25, 2009, powerfully illustrates that terrorists will go to great lengths to try to defeat the security measures that have been put in place since 9/11.

More specifically, the threats and hazards that challenge U.S. interests from a homeland security perspective include:

- <u>High-consequence weapons of mass destruction (WMD)</u>, in particular, improvised nuclear devices and high-consequence biological weapons, which would have the greatest potential effects if used against the United States. We know that non-state actors actively seek to acquire, build, and use such weapons and technologies, and that foreign states continue to develop high-consequence weaponry with the intent to intimidate or blackmail the international community and proliferate to other potentially hostile state or non-state actors. Dangerous materials, technology, and know-how circulate with ease in our globalized economy and are controlled unevenly around the world, raising the possibility of theft or accidental use and making it difficult to track and prevent proliferation.

- <u>Al-Qaeda and global violent extremism</u>, which directly threaten the United States and its allies. Terrorist networks exploit gaps in governance and security within both weak and advanced states. Some terrorist organizations benefit from active state-sponsorship and from the failure of other states to counter known terrorist organizations or sources of support within their borders. Terrorist

> **"We will . . . relentlessly confront violent extremists** who pose a grave threat to our security— because we reject the same thing that people of all faiths reject: the killing of innocent men, women, and children."
>
> – President Barack Obama

organizations have expressed the intent to employ mass-casualty WMD as well as smaller scale attacks against prominent political, economic, and infrastructure targets in the United States and around the world.

II. TODAY'S SECURITY ENVIRONMENT

- High-consequence and/or wide-scale cyber attacks, intrusions, disruptions, and exploitations, which, when used by hostile state or non-state actors, could massively disable or impair critical international financial, commercial, physical, and other infrastructure. This in turn could cripple the global movement of people and goods worldwide and bringing legitimate and vital social and economic processes to a standstill. These cyber attacks involve individuals and groups who conduct intrusions in search of information to use against the United States, and those who spread malicious code in an attempt to disrupt the national information infrastructure.

- Pandemics, major accidents, and natural hazards, which can result in massive loss of life and livelihood equal to or greater than many deliberate malicious attacks. Certain public health threats, such as disease outbreaks and natural hazards (e.g., hurricanes and floods), occur organically. Others can be introduced into the United States through the movement of people and goods across our borders.

- Illicit trafficking and related transnational crime, which can undermine effective governance and security, corrupt strategically vital markets, slow economic growth, and destabilize weaker states. Transnational crime and trafficking facilitate the movement of narcotics, people, funds, arms, and other support to hostile actors, including terrorist networks. Importantly for the American homeland, the dramatic detrimental effect of illegal trafficking and transnational criminal organizations is apparent in societies within the Western Hemisphere.

- Smaller scale terrorism, which may include violent extremists and other state or non-state actors conducting small-scale explosive and cyber attacks and intrusions against population centers, important symbolic targets, or critical infrastructure.

In addition to these specific threats and hazards, America's national interests are also threatened by global challenges and long-term trends. These include:

- Economic and financial instability that can undermine confidence in the international order, fuel global political turbulence, and induce social and political instability in weak states abroad.

- Dependence on fossil fuels and the threat of global climate change that can open the United States to disruptions and manipulations in energy supplies and to changes in our natural environment on an unprecedented scale. Climate change is expected to increase the severity and frequency of weather-related hazards, which could, in turn, result in social and political destabilization, international conflict, or mass migrations.

II. TODAY'S SECURITY ENVIRONMENT

- <u>Nations unwilling to abide by international norms</u> that can threaten U.S. security interests directly or indirectly by sponsoring terrorism, encouraging WMD proliferation, serving as a source of cyber disruptions, committing human rights atrocities, or providing safe haven to transnational criminal networks.

- <u>Sophisticated and broadly available technology</u>, which empowers our adversaries. We must adapt our intelligence and counterintelligence practices to defeat hostile operations and the use of intelligence tradecraft by small groups and individuals planning destructive attacks against the homeland.

- <u>Other drivers of illicit, dangerous, or uncontrolled movement of people and goods</u>, including fragile and failing states, regional instability, competition for resources, demographic shifts, environmental degradation, genocide, and other gross violations of human rights. These same drivers can also foster terrorism and violent extremist ideology, breed transnational crime, and facilitate the proliferation of high-consequence weaponry.

The national security of the United States depends on a comprehensive approach to preserve and advance our interests while managing the risks posed by the threats outlined above. An effective strategy for homeland security forms an important component of our overarching national security strategy, and three assumptions in particular shape its development.

First, rapid technological change will continue to alter social, economic, and political forces, rapidly disperse information, and provide new means for our adversaries and competitors to challenge us. The increasing interconnectivity of infrastructure and its dependence on cyber systems creates opportunities for adversaries to use cyber tools to attack critical infrastructure and gain access to government, business, and personal information systems. Second, multiple simultaneous crises will likely challenge the Nation and its resources, requiring all stakeholders to be capable of managing crises including some for extended periods. Multiple simultaneous crises will also place a premium on all stakeholders' knowledge of and ability to use incident management protocols and procedures, and will challenge national priority setting and resource allocation demands. Finally, we must guard against the danger of complacency as memories of the 9/11 attacks and other major crises recede. The failed airline plot of December 25, 2009, serves to heighten our vigilance, but we know that readiness is costly and requires sustained commitment.

II. TODAY'S SECURITY ENVIRONMENT

Assumptions Concerning the Security Environment

- **Violent extremist groups**, including potential homegrown extremists, will continue to use terrorism to attack U.S. targets;

- Technologies associated with WMD, often dual-use, will circulate easily in a globalized economy, challenging traditional **WMD nonproliferation and counterproliferation efforts**, especially in the nuclear and biological areas;

- Terrorists, proliferators, and other criminal elements will seek to take advantage of the **increasingly globalized financial system** and its legitimate and beneficial functions to move money in support of their dangerous conduct;

- Economic crises and disparities will continue to induce social and/or political instability, in some cases increasing **migrant and refugee flows— legal and illegal—into the United States**;

- Globalization will continue to make it increasingly difficult to prevent **health threats to the United States**, whether from emerging disease or deliberate attacks, or via imports;

- **Technological change and cyber threats** from state and non-state actors will continue to alter social, economic, and political forces, allow for the rapid dissemination of information, and provide new means for adversaries to challenge the United States;

- **Climate change** will increase the severity and frequency of weather-related hazards such as extreme storms, high rainfalls, floods, droughts, and heat waves;

- The security environment will continue to pose the potential for **multiple simultaneous crises**; and

- There is a danger of **complacency** as major crises recede.

This page intentionally left blank.

III. DEFINING AND FRAMING HOMELAND SECURITY

Because the term is in such widespread use, it may be easy today to overlook the fact that *homeland security* is a relatively new concept. Yet it is one that can trace its roots to traditional functions such as civil defense, emergency response, law enforcement, customs, border control, and immigration. Homeland security captures the effort to adapt these traditional functions to confront new threats and evolving hazards.

While homeland security is still relatively new, it may be useful to recall that the concept of *national security* was also little known until the 1930s, and was only formally established as an organizing principle after World War II. The *National Security Act of 1947* brought together the Department of War and the Department of the Navy into a single integrated entity that became the Department of Defense. The act also created the National Security Council and a position on the President's staff that would later become the National Security Advisor. The innovation was to bring together under one overall concept the consideration of foreign affairs and military policy, which had been, up until that time, two largely separate governmental domains. Over the decades, aspects of economic policy, trade policy, energy policy, and countering transnational threats were also drawn into the ambit of national security.

In 2002, the *Homeland Security Act* sought to integrate the various elements of homeland security in a similar manner, creating both the Department of Homeland Security and the Homeland Security Council. In effect, the 2002 *Homeland Security Act* added a third concept to the military and foreign affairs pillars of national security by associating domestic security concerns with national security.

Homeland security describes the intersection of evolving threats and hazards with the traditional governmental and civic responsibilities of civil defense, emergency response, law enforcement, customs, border control, and immigration. In combining these responsibilities under one overarching concept, homeland security breaks down longstanding stovepipes of activity that could be exploited by those seeking to harm America. Homeland security also creates a greater emphasis on and need for joint actions and efforts across previously discrete elements of government and society.

III. DEFINING AND FRAMING HOMELAND SECURITY

The Homeland Security Enterprise

Given this historical context, the question "What is homeland security?" recognizes that, in fact, securing the United States and its people represents an overarching national objective. Equally important, and aside from obviously identifying a Cabinet-level department of the Federal Government, homeland security is a widely distributed and diverse—but unmistakable—national enterprise.

The term "enterprise" refers to the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities. It

> ## The homeland security "enterprise"
>
> refers to the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities. It connotes a broad-based community with a common interest in the safety and well-being of America and American society.

connotes a broad-based community with a common interest in the public safety and well-being of America and American society and is composed of multiple partners and stakeholders whose roles and responsibilities are distributed and shared. Yet it is important to remember that these partners and stakeholders face diverse risks, needs, and priorities. The challenge for the enterprise, then, is to balance these diverse needs and priorities, while focusing on our shared interests and responsibilities to collectively secure our homeland.

As the Commander-in-Chief and the leader of the Executive Branch, the President of the United States is uniquely responsible for the safety, security, and resilience of the Nation. The White House leads overall homeland security policy direction and coordination. Individual Federal agencies, in turn, are empowered by law and policy to fulfill various aspects of the homeland security mission. The Secretary of Homeland Security leads the Federal agency as defined by statute charged with homeland security: preventing terrorism and managing risks to critical infrastructure; securing and managing the border; enforcing and administering immigration laws; safeguarding and securing cyberspace; and ensuring resilience to disasters. In some areas, like securing our borders or managing our immigration system, the Department of Homeland Security possesses unique capabilities and, hence, responsibilities. In other areas, such as critical infrastructure protection or emergency management, the Department's role is largely one of leadership and stewardship on behalf of those who have the capabilities to get the job done. In still other areas, such as counterterrorism, defense, and diplomacy, other Federal

III. DEFINING AND FRAMING HOMELAND SECURITY

departments and agencies have critical leadership roles and responsibilities, including the Departments of Justice, Defense, and State, the Federal Bureau of Investigation, and the National Counterterrorism Center. State, local, tribal, and territorial governments all play vital roles in protecting the homeland. Homeland security will only be successful when we fully leverage the distributed and decentralized nature of the entire enterprise in the pursuit of our common goals.

Therefore, key leadership responsibilities to achieve our homeland security missions are discharged through engagement and collaboration with the vast array of homeland security enterprise partners and stakeholders. As a distributed system, no single entity is responsible for or directly manages all aspects of the enterprise. Different agencies and offices direct and lead specific homeland security activities at the Federal, State, local, tribal, and territorial levels, as well as within the private sector—and between and among all of these entities—for the full range of homeland security purposes. And because responsibilities are distributed, entities that provide direction and leadership in one instance may play supporting roles in another. **Appendix A** reflects the current alignment of roles and responsibilities across the enterprise.

With the establishment of homeland security, and the linking of domestic security concerns to broader national security interests and institutions, there is a temptation to view homeland security so broadly as to encompass all national security and domestic policy activities. This is not the case. Homeland security is deeply rooted in the security and resilience of the Nation, and facilitating lawful interchange with the world. As such, it intersects with many other functions of government. Homeland security is built upon critical law enforcement functions, but is not about preventing all crimes or administering our Nation's judicial system. It is deeply embedded in trade activities, but is neither trade nor economic policy. It requires international engagement, but is not responsible for foreign affairs. Rather, homeland security is meant to connote a concerted, shared effort to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.

> *Homeland security is a concerted national effort to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.*

III. DEFINING AND FRAMING HOMELAND SECURITY

The Evolution of Homeland Security

As noted earlier, although the integrated concept of homeland security arose at the turn of the 21st century, homeland security traces its roots to concepts that originated with the founding of the Republic. Homeland security describes the intersection of new threats and evolving hazards with traditional governmental and civic responsibilities for civil defense, emergency response, customs, border control, law enforcement, and immigration. Homeland security draws on the rich history, proud traditions, and lessons learned from these historical functions to fulfill new responsibilities that require the engagement of the entire homeland security enterprise and multiple Federal departments and agencies.

Figure 1. The Evolution of Homeland Security

Traditional Responsibilities

Maritime Security
Foreign Agricultural Threats
Aviation Security
Land Border Security
Transportation Security
Leadership Protection
Financial System Security
Trade Facilitation
Migration Security
Emergency Management
Immigration Administration and Enforcement
Intelligence and Law Enforcement

New Threats and Evolving Hazards

Weapons of Mass Destruction
Global Terrorism
Cyber Attacks
Pandemics and Natural Disasters
Illegal Trafficking and Related Transnational Crime
Smaller Scale Terrorism

Core Homeland Security Mission Areas

Preventing Terrorism and Enhancing Security
Securing and Managing Our Borders
Enforcing and Administering Our Immigration Laws
Safeguarding and Securing Cyberspace
Ensuring Resilience to Disasters

The Key Concepts of Homeland Security

For the past 7 years, homeland security has rested on four key activities—prevention, protection, response, and recovery—oriented principally against the threat of terrorism. Preventing a terrorist attack in the United States remains the cornerstone of homeland security. It is clear, however, that this emphasis on terrorism does not capture the full range of interconnected threats and challenges that characterize today's world. A robust notion of homeland security must take account of our essential need to safely, securely, and intensively engage the rest of the world—through trade, travel, and other exchanges. In other words, a place where the American way of life can thrive.

Three key concepts form the general foundation for a comprehensive approach to homeland security going forward: Security, Resilience, and Customs and Exchange.

III. DEFINING AND FRAMING HOMELAND SECURITY

Security: Protect the United States and its people, vital interests, and way of life. Homeland security relies on our shared efforts to prevent and deter attacks by identifying and interdicting threats, denying hostile actors the ability to operate within our borders, and protecting the Nation's critical infrastructure and key resources. Initiatives that strengthen our protections, increase our vigilance, and reduce our vulnerabilities remain important components of our security. This is not to say, however, that security is a static undertaking. We know that the global systems that carry people, goods, and data around the globe also facilitate the movement of *dangerous* people, goods, and data, and that within these systems of transportation and transaction, there are key nodes—for example, points of origin and transfer, or border crossings—that represent opportunities for interdiction. Thus, we must work to confront threats at every point along their supply chain—supply chains that often begin abroad. To ensure our homeland security then, we must engage our international allies, and employ the full breadth of our national capacity—from the Federal Government, to State, local, tribal, and territorial police, other law enforcement entities, the Intelligence Community, and the private sector—and appropriately enlist the abilities of millions of American citizens.

> **"The terrorists have used our open society against us.** In wartime, government calls for greater powers, and then the need for those powers recedes after the war ends. This struggle will go on. Therefore, while protecting our homeland, Americans should be mindful of the threats to vital personal and civil liberties. This balancing is no easy task, but we must constantly strive to keep it right. This shift of power and authority to the government calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life."
>
> – The 9/11 Commission Report

Resilience: Foster individual, community, and system robustness, adaptability, and capacity for rapid recovery. Our country and the world are underpinned by interdependent networks along which the essential elements of economic prosperity—people, goods and resources, money, and information—all flow. While these networks reflect progress and increased efficiency, they are also sources of vulnerability. The consequences of events are no longer confined to a single point; a disruption in one place can ripple through the system and have immediate, catastrophic, and multiplying consequences across the country and around the world.

Despite our best efforts, some attacks, accidents, and disasters will occur. Therefore, the challenge is to foster a society that is robust, adaptable, and has the capacity for rapid recovery. In this context, individuals, families, and communities—and the systems that sustain them—must be informed, trained, and

III. DEFINING AND FRAMING HOMELAND SECURITY

materially and psychologically prepared to withstand disruption, absorb or tolerate disturbance, know their role in a crisis, adapt to changing conditions, and grow stronger over time.

> **"Our goal** is to ensure a more resilient Nation—one in which individuals, communities, and our economy can adapt to changing conditions as well as withstand and rapidly recover from disruption due to emergencies."
>
> – President Barack Obama

This concept is not new, and different eras in our history reflect an unwavering focus on building national resilience. The history of civil defense in the United States, for example, is marked by sweeping national debates about concepts that, if not by name, were nevertheless entirely about resilience. Notable among these was the debate spanning the Truman and Eisenhower administrations about whether to expend resources on sheltering individuals in the face of nuclear attack or to focus investments in a national highway system to facilitate mass evacuation of urban populations. These issues were beset with the same challenges that confront us today, including how to foster a decentralized approach to security, and how to best meet the challenge of helping our citizens prepare psychologically and materially for attacks and disasters that do occur. The rapid evolution of national security threats and the arrival of the information age have increased the urgency of building up—and reemphasizing—our historically resilient posture.

Customs and Exchange: Expedite and enforce lawful trade, travel, and immigration. The partners and stakeholders of the homeland security enterprise are responsible for facilitating and expediting the lawful movement of people and goods into and out of the United States. This responsibility intersects with and is deeply linked to the enterprise's security function. We need a smarter, more holistic approach that embeds security and resilience directly into global movement systems. Strengthening our economy and promoting lawful trade, travel, and immigration must include security and resilience, just as security and resilience must include promoting a strong and competitive U.S. economy, welcoming lawful immigrants, and protecting civil liberties and the rule of law. We view security along with customs and exchange as mutually reinforcing and inextricably intertwined through actions such as screening, authenticating, and maintaining awareness of the flow of people, goods, and information around the world and across our borders.

III. DEFINING AND FRAMING HOMELAND SECURITY

Customs in Historical Context

After declaring independence, the United States found itself on the brink of bankruptcy. To raise revenue, the second act of Congress—the *Tariff Act of 1789*—authorized the first Secretary of the Treasury, Alexander Hamilton, to collect duties on imported goods. A month later, in its fifth act, Congress established 59 customs collection districts around the country and designated ports of entry under the jurisdiction of the Department of the Treasury's Collectors of Customs.

From inception, the Collectors of Customs were given numerous responsibilities designed to support the collection of customs revenue. Recognizing that revenue would increase if more ships could make it to port safely and quickly, Congress immediately created the Lighthouse Service, which eventually came under Collectors of Customs authority, to construct and maintain all navigational aids. To assist in the collection of duties and tonnage taxes, and to combat smuggling by privateers, which negatively impacted revenue collection, a maritime law enforcement arm was added a year later—the U.S. Revenue Marine. As the Nation's land borders expanded, the U.S. Customs Border Patrol was created to address smuggling between ports of entry.

The Collectors of Customs were assigned other tasks that were inherently intertwined with their customs responsibilities. Because their ships already patrolled the coastline, the Revenue Marine assumed responsibility for maritime security and, in the 1840s with its acquisition of the Life Saving Service, maritime safety. The Collectors of Customs were also charged with implementing immigration policy and enforcing immigration law, because they were representatives of the Federal Government at ports of entry. By 1853, the Collectors of Customs had authority over customs and immigration law enforcement, maritime safety and security, and border security.

Beginning in the late 1800s, however, the Collectors of Customs structure was reorganized. In 1871, the Revenue Marine (which had been renamed the Revenue Cutter Service) and Life Saving Service were removed from Collectors of Customs authority. The two organizations combined in 1915 to form the U.S. Coast Guard. In 1891, Congress moved the Collectors' immigration functions to the Office of the Superintendent of Immigration, which later evolved into the Immigration and Naturalization Service. By the turn of the century, the Collectors of Customs (eventually renamed the U.S. Customs Service) had become an organization focused solely on customs enforcement and antismuggling. Around the same time, growing income from excise taxes and, in 1913, an income tax meant that customs duties were no longer the primary source of Federal Government revenue.* The facilitation of commerce and immigration in support of overall economic growth became a substantial priority alongside the collection of customs revenue.

For the next 100 years, customs and immigration enforcement, border security, and maritime safety and security functions remained distributed across multiple agencies within three cabinet departments—the Department of the Treasury (customs), the Department of Justice (immigration enforcement and border security), and the Department of Transportation (maritime safety and security). The creation of the Department of Homeland Security (DHS) in 2003 reunited these long interrelated and mutually supportive functions. Every day as part of DHS, the U.S. Coast Guard, U.S. Customs and Border Protection, Transportation Security Administration, U.S. Citizenship and Immigration Services, and U.S. Immigration and Customs Enforcement undertake countless activities to expedite and facilitate the flow of goods and people across U.S. borders. As these agencies have previously done—in some cases for hundreds of years—they ensure seamless integration of these responsibilities with the task of upholding and promoting the security of the country.

* Today, customs revenue remains second only to internal revenue taxes as the most significant source of Federal revenue, totaling over $30B annually.

This page intentionally left blank.

IV. Overview of the Homeland Security Missions

The vision of homeland security is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.

As noted earlier, three key concepts form the foundation of our national homeland security strategy designed to achieve this vision: Security, Resilience, and Customs and Exchange. In turn, these key concepts drive broad areas of activity that the QHSR process defines as homeland security missions. *These missions are* _enterprise-wide, and not limited to the Department of Homeland Security._ These missions and their associated goals and objectives tell us in detail what it means to prevent, to protect, to respond, and to recover, as well as to build in security, to ensure resilience, and to facilitate customs and exchange. 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 are the people who regularly interact with the public, who are responsible for public safety and security, who own and operate our Nation's critical infrastructures and services, who perform research and develop technology, and who keep watch, prepare for, and respond to emerging threats and disasters. These homeland security professionals must have a clear sense of what it takes to achieve the overarching vision articulated above.

The Core Missions

There are five homeland security missions:

1. Preventing terrorism and enhancing security;
2. Securing and managing our borders;
3. Enforcing and administering our immigration laws;
4. Safeguarding and securing cyberspace; and
5. Ensuring resilience to disasters.

In addition, we must specifically focus on maturing and strengthening the homeland security enterprise itself.

IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

For each mission, the following discussion, supported with additional material set forth in Section V, details specific goals and objectives that outline what is required for success. These mission goals and objectives reflect the considered analysis conducted through the QHSR process. This analysis included literature reviews, subject-matter expert consultation, public comment, and testing of conclusions against preliminary analytic models. **Appendix B** provides an overview of the QHSR process. The goals and objectives set the stage for developing and applying risk management tools to establish programmatic priorities, develop more specific performance measures, and pursue greater integrated planning across the homeland security enterprise.

IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

MISSION 1: PREVENTING TERRORISM AND ENHANCING SECURITY

Preventing a terrorist attack in the United States remains the cornerstone of homeland security. Our vision is a secure and resilient Nation that effectively prevents terrorism in ways that preserve our freedom and prosperity. Achieving this vision requires us to focus on the core goal of preventing terrorist attacks, highlighting the challenges of preventing attacks using chemical, biological, radiological, and nuclear (CBRN) weapons and managing risks to critical infrastructure.

We must be vigilant against the use of terrorist tactics employed by malicious actors seeking to harm the United States. Thus, a key element of preventing terrorism is to understand not only the threat that currently confronts us—for example, the terrorist use of explosives—but also evolving and emerging threats. We must actively monitor those threats and put them in an appropriate context so we can apply the most effective threat mitigation strategies possible, including understanding how best to protect against terrorist capabilities and deter and disrupt operations of those who would use terrorist tactics to advance their aims. We must develop a comprehensive understanding of the threats and malicious actors that have the desire and ability to harm the United States. These include individuals, terrorist organizations, hostile foreign intelligence services, those seeking to proliferate weapons of mass destruction, and criminal enterprises. Beyond these efforts, however, we must also stop the spread of violent extremism. In this regard, it is important that we actively engage communities across the United States.

> **"We are at war against al-Qaeda,** a far-reaching network of violence and hatred that attacked us on 9/11, that killed nearly 3,000 innocent people, and that is plotting to strike us again. And we will do whatever it takes to defeat them."
>
> – President Barack Obama

CBRN weapons, especially high-consequence nuclear and biological weapons, pose a particular challenge to our security. We must anticipate emerging CBRN threats, control both access to and movement of CBRN, and expand and strengthen our capabilities to detect, protect against, and deter hostile use.

In addition, we must effectively manage terrorist-based as well as other risks to critical infrastructure. The security and resilience of the critical systems, services, and resources that sustain our daily lives are vital to ensuring that our Nation continues to prosper and thrive. We must deepen our understanding of the nature of the risks to these infrastructures and effectively prioritize our efforts to reduce vulnerabilities. In addition to protecting infrastructure and critical facilities and

IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

networks, we must also work to make critical infrastructure resilient, including not only stand-alone facilities, but also interdependent systems and networks within and across critical infrastructure sectors.

Finally, one of America's underlying strengths is the ability of the democratic process to withstand the test of time and persevere regardless of efforts to disrupt it. Ensuring the continuity of government and government operations, and protecting our national leaders, is essential to preserving the framework established in the Constitution.

These mission goals and objectives reflect the continued primary importance placed on preventing terrorism. They also reflect a continuing emphasis regarding CBRN materials and technologies, as well as critical infrastructure and key resources. The mission goals and objectives set forth here reflect the President's emphasis on preventing introduction and use of high-consequence weapons of mass destruction, the continued fight against al-Qaeda, and the imperative to increase not only security but also resilience of America's critical infrastructure and key resources.

As noted earlier, the nature of the homeland security enterprise demands that these goals are executed in the context of extensive collaboration at every level of the homeland security enterprise through cooperation with State, local, tribal, and territorial governments, nongovernmental entities, and the private sector.

IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

Preventing Terrorism and Enhancing Security
Mission Goals and Objectives

Goal 1.1: Prevent Terrorist Attacks: Malicious actors are unable to conduct terrorist attacks within the United States.

Objectives

- **Understand the threat:** Acquire, analyze, and appropriately share intelligence and other information on current and emerging threats.
- **Deter and disrupt operations:** Deter, detect, and disrupt surveillance, rehearsals, and execution of operations by terrorists and other malicious actors.
- **Protect against terrorist capabilities:** Protect potential targets against the capabilities of terrorists, malicious actors, and their support networks to plan and conduct operations.
- **Stop the spread of violent extremism:** Prevent and deter violent extremism and radicalization that contributes to it.
- **Engage communities:** Increase community participation in efforts to deter terrorists and other malicious actors and mitigate radicalization toward violence.

Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities: Malicious actors, including terrorists, are unable to acquire or move dangerous chemical, biological, radiological, and nuclear materials or capabilities within the United States.

Objectives

- **Anticipate emerging threats:** Identify and understand potentially dangerous actors, technologies, and materials.
- **Control access to CBRN:** Prevent terrorists and other malicious actors from gaining access to dangerous materials and technologies.
- **Control movement of CBRN:** Prevent the illicit movement of dangerous materials and/or technologies.
- **Protect against hostile use of CBRN:** Identify the presence of and effectively locate, disable, or prevent the hostile use of CBRN.

Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events: Key sectors actively work to reduce vulnerability to attack or disruption.

Objectives

- **Understand and prioritize risks to critical infrastructure:** Identify, attribute, and evaluate the most dangerous threats to critical infrastructure and those categories of critical infrastructure most at risk.
- **Protect critical infrastructure:** Prevent high-consequence events by securing critical infrastructure assets, systems, networks, or functions—including linkages through cyberspace—from attacks or disruption.
- **Make critical infrastructure resilient:** Enhance the ability of critical infrastructure systems, networks, and functions to withstand and rapidly recover from damage and disruption and adapt to changing conditions.
- **Protect government leaders, facilities, and special events.** Preserve continuity of government and ensure security at events of national significance.

IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

MISSION 2: SECURING AND MANAGING OUR BORDERS

A safe and secure homeland requires that we maintain effective control of our air, land, and sea borders. Secure, well-managed borders must not only protect the United States against threats from abroad; they must they must also expedite the safe flow of lawful travel and commerce. Achieving this vision requires that we focus on three interrelated goals.

First, we must achieve effective control of the physical borders and approaches to the United States. Achieving this aim means not only that we are able to prevent the illegal entry of inadmissible persons and contraband and the illegal exit of dangerous goods, proceeds of crime, and malicious actors, but also that we can securely expedite the cross-border flow of lawful immigration, travel, and commerce at our borders. Indeed, these "twin goals" mutually reinforce each other. The more we use technology, information, and training to support operations that identify and expedite lawful travel and commerce across our borders, the more officials at the border can focus on the known threats that require more scrutiny. We must and can achieve *both* greater security and greater interchange with the world.

Second, to secure our Nation, we must work together to look beyond our borders to identify and disrupt threats well before they reach our shores. Accordingly, we must work with our international partners and with the private sector to prevent the exploitation of the interconnected trading, transportation, and transactional systems that move people and commerce throughout the global economy and across our borders. At the same time, we must also work with those same partners to ensure the security and resilience of those systems in order to expedite and reduce unnecessary encumbrances to lawful travel and trade that may impair economic vitality. America must remain open for business and exchanges with the world, must remain true to its principles of privacy, civil rights, and civil liberties, and must be welcoming of lawful visitors and immigrants.

> "**We will strengthen our defenses, but we will not succumb to a siege mentality** that sacrifices the open society and liberties and values that we cherish as Americans, because great and proud nations don't hunker down and hide behind walls of suspicious and mistrust. That is exactly what our adversaries want…"
>
> – President Barack Obama

Third, achieving this vision also requires disrupting and dismantling transnational criminal and terrorist organizations that smuggle or traffic people, illicit goods, or the proceeds of crime across the U.S. border, and commit violent acts. Transnational criminal and terrorist organizations present a dual threat that must be countered. These organizations seek to exploit lawful movement systems for

IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

harmful or dangerous purposes while also seeking to establish alternative illicit pathways through which people and illegal goods—from narcotics to terrorists to illicit funds to dangerous weaponry—can cross U.S. borders. These organizations may also intend to destabilize governments, commit violence, and intimidate innocent people. In order to secure our homeland, therefore, we must also focus on disrupting and dismantling these organizations that seek to exploit the global trade and travel systems that transcend and permeate our borders.

The inclusion of border security and management in its entirety represents an evolution of thinking in homeland security, beyond simply border security. This approach to border security and management also recognizes that while aviation security, maritime security, and land border security are all critical elements of homeland security, we must consider these elements together as an integrated set of concerns, so as not to allow stovepipes and divisions to develop between our security approaches within each of these domains of activity. Moreover, the three-pronged approach set forth here goes beyond the traditional concern with the border itself. This approach emphasizes securing lawful trade and travel through global movement systems, to prevent actions like the attempted terrorist attack on Flight 253 on December 25, 2009, which used the lawful global travel system as a vector for attack. This approach also focuses on disrupting criminal and terrorist organizations that engage in smuggling and trafficking across the U.S. border. These organizations exploit our lawful trade and travel systems for malicious ends, and create illicit smuggling and trafficking pathways that present a threat to our security and economic well-being.

This three-pronged approach to securing and managing our borders can only be achieved by cooperative efforts among Federal departments and agencies, our international partners, and global transnational private-sector partners to establish secure and resilient global trading, transportation, and transactional systems that facilitate the flow of lawful travel and commerce. This approach also depends on partnerships with Federal, State, local, tribal, territorial, and international law enforcement agencies to share information and conduct coordinated and integrated operations. In working together, we are safer, stronger, and can more effectively achieve our shared vision of secure, well-managed borders that protect our people, expedite lawful travel and commerce, and preserve our freedoms and way of life.

IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

Securing and Managing Our Borders
Mission Goals and Objectives

Goal 2.1: Effectively Control U.S. Air, Land, and Sea Borders: Prevent the illegal flow of people and goods across U.S. air, land, and sea borders while expediting the safe flow of lawful travel and commerce.

Objectives

- **Prevent illegal entry:** Prevent the illegal entry of people, weapons, dangerous goods, and contraband, and protect against cross-border threats to health, food, environment, and agriculture, while facilitating the safe flow of lawful travel and commerce.
- **Prevent illegal export and exit:** Prevent the illegal export of weapons, proceeds of crime, and other dangerous goods, and the exit of malicious actors.

Goal 2.2: Safeguard Lawful Trade and Travel: Ensure security and resilience of global movement systems.

Objectives

- **Secure key nodes:** Promote the security and resilience of key nodes of transaction and exchange within the global supply chain.
- **Secure conveyances:** Promote the safety, security, and resilience of conveyances in the key global trading and transportation networks.
- **Manage the risk posed by people and goods in transit.**

Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations: Disrupt and dismantle transnational organizations that engage in smuggling and trafficking across the U.S. border.

Objectives

- **Identify, disrupt, and dismantle transnational criminal and terrorist organizations:** Disrupt transnational criminal or terrorist organizations involved in cross-border smuggling, trafficking, or other cross-border crimes, dismantle their infrastructure, and apprehend their leaders.
- **Disrupt illicit pathways:** Identify, disrupt, and dismantle illicit pathways used by transnational criminal and terrorist organizations.

IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

MISSION 3: ENFORCING AND ADMINISTERING OUR IMMIGRATION LAWS

Virtually all Americans are affected by our immigration system. A fair and effective immigration system enriches American society, unifies families, and promotes our security. Conversely, persistent problems in immigration policy can consume valuable resources needed to advance other security objectives, undermine confidence in the rule of law, and make it harder to focus on the most dangerous threats facing our country. In short, the success of our Nation's immigration policy plays a critical role in advancing homeland security, and our overall homeland security policy must be implemented in a manner that supports an immigration system that succeeds in advancing American interests.

At the heart of any Nation's immigration regime is the imperative to know who lives and works within its national borders. Immigration policy must deter immigration violations, help eliminate the conditions that foster illegal immigration, and improve system efficiency, fairness, and integrity. This vision reflects an emphasis on both immigration enforcement and immigration services, allowing the government to efficiently facilitate lawful immigration while identifying and removing those who violate our laws. Finally, the integration of lawful immigrant communities into American society is central to establishing a safe and secure homeland where all Americans can thrive. The American tradition of welcoming lawful immigrants is not merely a reflection of America's founding values—it also provides national and community benefits in increased security and prosperity.

Successful immigration management will require a unified approach that employs shared policy and priorities, a common understanding and respect for stakeholder roles, as well as improved sharing of information and analysis. As part of this process, the United States must establish effective laws and policies to govern the immigration system.

The strategic aims and objectives set forth below address the key factors needed to promote legal immigration, combat illegal immigration, and effectively administer and enforce our immigration laws.

Enforcing and Administering Our Immigration Laws
Mission Goals and Objectives

Goal 3.1: Strengthen and Effectively Administer the Immigration System: Promote lawful immigration, expedite administration of immigration services, and promote the integration of lawful immigrants into American society.

Objectives

- **Promote lawful immigration:** Clearly communicate to the public information on immigration services and procedures.
- **Effectively administer the immigrations services system:** Create a user-friendly system that ensures fair, consistent, and prompt decisions.
- **Promote the integration of lawful immigrants into American society:** Provide leadership, support, and opportunities to immigrants to facilitate their integration into American society and foster community cohesion.

Goal 3.2: Prevent Unlawful Immigration: Reduce conditions that encourage foreign nationals to illegally enter and remain in the United States, while identifying and removing those who violate our laws.

Objectives

- **Reduce demand:** Eliminate the conditions that encourage illegal employment.
- **Eliminate systemic vulnerabilities:** Prevent fraud, abuse, and exploitation, and eliminate other systemic vulnerabilities that threaten the integrity of the immigration system.
- **Prevent entry or admission:** Prevent entry or admission of criminals, fugitives, other dangerous foreign nationals, and other unauthorized entrants.
- **Arrest, detain, prosecute, and remove:** Arrest, detain, prosecute, and remove criminal, fugitive, dangerous, and other unauthorized foreign nationals consistent with due process and civil rights protections.

IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

MISSION 4: SAFEGUARDING AND SECURING CYBERSPACE

Our economic vitality and national security depend today on a vast array of interdependent and critical networks, systems, services, and resources. We know this interconnected world as *cyberspace*, and without it we cannot communicate, travel, power our homes, run our economy, or obtain government services. Its benefits are tremendous.

Yet as we migrate ever more of our economic and societal transactions to cyberspace, these benefits come with increasing risk. Not only is cyberspace inherently insecure as built, but as a Nation we face a variety of adversaries who are working day and night to use our dependence on cyberspace against us. Sophisticated cyber criminals and nation-states, among others, are among the actors in cyberspace who now pose great cost and risk both to our economy and national security. They exploit vulnerabilities in cyberspace to steal money and information, and to destroy, disrupt, or threaten the delivery of critical services.

For this reason, safeguarding and securing cyberspace has become one of the homeland security community's most important missions. Our vision is a cyberspace that supports a secure and resilient infrastructure, that enables innovation and prosperity, and that protects privacy and other civil liberties by design. It is one in which we can use cyberspace with confidence to advance our economic interests and maintain national security under all conditions.

We will achieve this vision by focusing on two goals: (1) helping to create a safe, secure, and resilient cyber environment; and (2) promoting cybersecurity knowledge and innovation. We must enhance public awareness and ensure that the public both recognizes cybersecurity challenges and is empowered to address them. We must create a dynamic cyber workforce across government with sufficient capacity and expertise to manage current and emerging risks. We must invest in the innovative technologies, techniques, and procedures necessary to sustain a safe, secure, and resilient cyber environment. Government must work creatively and collaboratively with the private sector to identify solutions that take into account both public and private interests, and the private sector and academia must be fully empowered to see and solve ever larger parts of the problem set. Finally, because cybersecurity is an exceedingly dynamic field, we must make specific efforts to ensure that the Nation is prepared for the cyber threats and challenges of tomorrow, not only of today. To do this, we must promote cybersecurity knowledge and innovation. Innovation in technology, practice, and policy must further protect—not erode—privacy and civil liberties.

Safeguarding and Securing Cyberspace
Mission Goals and Objectives

Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment: Ensure malicious actors are unable to effectively exploit cyberspace, impair its safe and secure use, or attack the Nation's information infrastructure.

Objectives

o **Understand and prioritize cyber threats:** Identify and evaluate the most dangerous threats to Federal civilian and private-sector networks and the Nation.
o **Manage risks to cyberspace:** Protect and make resilient information systems, networks, and personal and sensitive data.
o **Prevent cyber crime and other malicious uses of cyberspace:** Disrupt the criminal organizations and other malicious actors engaged in high-consequence or wide-scale cyber crime.
o **Develop a robust public-private cyber incident response capability:** Manage cyber incidents from identification to resolution in a rapid and replicable manner with prompt and appropriate action.

Goal 4.2: Promote Cybersecurity Knowledge and Innovation: Ensure that the Nation is prepared for the cyber threats and challenges of tomorrow.

Objectives

o **Enhance public awareness:** Ensure that the public recognizes cybersecurity challenges and is empowered to address them.
o **Foster a dynamic workforce:** Develop the national knowledge base and human capital capabilities to enable success against current and future threats.
o **Invest in innovative technologies, techniques, and procedures:** Create and enhance science, technology, governance mechanisms, and other elements necessary to sustain a safe, secure, and resilient cyber environment.

IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

MISSION 5: ENSURING RESILIENCE TO DISASTERS

Despite ongoing vigilance and efforts to protect this country and its citizens, major accidents and disasters, as well as deliberate attacks, will occur. The challenge is to build the capacity of American society to be resilient in the face of disruptions, disasters, and other crises. Our vision is a Nation that understands the hazards and risks we face; is prepared for disasters; can withstand the disruptions disasters may cause; can sustain social trust, economic, and other functions under adverse conditions; can manage itself effectively during a crisis; can recover quickly and effectively; and can adapt to conditions that have changed as a result of the event.

The strategic aims and objectives for this mission are grounded in the four traditional elements of emergency management: hazard mitigation, enhanced preparedness, effective emergency response, and rapid recovery. Together, these elements create the resilience to disasters so necessary to the functioning and prosperity of this Nation.

Achieving resilience will require a significant change in U.S. emergency management from a primary focus on response and recovery to one that takes a wider view, balancing response and recovery with mitigation and preparedness. In addition, we must more fully incorporate a comprehensive understanding of risk to establish priorities and inform decisionmaking. Resilience will also require a shift from a reliance on top-down emergency management to a process that engages all stakeholders—local, tribal, territorial, and State governments, Federal departments and agencies, as well as nongovernmental organizations, the private sector, and individuals, families, and communities.

Disasters, by their very nature, occur locally—in communities very often far removed from Federal assets. The elements of the homeland security enterprise geared toward responding to disasters are thus widely distributed. Experience shows that the first line of defense rests with individuals, families, and communities, who must take responsibility for their own safety and must be prepared to respond to and possibly endure a crisis when disaster strikes. State, local, territorial, and tribal responders will usually be the first official presence on the scene, while the Federal Government will provide support when effective response exceeds their capabilities. Nongovernmental organizations are also key partners and provide essential humanitarian and relief services, while the private sector is responsible for the economic welfare of areas affected by disasters and for much of the Nation's critical infrastructure.

Disasters such as 9/11 and Hurricane Katrina have demonstrated that despite occurring in specific locations, catastrophes have national consequences whose burdens we all share. Disasters have also illustrated the ability and importance of

IV. Overview of the Homeland Security Missions

communities to come together to help one another through difficult times and of effective information sharing and situational awareness. The strategic aims and objectives for this mission reinforce the importance of the traditional emergency management activities—preparing individuals, communities, organizations, and governments to be able to respond to and recover from all threats and hazards—but also advance the importance of taking a more holistic approach when considering these activities to ensure greater resilience in our communities and for our Nation.

IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

Ensuring Resilience to Disasters **Mission Goals and Objectives**

Goal 5.1: Mitigate Hazards: Strengthen capacity at all levels of society to withstand threats and hazards.

Objectives

- o **Reduce the vulnerability of individuals and families:** Improve individual and family capacity to reduce vulnerabilities and withstand disasters.
- o **Mitigate risks to communities:** Improve community capacity to withstand disasters by mitigating known and anticipated hazards.

Goal 5.2: Enhance Preparedness: Engage all levels and segments of society in improving preparedness.

Objectives

- o **Improve individual, family, and community preparedness:** Ensure individual, family, and community planning, readiness, and capacity-building for disasters.
- o **Strengthen capabilities:** Enhance and sustain nationwide disaster preparedness capabilities, to include life safety, law enforcement, information sharing, mass evacuation and shelter-in-place, public health, mass care, and public works.

Goal 5.3: Ensure Effective Emergency Response: Strengthen response capacity nationwide.

Objectives

- o **Provide timely and accurate information to the public:** Establish and strengthen pathways for clear, reliable, and current emergency information, including effective use of new media.
- o **Conduct effective disaster response operations:** Respond to disasters in an effective and unified manner.
- o **Provide timely and appropriate disaster assistance:** Improve governmental, nongovernmental, and private-sector delivery of disaster assistance.

Goal 5.4: Rapidly Recover: Improve the Nation's ability to adapt and rapidly recover.

Objectives

- o **Enhance recovery capabilities:** Establish and maintain nationwide capabilities for recovery from major disasters.
- o **Ensure continuity of essential services and functions:** Improve capabilities of families, communities, private-sector organizations, and all levels of government to sustain essential services and functions.

IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

This QHSR has drawn on our Nation's experience in the years since 9/11 to highlight the importance of joining efforts across all levels of society and government in a common homeland security enterprise. Looking forward, and as we consider the evolution of homeland security and this enterprise, we recognize that the enterprise itself requires active stewardship. In this regard, we have identified several key areas for strengthening: shared awareness of risks and threats; community capability and readiness; unity of effort across all participants in the homeland security enterprise; and innovation through active application of leading-edge science and technology.

The effort to strengthen the homeland security enterprise must begin with an evolution in how we think about homeland security itself. All of the most advanced, high-tech tools in the world will not transform our security unless we change our way of thinking, the way we approach individual, family, and community preparedness, the way we organize, train, and equip our professional capabilities, and the way all of these elements interact. Today, we must counter myriad threats that range from hostile aircraft entering our airspace to people carrying backpacks to suspicious packages left on subways. For other hazards—major accidents, natural disasters—we must be better able to respond to crises, while recognizing that the Federal Government will not always serve as the primary lead. We must also find better ways to mitigate common hazards and reduce systemic vulnerabilities.

We must shorten the cycles of identifying possible threats to addressing them—whether by interdicting hostile actors, stopping dangerous cargoes, or detecting releases of deadly chemical or biological weapons and quickly providing antidotes or treatments. This means building greater real-time, shared threat information analysis and situational awareness. It means aggressively identifying, countering, and defeating hostile intelligence activities against the homeland. It also means building stronger, more capable communities to address threats before they manifest themselves and to shorten the crisis-to-care timelines following a disaster.

We must avoid stovepipes that hinder appropriate information sharing and analysis, and we must foster greater information sharing without undermining privacy protections or civil liberties. Moving from a top-down, command and control model to a more bottom-up approach in homeland security will require greater dynamic coordination—where individuals, communities, and other stakeholders at all levels understand their roles and are empowered with information, resources, and the capability to be part of our national effort to protect ourselves.

IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

We must also strengthen communities so that they have the information, training, and equipment they need to respond effectively in the immediate face of a warning or crisis event. Creating capable communities will require that we establish clear standards for readiness, promulgate accurate and timely information to communicate risks, make opportunities for training, education, and exercises available, and ensure that critical capabilities—such as effective interoperable communications—are in place and functional. Achieving this goal will demand active partnering among all levels of government.

In addition, there is a need to enhance the skills and abilities of homeland security professionals as part of the larger national security professional development effort, expand the partnerships upon which the homeland security enterprise depends, develop technologies that support the achievement of homeland security mission goals and objectives, and institutionalize processes that will support effective and informed decisionmaking and unity of effort within the enterprise. Each of these aims strengthens decisionmaking, identification of priorities, and successful execution of the homeland security missions.

The strategic aims and objectives for maturing and strengthening the homeland security enterprise are drawn from the common themes that emerge from each of the homeland security mission areas. Ensuring shared awareness of risks and threats, building capable communities, creating unity of effort, and enhancing the use of science and technology underpin our national efforts to prevent terrorism and enhance security, secure and manage our borders, enforce and administer our immigration laws, safeguard and secure cyberspace, and ensure resilience to disasters.

IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

Maturing and Strengthening the Homeland Security Enterprise
Goals and Objectives

Enhance Shared Awareness of Risks and Threats: Establish a comprehensive system for building and sharing awareness of risks and threats.

Objectives
- o **Establish an approach to national-level homeland security risk assessments:** Develop and implement a methodology to conduct national-level homeland security risk assessments.
- o **Share information and analysis:** Enhance critical tools and institutionalize arrangements for effective, timely sharing of information and analysis.
- o **Screen and verify identity:** Establish a robust approach to identity verification that safeguards individual privacy and civil rights.
- o **Enhance domain awareness:** Ensure shared situational awareness in the air, land, and maritime domains.
- o **Integrate counterintelligence:** Use and integrate counterintelligence in all aspects of homeland security to thwart attacks against the homeland.
- o **Establish a common security mindset:** Promote a common understanding of security and threat awareness as a shared responsibility.

Build Capable Communities: Foster communities that have information, capabilities, and resources to prevent threats, respond to disruptions, and ensure their own well-being.

Objectives
- o **Set capability and capacity standards:** Identify core capability and capacity targets to guide homeland security investments and activities across the enterprise.
- o **Enhance systems for training, exercising, and evaluating capabilities.**
- o **Maintain and sustain equipment and capabilities:** Promote smart investment in operational capabilities.

Foster Unity of Effort: Foster a broad national culture of cooperation and mutual aid.

Objectives
- o **Build a homeland security professional discipline:** Develop the homeland security community of interest at all levels of government as part of a cadre of national security professionals.
- o **Promote regional response capacity:** Promote mutual aid agreements for response requirements that exceed local capacity.
- o **Institutionalize homeland security planning:** Develop a planning system to execute homeland security activities.
- o **Further enhance the military-homeland security relationship:** Strengthen unity of effort between military and civilian activities for homeland security.
- o **Strengthen the ability of Federal departments and agencies to support homeland security missions**
- o **Expand and extend governmental and private sector international partnerships:** Transform how government and the private sector interact.
- o **Mature the Department of Homeland Security:** Improve DHS's organizational and programmatic alignment and its management systems and processes.

Foster Innovative Approaches and Solutions Through Leading-Edge Science and Technology: Ensure scientifically informed analysis and decisions are coupled to innovative and effective technological solutions.

Objectives
- o **Scientifically study threats and vulnerabilities:** Pursue a rigorous scientific understanding of current and future threats to homeland security and the possible means to their prevention and mitigation.
- o **Develop innovative approaches and effective solutions:** Encourage and enable innovative approaches to critical homeland security challenges, fostering collaborative efforts involving government, academia, and the private sector.

V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

This section elaborates the goals and objectives for each of the five homeland security missions, as well as for maturing and strengthening the homeland security enterprise. As noted above, these missions and their associated goals and objectives tell us in detail what it means to prevent, to protect, to respond, and to recover, as well as to build in security, to ensure resilience, and to facilitate customs and exchange. These missions are <u>enterprise-wide</u>, and not limited to the Department of Homeland Security. Five selected strategic outcomes are identified for each mission, along with key actions for each of the mission objectives.

Mission 1: Preventing Terrorism and Enhancing Security

- Goal 1.1: Prevent Terrorist Attacks
- Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities
- Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events

Mission 2: Securing and Managing Our Borders

- Goal 2.1: Effectively Control U.S. Air, Land, and Sea Borders
- Goal 2.2: Safeguard Lawful Trade and Travel
- Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations

Mission 3: Enforcing and Administering Our Immigration Laws

- Goal 3.1: Strengthen and Effectively Administer the Immigration System
- Goal 3.2: Prevent Unlawful Immigration

Mission 4: Safeguarding and Securing Cyberspace

- Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment
- Goal 4.2: Promote Cybersecurity Knowledge and Innovation

Mission 5: Ensuring Resilience to Disasters

- Goal 5.1: Mitigate Hazards
- Goal 5.2: Enhance Preparedness
- Goal 5.3: Ensure Effective Emergency Response
- Goal 5.4: Rapidly Recover

V. Missions, Goals, and Objectives of Homeland Security

Mission 1: Preventing Terrorism and Enhancing Security

Preventing terrorism in the United States is the cornerstone of homeland security. Ensuring that malicious actors cannot conduct terrorist attacks within the United States, preventing the illicit or hostile use of chemical, biological, radiological, and nuclear (CBRN) materials or capabilities within the Unites States, and managing risks to our critical infrastructure and key resources helps us realize our vision of a secure and resilient Nation.

Key Strategic Outcomes
- Acts of terrorism against transportation systems are thwarted prior to successful execution.   - The manufacture, storage, or transfer of dangerous materials is protected by physical, personnel, and cybersecurity measures commensurate with the risks.   - Any release of high-consequence biological weapons is detected in time to protect populations at risk from the release.   - Critical infrastructure sectors adopt and sector partners meet accepted standards that measurably reduce the risk of disrupting public health and safety, critical government services, and essential economic activities.   - Governmental executive leadership is protected from hostile acts by terrorists and other malicious actors.

Goal 1.1: Prevent Terrorist Attacks

Malicious actors are unable to conduct terrorist attacks within the United States. Success in achieving this goal rests on our ability to strengthen public- and private-sector activities designed to counter terrorist efforts to plan and conduct attacks. Success also depends on strengthening our ability to investigate and arrest perpetrators of terrorist crimes and to collect intelligence that will help prevent future terrorist activities.

Objectives

- **Understand the threat: Acquire, analyze, and appropriately share intelligence and other information on current and emerging threats.** Homeland security partners require a shared understanding of the current and emerging threats from terrorists and other malicious actors to inform the development of risk management strategies. As has long been recognized, information and intelligence regarding emerging threats must be collected,

V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

analyzed, and disseminated appropriately and promptly. Homeland security partners must use compatible information architecture and data standards where possible to maximize the acquisition, access, retention, production, use, management, and appropriate safeguarding of this information.

- **Deter and disrupt operations: Deter, detect, and disrupt surveillance, rehearsals, and execution of operations by terrorists and other malicious actors.** We must deter and disrupt malicious actors and dismantle support networks at every step of their operations. This objective also includes identifying and disrupting efforts to corrupt cyber or movement systems, breach confidentiality, or deny authorized access. Prompt and appropriate law enforcement and legal action against perpetrators and dismantling of their support networks will mitigate hostile actions.

- **Protect against terrorist capabilities: Protect potential targets against the capabilities of terrorists, malicious actors, and their support networks to plan and conduct operations.** We must be able to protect against the capabilities that malicious actors might use to conduct terrorism against the United States. This objective includes detecting, disrupting, and preventing the ability of malicious actors intent on using terrorism to train, plan, travel, finance their operations, communicate, and acquire weapons—including high-yield explosives. We must protect against the full range of these capabilities in order to reduce the likelihood of a successful attack against the United States.

- **Stop the spread of violent extremism: Prevent and deter violent extremism and radicalization that contributes to it.** Reducing violent extremism will frustrate terrorist efforts to recruit operatives, finance activities, and incite violence. In particular, efforts must focus not only at the community level, but also on cyberspace.

- **Engage communities: Increase community participation in efforts to deter terrorists and other malicious actors and mitigate radicalization toward violence.** Individual citizens and cohesive communities are key partners in the homeland security enterprise and have an essential role to play in countering terrorism. Mechanisms for identifying and reporting suspicious activities must be made clear and accessible. Moreover, enhanced public preparedness and effective warning systems can empower communities, help minimize fear, and diminish the effectiveness of terrorist tactics.

V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

Goal 1.2: Prevent the Unauthorized Acquisition or Use of CBRN Materials and Capabilities

---

Malicious actors, including terrorists, are unable to acquire or move dangerous chemical, biological, radiological, and nuclear materials or capabilities within the United States. Although the Nation remains committed to preventing all attacks by terrorists and other malicious actors, certain chemical, biological, radiological, and nuclear attacks pose a far greater potential to cause catastrophic consequences. Consequently, particular attention must be paid to the security of dangerous chemical, biological, radiological, and nuclear materials and technologies.

Objectives

- **Anticipate emerging threats: Identify and understand potentially dangerous actors, technologies, and materials.** It is incumbent upon us to identify changing capabilities *before* their first use so that appropriate risk management strategies can be developed and executed. Homeland security partners must identify, characterize, and have timely and appropriate information and analysis on emerging and potentially dangerous technologies and materials. Information and analysis on emerging threats must be appropriately and effectively shared among homeland security partners.

- **Control access to CBRN: Prevent terrorists and other malicious actors from gaining access to dangerous materials and technologies.** American industry transforms raw materials and technologies into economic progress, but in the wrong hands, such materials and capabilities pose critical threats to public health and safety. Controlling access to CBRN materials and technologies is an essential step in preventing their illicit use. Access to these materials and technologies must be limited to legitimate users. Industries that manufacture, store, or sell potentially dangerous materials, and experts with knowledge of their use, must maintain awareness of the status of CBRN materials and technologies and assume responsibility for their security and control. Personnel surety programs must be strengthened. Finally, the manufacturing, storage, and transfer of dangerous materials must be protected by physical and cybersecurity measures commensurate with the risks they pose.

- **Control movement of CBRN: Prevent the illicit movement of dangerous materials and technologies.** Should malicious actors obtain CBRN, attacks can be prevented or deterred if movement of CBRN is more effectively controlled. Differentiating between the licit and illicit movement of dangerous materials and technologies will require the cooperation of public- and private-sector homeland

security enterprise partners to ensure such materials and technologies are secure and accounted for, and their movement is known to appropriate authorities. Terrorists and other malicious actors must be impeded in their ability to move dangerous materials, technologies, and expertise into, within, or out of the United States through appropriate screening, detection, and inspection regimes, and through efforts to prevent the financing of their activities.

- **Protect against hostile use of CBRN:** I**dentify the presence of and effectively locate, disable, or prevent the hostile use of CBRN.** Measures must be in place to discover the presence of CBRN, as well as to rapidly apply the technology and expertise necessary to locate, disable, or otherwise prevent use of CBRN weapons.

Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events

---

Key sectors actively work to reduce vulnerability to attack or disruption. The American way of life depends upon the effective functioning of the Nation's critical infrastructure and key resources, and the protection of key leadership and events. Although considerable advances have been made in identifying critical infrastructure assets and systems, and understanding the current, emerging, and future risks to those infrastructures, the breadth of the infrastructure, its increasing reliance on cyberspace, and its criticality necessitates continued diligence.

Objectives

- **Understand and prioritize risks to critical infrastructure: Identify, attribute, and evaluate the most dangerous threats to critical infrastructure and those categories of critical infrastructure most at risk.** Homeland security partners and stakeholders need a shared understanding of the risks to and the interdependencies that connect the Nation's critical

> **Homeland security includes the unique responsibility of protecting the President of the United States**, the Vice President, visiting heads of state, and the Presidential campaign process, as well as ensuring the continuity of national leadership. At the Federal level, the U.S. Secret Service assumed this responsibility after the assassination of President William McKinley in 1901. At the State, local, tribal, and territorial levels, law enforcement agencies and protective services provide similar functions.

infrastructure and key resources. Homeland security partners must provide and receive information and assessments on current and emerging risks in time to carry out their risk management responsibilities, while enjoying access to the data, tools, and expertise to make informed risk management decisions. Acquisition, access, retention, production, use, and management of threat and risk information must be maximized through compatible information architecture and data standards. Risk management decisions made by homeland security partners must account for interdependencies across sectors and jurisdictions.

- **Protect critical infrastructure: Prevent high-consequence events by securing critical infrastructure assets, systems, networks, or functions— including linkages through cyberspace—from attacks or disruption.** Homeland security partners must be aware of the risk profiles of and risk management strategies for critical infrastructure, to include key governmental sites that have national symbolic importance as well as serve as vital functions to our democratic institutions. Measures to control, and in some cases deny, access to critical infrastructure assets, systems, and networks must be consistently implemented, upgraded, and enforced. These measures must also continuously adapt based on an improved understanding of changing threats and risks. Additionally, business processes and infrastructure operations must be changed or revised and technologies incorporated to reduce the risk of high-consequence events.

- **Make critical infrastructure resilient: Enhance the ability of critical infrastructure systems, networks, and functions to withstand and rapidly recover from damage and disruption and adapt to changing conditions.** The Nation cannot rely on protection strategies alone to ensure the continuity of critical functions, particularly those necessary for public health and safety. Homeland security partners must develop, promulgate, and update guidelines, codes, rules, regulations, and accepted standards when appropriate, that measurably reduce the risk of damage and disruption to critical functions, networks, and systems, and ensure their resilience. Design of new infrastructure and infrastructure improvements must anticipate change in the risk environment, incorporate lessons from past events and exercises, and consider and build in security and resilience from the start. Finally, a skilled workforce with sufficient capacity and expertise is necessary in order to ensure the functionality of critical infrastructure.

V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

- **Protect governmental leaders, facilities, and special events: Preserve continuity of government and ensure security at events of national significance.** Preserving continuity of government is essential to the stability of the Nation. Detecting, disrupting, and responding to crises under any contingency requires collaboration throughout the homeland security enterprise. Identifying, analyzing, and disseminating protective intelligence information pertaining to individuals, groups, and technologies that pose a danger to our Nation's leadership and visiting heads of state and government is imperative to safeguarding our Nation's interests. So too is actual protection of government facilities. In addition, Federal, State, local, tribal, and territorial homeland security partners execute operational security plans that ensure the safety of American citizens at events of national significance. Homeland security stakeholders play a critical role in the execution of layered security measures to address the threat spectrum. Developing and fostering critical coalitions such as task forces, fusion centers, and working groups reinforces strategic investigative alliances, aids in identifying patterns and trends, and allows sharing of emerging technologies, systems, and methodologies.

V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

MISSION 2: SECURING AND MANAGING OUR BORDERS

A safe and secure homeland requires that we maintain effective control of our air, land, and sea borders; that we safeguard lawful trade and travel; and that we disrupt transnational organizations that engage in smuggling and trafficking across the U.S. border. This three-pronged approach to securing and managing our borders can only be achieved by working with partners from across the homeland security enterprise to establish secure and resilient global trading, transportation, and transactional systems that facilitate the flow of lawful travel and commerce. This approach also depends on partnerships with Federal, State, local, tribal, territorial, and international law enforcement agencies to share information and conduct coordinated and integrated operations. In working together, we can more effectively achieve our shared vision and preserve our freedoms and way of life.

Key Strategic Outcomes

- The entry or approach of all high-consequence WMD and related materials and technologies is prevented.

- Terrorists and other high-risk individuals are prevented from using commercial or noncommercial transportation destined for the United States.

- The identity of all individuals who are encountered at U.S. borders and in global movement systems entering the United States is verified.

- Individuals with known ties to terrorism or transnational criminal activities are not granted access to secure areas within the global movement system.

- No highly dangerous pathogens or organisms are introduced across U.S. borders.

Goal 2.1: Effectively Control U.S. Air, Land, and Sea Borders

Prevent the illegal flow of people and goods across U.S. air, land, and sea borders while expediting the safe flow of lawful travel and commerce. Key to achieving secure and well-managed borders are the broad legal authorities utilized by trained officers to conduct appropriate searches, seizures, arrests, and other key enforcement activities. These security and enforcement activities are balanced, however, by the need to facilitate the lawful transit of people and goods across our borders. Through the collection, analysis, and proper sharing of information, the use of screening and identification verification techniques, the employment of advanced detection and other technologies, the use of "trusted traveler" or "trusted shipper" approaches, and cooperation with our international partners and the private sector,

V. Missions, Goals, and Objectives of Homeland Security

we can achieve security at our borders, enforce the laws, and ensure our prosperity and freedom by speeding lawful travel and commerce.

Objectives

- **Prevent illegal entry: Prevent the illegal entry of people, weapons, dangerous goods, and contraband, and protect against cross-border threats to health, food, environment, and agriculture, while facilitating the safe flow of lawful travel and commerce.** Central to the mission of controlling our borders is preventing the illegal entry of dangerous persons, contraband, or other illicit goods—whether they are terrorists, highly dangerous weapons, illicit drugs, dangerous pathogens, invasive species, or counterfeit software. Preventing illegal entry must be accomplished both at official ports of entry—in concert with facilitating the safe flow of lawful travel and commerce—and in the long stretches between these points, as well as along our maritime borders and across our air boundaries. We must substantially increase situational awareness at our borders and approaches in order to help detect and classify potential threats and effectively resolve them. We must positively identify individuals encountered to determine their risk to the country, and expedite the collection, sharing, and analysis of all relevant information so that border officers can make accurate security determinations, reduce unknowns in the system, and expedite low-risk individuals and commerce. We must enhance measures aimed at deterring illegal migration and contraband smuggling, thereby reducing "pull" factors that draw unlawful migrants and dangerous goods. Finally, we must build on our existing partnerships with our North American neighbors in order to collaboratively address threats to the continent and approaches and more effectively expedite and secure the lawful flow of travel and commerce within the North American community.

- **Prevent illegal export and exit: Prevent the illegal export of weapons, proceeds of crime, and other dangerous goods, and the exit of malicious actors.** Gaining control of the borders also means gaining better control of what leaves our country. Indeed, violent international drug trafficking organizations are fueled by the proceeds of drug sales smuggled out of the United States, and armed by weapons, some of which are obtained in this country and smuggled across our borders. Hostile and criminal actors seek to smuggle weapons, weapons components, bulk cash, and controlled technologies out of the United States, as well as seek U.S.-based financing for their activities. To address these threats, relevant authorities must identify and assess the risk of all commercial cargo exiting the United States through official channels, and known or suspected terrorists or criminals must be prevented from departing the United

V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

States. Additionally, outbound smuggling must be reduced through collaboration with international and private-sector partners, both at home and overseas. Finally, authorities throughout the homeland security enterprise must identify, share, and act upon information to prevent all known or suspected terrorists and wanted criminals from leaving the United States or seeking to enter neighboring countries.

Goal 2.2: Safeguard Lawful Trade and Travel

Ensure security and resilience of global movement systems. The global economy is increasingly a seamless economic environment connected by systems and networks that transcend national boundaries. The United States is deeply linked to other countries through the flow of goods and services, capital and labor, and information and technology into and across our borders. As much as these global systems and networks are critical to the United States and our prosperity, their effectiveness and efficiency also make them attractive targets for exploitation by our adversaries, terrorists, and criminals. Thus, border security cannot begin simply at our borders. The earlier we can identify, understand, interdict, and disrupt plots and illegal operations, the safer we will be at home. In other words, our borders should not be our first line of defense against global threats. This premise demands a focus on using our national leverage to build partnerships to secure key nodes and conveyances in the global trading and transportation networks, as well as to manage the risks posed by people and goods in transit. Moreover, U.S. national interests—in a competitive U.S. economy and a stable global trading system—require us to work with international partners and the private sector to secure global movement systems. These same national interests are also served by ensuring the free, lawful movement of people and commerce through the global economy and across U.S. borders in a manner that does not impair economic vitality, while at the same time safeguarding privacy, civil rights, and civil liberties.

Objectives

- **Secure key nodes: Promote the security and resilience of key nodes of transaction and exchange within the global supply chain.** A variety of actors are involved in the complex process of moving goods and people through the global supply chain from origin to final destination. Each nodal transfer—such as from one international airport or seaport to another, or from one entity to the next—presents adversaries with a new opportunity to introduce a threat into the global supply chain or exploit this system for their own purposes. These key nodes and exchange points must be secured from threats and made able to withstand disruption. In addition, advance information and sophisticated

V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

analytic capabilities must be used to reduce unknowns in the system, so that interventions can focus on identified threats or higher risks. Finally, the U.S. Government must work with its international partners and the private sector to build on existing efforts to develop, strengthen, and implement international standards for securing the key systems of the global economy and more effectively facilitating the flow of lawful travel and commerce throughout the world and across U.S. borders.

- **Secure conveyances: Promote the security and resilience of conveyances in the key global trading and transportation networks.** A key component of global movement systems are the conveyances—the forms of transit used to move people and goods from a point of origin toward a final destination—and the operators in that system, including air carriers, cruise ship operators, exporters, cargo carriers, importers, manufacturers, and longshoremen, among others. Operators and the conveyances used to move people and goods from an origin toward a final destination must be identified and determined not to pose a threat to the United States or the larger global movement system. In addition, operators must ensure against the misuse of equipment or transportation that would allow for the introduction of dangerous or illegal contents into the system. Finally, conveyances or shipments approaching or entering the United States through a port of entry must be assessed to determine if they may legally enter the United States, or whether they should be subject to additional inspection, if deemed a potential threat or if authorities otherwise believe appropriate.

- **Manage the risk posed by people and goods in transit.** People seeking to come to the United States, as well as goods in transit, must be positively identified and determined not to pose a threat to this country or the larger global movement system as far in advance as possible. For movement of people, this assessment can be performed early through visa processes, online application for travel authorization, and advance provision of passenger biographical information, in order to expedite the flow of international travel. For movement of goods, the assessment is ideally done well before shipment to the United States, or even earlier in the supply chain, in conjunction with private-sector entities and international partners. Identifying people and goods that pose minimal risk as early in the process as possible and securely expediting their travel to and through the United States also facilitates the flow of lawful travel and commerce and reduces friction in the global economy. Supporting networks to share information and analysis regarding people and goods must be robust and effective while protecting privacy and civil liberties. Enhanced global

standards for information collection and sharing increase the effectiveness of these risk assessment efforts. These activities are key to ensuring the safe, lawful flow of commerce, reducing processing times for individuals and goods seeking lawful entry to the country, and ensuring that the United States remains open for business to the world and welcoming of international visitors.

Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations

---

Disrupt and dismantle transnational organizations that engage in smuggling and trafficking across the U.S. border. We have also learned in the years since 9/11 that it is not enough to simply interdict trouble at the border or enhance the protection of global systems for trade and travel. Criminals, terrorist networks, and other malicious actors will seek to exploit the same interconnected systems and networks of the global economy for nefarious purposes, or create their own illicit pathways for smuggling and trafficking—of illegal drugs, illegal migrants, terrorists, or even highly dangerous weapons. When these organizations or actors are successful, they also may increase corruption and engage in a wide variety of other criminal activities such as money laundering, bulk cash smuggling, and intellectual property crime, which threaten the rule of law, potentially endanger lives, and generate wider destabilization. Thus, our border strategy must also focus on reducing the power and capability of these transnational criminal and terrorist organizations.

Objectives

- **Identify, disrupt, and dismantle transnational criminal and terrorist organizations: Disrupt transnational criminal or terrorist organizations involved in cross-border smuggling, trafficking, or other cross-border crimes, dismantle their infrastructure, and apprehend their leaders.** Identifying, disrupting, and dismantling criminal and terrorist organizations transcends any one Federal agency, State, local, tribal, or territorial law enforcement agency, or Intelligence Community partner. Success will require many key activities. First, all relevant information held by authorities concerning known or suspected terrorists, criminals, illicit organizations and networks, and inadmissible foreign nationals must be appropriately shared among agencies so malicious actors are interdicted by authorities. Working together, the operations of the major transnational criminal and terrorist organizations must be disrupted, and supporting organizations, networks, and infrastructure must be substantially dismantled. The leaders of these organizations must be apprehended and brought to justice.

V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

- **Disrupt illicit pathways: Identify, disrupt, and dismantle illicit pathways used by criminal and terrorist organizations.** In addition to exploiting lawful systems for global travel and trade, criminal and terrorist organizations create their own illegal pathways for smuggling and trafficking people and goods across international borders. While these routes and conveyances may be used today to transport illicit narcotics or facilitate illegal migration, the same routes may also be used to smuggle terrorists and their tools and finances, or even highly dangerous weapons and materials. Working appropriately with domestic law enforcement partners, the Intelligence Community, and foreign partners, we must identify these illicit pathways, understand their nodes and conveyances, monitor their use, and effectively intervene to stop dangerous people or goods in transit and dismantle the pathways themselves.

V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

MISSION 3: ENFORCING AND ADMINISTERING OUR IMMIGRATION LAWS

A fair and effective immigration system must protect the public while also enriching American society and promoting economic prosperity. At the same time, it must also deter immigration violations, work to eliminate the conditions that foster illegal immigration, and improve the efficiency, fairness, and integrity of our immigration system.

Key Strategic Outcomes
• The identities of individuals seeking immigration services are verified at first contact and throughout the immigration process. • All workers are verified as legally authorized to work in the United States. • Real-time information, data, trends, and intelligence on terrorist or criminal organizations and individuals are accessible to all Federal immigration partners. • Criminal organizations and individuals are prevented from transporting, housing, or harboring illegal aliens. • All communities that are home to immigrant populations have programs that effectively integrate immigrants into American civic society.

Goal 3.1: Strengthen and Effectively Administer the Immigration System

Promote lawful immigration, expedite administration of immigration services, and promote the integration of lawful immigrants into American society. Effective administration of the immigration system depends on ensuring that immigration decisions are fair, lawful, and sound; that the immigration system is interactive and user friendly; that policy and procedural gaps are systematically identified and corrected; and that vulnerabilities that would allow persons to exploit the system are eliminated. In addition, effectively administering the immigration system includes efforts to integrate lawful immigrants into American society.

Objectives

• **Promote lawful immigration: Clearly communicate with the public about immigration services and procedures.** Lawful immigration contributed greatly to the building of America and continues to enrich our society, our economy, and our way of life. Promoting lawful immigration requires transparent procedures and sustained efforts to inform the public about immigration programs and policies. Thus, to promote lawful immigration, all

appropriate information regarding immigration programs, eligibility requirements, application instructions, and status updates must be available to external users through multiple user-friendly avenues, including an interactive, Web-based portal. Feedback from stakeholders must be obtained and assessed in an integrated manner, and solutions, current policies, and policy changes must be clearly communicated to stakeholders and to the public.

- **Effectively administer the immigration services system: Create a user-friendly system that ensures fair, consistent, and prompt decisions.** Applications for immigration services must be efficiently and effectively received and managed. All information needed to make immigration decisions must be available to appropriate agencies electronically and in real-time, including active individual case files and biometric information. In addition, gaps and inconsistencies in policies and procedures must be identified and corrected, while policy guidance must be effectively communicated to the field. Finally, policy implementation must be evaluated to ensure compliance and consistency in the field.

- **Promote the integration of lawful immigrants into American society: Provide leadership, support, and opportunities to lawful immigrants to facilitate their integration into American society and foster community cohesion.** Homeland security partners and stakeholders must work collectively to provide strategies that respect newcomers while encouraging and assisting eligible immigrants to naturalize. Communities that are home to lawful immigrants must have the necessary tools to engage lawful immigrants in civic activities and community issues. New lawful immigrant communities should be encouraged to become an integral part of American life. For their part, new lawful immigrants must obey all applicable laws and take affirmative steps to fully join their new society. This includes learning English and the civic principles that form the foundation of responsible citizenship.

> **Promoting integration** reinforces a resilient public where all people belong, are secure in their rights, are confident to exercise their civil liberties, and have opportunities to be full participants in America. The integration process ensures a stronger and more cohesive American society by inviting newcomers from every background to share in our core beliefs and be able to embrace the rights and responsibilities of citizenship.

V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

Goal 3.2: Prevent Unlawful Immigration

Reduce conditions that encourage foreign nationals to illegally enter and remain in the United States, while identifying and removing those who violate our laws. To prevent illegal immigration, all agencies charged with immigration administration and enforcement activities must address conditions and factors that create incentives for those illegally entering and staying within the United States. This effort includes identifying the conditions and addressing gaps in current laws, policies, and procedures that foster illegal immigration. Enforcement efforts must prioritize the identification and removal of dangerous foreign nationals who threaten our national security or the safety of our communities and must include safe and humane detention conditions and respect for due process and civil rights as accorded by law.

Objectives

- **Reduce demand: Eliminate the conditions that encourage illegal employment.** Reducing demand for unauthorized workers is essential to preventing illegal immigration. An employment eligibility verification system is critical in identifying employers whose business model depends on the abuse of workers without legal status. This verification system must be implemented with appropriate regard to privacy and civil rights. Furthermore, only a strong enforcement program that identifies and punishes employers who knowingly employ unauthorized workers as part of their business model will serve as an effective deterrent. Developing a collaborative, interagency approach to bring the combined authorities and enforcement resources of Federal, State, local, tribal, and territorial partners to target abusive employers will reduce demand for unauthorized workers by increasing the penalties against those who exploit them.

- **Eliminate systemic vulnerabilities: Prevent fraud, abuse, and exploitation, and eliminate other systemic vulnerabilities that threaten the integrity of the immigration system.** Systemic vulnerabilities that threaten the integrity of the immigration system must be eliminated by identifying and targeting system deficiencies and the root causes of system misuse. Fraud facilitators, criminal and terrorist organizations, and individuals must be prevented from engaging in immigration fraud and violators must be prosecuted. Targeting systemic vulnerabilities may require changing processes, amending regulations, collaborating with other partner agencies, or working with the Congress to strengthen our laws. Information sharing on fraud schemes, trends, immigration crime subjects, and intelligence among Federal, State, local, tribal, and territorial

law enforcement partners helps drive decisions and, thus, is a key component of this approach. Timeliness, clarity, and completeness of information are vital to screening operations, immigration decisionmaking, and combating fraud.

- **Prevent entry or admission: Prevent entry or admission of criminals, fugitives, other dangerous foreign nationals, and other unauthorized entrants.** Homeland security efforts must focus on keeping criminal, fugitive, and other dangerous foreign nationals from entering the United States. The use of technology and information sharing among key Federal partners is essential so that dangerous individuals are detected before they are granted an immigration benefit or visa, or are admitted at a port of entry. Threat screening processes, biometric identification, and timely access to information on trends and fraud must all be strengthened to enhance their effectiveness.

- **Arrest, detain, prosecute, and remove: Arrest, detain, prosecute, and remove criminal, fugitive, dangerous, and other unauthorized foreign nationals consistent with due process and civil rights protections.** Dangerous criminal aliens, human rights violators, and other foreign nationals who threaten our national security must be a high priority for law enforcement. This principle also applies when assigning detainees to higher or lower security detention facilities, or when providing alternatives to detention. Arrested individuals must be screened to identify victims of trafficking, refugees, and exploited persons, and they must be provided with access to legal resources.

V. Missions, Goals, and Objectives of Homeland Security

Mission 4: Safeguarding and Securing Cyberspace

Our security and way of life depend upon a vast array of interdependent and critical networks, systems, services, and resources. To have an infrastructure that is secure and resilient, enables innovation and prosperity, and protects privacy and other civil liberties by design, we must secure cyberspace and manage other risks to its safe use.

Key Strategic Outcomes
• Critical information systems and information and communications services are secure, reliable, and readily available.
• Homeland security partners develop, update, and implement guidelines, regulations, and standards that ensure the confidentiality, integrity, and reliability of systems, networks, and data.
• Cyber disruptions or attacks are detected in real-time, consequences are mitigated, and services are restored rapidly.
• Academic institutions produce and homeland security partners sustain a cybersecurity workforce that meets national needs and enables competitiveness.
• Critical infrastructure sectors adopt and sector partners meet accepted standards that measurably reduce the risk of cyber disruption or exploitation.

Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment

Ensure malicious actors are unable to effectively exploit cyberspace, impair its safe and secure use, or attack the Nation's information infrastructure. Cyber infrastructure forms the backbone of the Nation's economy and connects every aspect of our way of life. While the cyber environment offers the potential for rapid technological advancement and economic growth, a range of malicious actors may seek to exploit cyberspace for dangerous or harmful purposes, cause mass disruption of communications or other services, and attack the Nation's infrastructure through cyber means. We must secure the system of networks and information upon which our prosperity relies while promoting economic growth, protecting privacy, and sustaining civil liberties. Both public- and private-sector efforts are required to achieve these aims. In addition, a robust law enforcement and counterintelligence capability is essential to the success of our cybersecurity efforts.

V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

Objectives

- **Understand and prioritize cyber threats: Identify and evaluate the most dangerous threats to Federal civilian and private-sector networks and the Nation.** The speed of innovation in the cyber realm requires that sharing of information and analysis occur before malicious actors can exploit vulnerabilities. We must continuously sharpen our understanding of risks to our critical information infrastructure. Risk management decisions must incorporate cyber risks based on technological as well as nontechnological factors, and must address the differing levels of security required by different activities. Information and intelligence regarding emerging cyber threats and vulnerabilities must be collected, analyzed, and shared appropriately and promptly. Homeland security partners must provide and receive information and assessments on risks to and incidents involving information systems, networks, and data in time to carry out their risk management responsibilities. Finally, homeland security partners must use compatible information architecture and data standards to maximize the appropriate acquisition, access, retention, production, use, management, and safeguarding of risk information.

- **Manage risks to cyberspace: Protect and make resilient information systems, networks, and personal and sensitive data.** As with other aspects of homeland security, we cannot close every vulnerability and mitigate every risk. Instead, we must develop a risk management approach that accepts certain risks, reduces others, and concentrates on the most consequential. Developing and implementing effective risk management strategies incorporating both protection and resilience for cyber infrastructure will require partnership, coordination, and cooperation across all elements of the homeland security enterprise. Homeland security partners must develop, promulgate, and update guidelines, codes, rules, regulations, and accepted standards when appropriate, that ensure the confidentiality, integrity, and availability of systems, networks, and data without impairing innovation, and while enhancing privacy. Government must focus on and address strategic vulnerabilities in cyberspace. Government must also lead by example, effectively securing its own networks. However, both critical infrastructure sectors and government agencies must meet accepted standards that measurably reduce risk of cyber attack or disruption to public health and safety, critical government services, and essential economic activities. Security controls on information systems, networks, and data must be consistently implemented, monitored, upgraded, and enforced.

V. Missions, Goals, and Objectives of Homeland Security

- **Prevent cyber crime and other malicious uses of cyberspace:** **Disrupt the criminal organizations and other malicious actors engaged in high-consequence or wide-scale cyber crime.** The cyber environment presents the potential for sophisticated cyber threats, cyber espionage, and cyber attacks. We must identify and mitigate cyber threats by coordinating and integrating robust counterintelligence, counterterrorism, intelligence, and law enforcement activities to prevent attacks, disruptions, and exploitations. Through law enforcement efforts, we must identify and locate domestic and international cyber criminals involved in significant cyber intrusions, identity theft, financial crime, and national security-related crimes committed utilizing the Internet. We must ensure that criminal organizations engaged in high-consequence or wide-scale cyber crime are aggressively investigated and disrupted, and their leaders arrested, indicted, and prosecuted. Through counterintelligence efforts, we must identify and thwart hostile intelligence collection activities and other cyber threats directed against the Nation.

- **Develop a robust public-private cyber incident response capability:** **Manage cyber incidents from identification to resolution in a rapid and replicable manner with prompt and appropriate action.** The evolving nature of cyber threats necessitates that we recognize and respond to cyber incidents in a comprehensive and coordinated fashion involving both the public and private sectors. Cyber disruptions or attacks must be identified in time for a comprehensive response, and homeland security partners must develop and improve cyber incident contingency plans. Additionally, cyber incidents must be managed in accordance with a commonly understood and integrated response framework, and real-time analysis capabilities and processes must mitigate these incidents with an appropriate response. Finally, critical services must be restored and consequences must be mitigated following cyber incidents.

Goal 4.2: Promote Cybersecurity Knowledge and Innovation

Ensure that the Nation is prepared for the cyber threats and challenges of tomorrow. Cybersecurity is a dynamic field, and cyber threats and challenges evolve at breathtaking speed. Education, training, awareness, science, technology, and innovation must flourish in order to meet this challenge. While we must protect the Nation from cyber attacks that occur today, we must also prepare now to mitigate the most consequential cybersecurity risks that the United States and its people will face in 5, 10, and 20 years. We must make long-term investments that sustain a safe, secure, and reliable cyber environment, enable prosperity, further

V. Missions, Goals, and Objectives of Homeland Security

social and community uses of the Internet, and facilitate transactions and trade, while safeguarding privacy and civil liberties.

Objectives

- **Enhance public awareness: Ensure that the public recognizes cybersecurity challenges and is empowered to address them.** As we have seen in other homeland security mission areas, an aware and empowered public is our best defense against threats, and our greatest resource in building resilience and fostering innovation. Each individual, every business enterprise, and each government agency has a vital role to perform if cyberspace is to realize its full potential. For the Nation to remain secure and prosperous, government must not only succeed at its own cybersecurity mission but must also empower others to succeed in theirs. Communications to the public must emphasize their role in cybersecurity. Leaders in the public and private sectors must be more informed of the security implications of their decisions with respect to cyberspace.

- **Foster a dynamic workforce: Develop the national knowledge base and human capital capabilities to enable success against current and future threats.** A capable workforce must exist to protect cyber infrastructure from current, emerging, and future risks. A knowledgeable cybersecurity workforce must exist across government with sufficient capacity and expertise to manage current and emerging risks. We must better understand our own cyber strengths and weaknesses and those of our adversaries. Through learning, we can adapt and recalibrate our approaches, our areas of emphasis, and our operational objectives.

- **Invest in innovative technologies, techniques, and procedures: Create and enhance science, technology, governance mechanisms, and other elements necessary to sustain a safe, secure, and resilient cyber environment.** Cyberspace's inherent characteristics demand constant innovation in order to effectively counter threats. Small vulnerabilities can lead to severe challenges in securing the Nation's vast—and vastly critical—information infrastructure. Relatively small investments in adversary attack capabilities can require disproportionately large investments in defense. Technology will assist us, and better ways of using technology and people will allow us to bring capabilities to bear more effectively. There must be continuous emphasis on cyber research, development, innovation, and interoperability, which drives advances in technologies, techniques, and procedures. As part of the homeland security enterprise, government should work creatively and collaboratively with the private sector to identify tailored solutions that both take into account the need

to protect public and private interests and take an integrated approach to achieving clear objectives, preventing mass disruptions and exploitations of government systems and critical infrastructure through cyberspace. We must prioritize investment in programs that demonstrate the best opportunity to help mitigate national cyber risk. Innovation in technology, practice, and policy must further protect—not erode—privacy and civil liberties.

V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

MISSION 5: ENSURING RESILIENCE TO DISASTERS

The strategic aims and objectives for ensuring resilience to disasters are grounded in the four traditional elements of emergency management: hazard mitigation, enhanced preparedness, effective emergency response, and rapid recovery. Together, these elements will help create a Nation that understands the hazards and risks we face, is prepared for disasters, and can withstand and rapidly and effectively recover from the disruptions they cause.

Key Strategic Outcomes

- A standard for general community hazard mitigation is collaboratively developed and adopted by all communities.

- Individuals and families understand their responsibilities in the event of a community-disrupting event and have a plan to fulfill these responsibilities.

- Preparedness standards for life safety, law enforcement, mass evacuation and shelter-in-place, public health, mass care, and public works capabilities, including capacity levels for catastrophic incidents, have been developed and are used by all jurisdictions.

- Jurisdictions have agreements in place to participate in local, regional, and interstate mutual aid.

- All organizations with incident management responsibilities utilize the *National Incident Management System*, including the Incident Command System, on a routine basis and for all federally declared disasters and emergencies.

Goal 5.1: Mitigate Hazards

Strengthen capacity at all levels of society to withstand threats and hazards. Though the occurrence of some disasters is inevitable, it is possible to take steps to reduce the impact of damaging events that may occur. The Nation's ability to withstand threats and hazards requires an understanding of risks and robust efforts to reduce vulnerabilities. Mitigation provides a critical foundation to reduce loss of life and property by closing vulnerabilities and avoiding or lessening the impact of a disaster, thereby creating safer communities. Mitigation seeks to break out of the cycle of disaster damage, reconstruction, and repeated damage. Mitigating vulnerabilities reduces both the direct consequences and the response and recovery requirements of disasters.

V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

Objectives

- **Reduce the vulnerability of individuals and families: Improve individual and family capacity to reduce vulnerabilities and withstand disasters.** Individuals and families must be a focal point of mitigation efforts, as they are best positioned to reduce their own vulnerabilities. Promoting individual and family mitigation requires identifying the factors that influence the psychological and social resilience of individuals. Government must actively engage to help individuals understand the risks that their communities face, the resources available to them, and the steps they can take to prepare themselves, their homes, and their businesses.

- **Mitigate risks to communities: Improve community capacity to withstand disasters by mitigating known and anticipated hazards.** Community-level mitigation measures have historically proven successful in reducing the effects of disasters. Standards for general community hazard mitigation, such as building codes and land and water use policies, must be in place and enforced around the country. In addition, measures to reduce the consequences of disasters on critical infrastructure and essential systems and services, including supply chains, health care systems, communications networks, and transportation systems, must be incorporated into development planning. Insurance policies—including those offered or otherwise supported by the Federal Government—should include hazard mitigation incentives.

Goal 5.2: Enhance Preparedness

Engage all levels and segments of society in improving preparedness. Active participation by all segments of society in planning, training, organizing, and heightening awareness is an essential component of national preparedness. While efforts have traditionally focused on the preparedness of government and official first responders, individuals prepared to care for themselves and assist their neighbors in emergencies are important partners in community preparedness efforts. Because neighbor-to-neighbor assistance, when done safely, decreases the burden on first responders, individuals should be seen as force multipliers who may also offer specialized knowledge and skills.

Objectives

- **Improve individual, family, and community preparedness: Ensure individual, family, and community planning, readiness, and capacity-building for disasters.** Prepared individuals and families enhance overall

community resilience and reduce the burden on government emergency responders. Individuals and families must be prepared to care for themselves for a reasonable period of time after a disaster—some experts have suggested the first 72 hours—and assist their neighbors, reserving scarce public resources to assist those who are injured, incapacitated, or otherwise unable to care for themselves. The public must be engaged in order to build a collective understanding of their risks, the resources available to assist their preparations, and their roles and responsibilities in the event of a disaster. Participation in community disaster response programs such as Community Emergency Response Teams (CERTs), other Citizen Corps programs, and similar volunteer teams maintained by nongovernmental organizations must be enhanced, and community-based training and exercises must be increased, to help individuals gain the skills necessary to respond to disasters safely and in coordination with local authorities. Community organizations, including local NGOs, faith-based groups, and advocacy groups for vulnerable populations—often cornerstones of communities, but not traditionally involved in emergency management—must be integrated into community planning, risk reduction, and preparedness activities.

- **Strengthen capabilities: Enhance and sustain nationwide disaster preparedness capabilities, to include life safety, law enforcement, mass evacuation and shelter-in-place, public health, mass care, and public works.** Homeland security partners must be prepared for the variety of requirements resulting from a disaster. Joint hazard identification and risk analysis can help determine consensus-based, tiered preparedness standards for States, regions, and localities. These preparedness standards will then allow us to develop nationally the capabilities we will need to address the full range of threats and hazards that we face.

  Because success in day-to-day operations often foreshadows success in larger incidents, critical emergency response capabilities must be enhanced and all organizations with incident management responsibilities must be encouraged to use the Incident Command System (ICS) or a comparable system compliant with the *National Incident Management System* for day-to-day emergencies. In addition, we must evaluate our performance in exercises and learn from our responses to actual incidents to identify and close capability and capacity gaps and improve response and recovery operations.

V. Missions, Goals, and Objectives of Homeland Security

Goal 5.3: Ensure Effective Emergency Response

Strengthen response capacity nationwide. Because it is impossible to eliminate all risks, a resilient Nation must have a robust capacity to respond when disaster strikes. Such response must be effective and efficient and grounded in the basic elements of incident management. When an incident occurs that is beyond local response capabilities, communities must be able to obtain assistance from neighboring jurisdictions and regional partners quickly, making a robust regional capacity vital to effective emergency response.

Objectives

- **Provide timely and accurate information to the public: Establish and strengthen pathways for clear, reliable, and current emergency information, including effective use of new media.** Timely, appropriate, and reliable communication with the public

Less than three minutes after **American Airlines Flight 77 crashed into the Pentagon**, Arlington County Fire Department officials were on scene, leading the effort to establish a unified command and control structure under protocols set forth in the Incident Command System (now part of the *National Incident Management System*) and the Federal Response Plan (a predecessor to today's *National Response Framework*). These interagency emergency management frameworks were well known to first responders because of common regional use, extensive training, and operational experience in the field. In the hours following the attack, thousands of personnel from some 50 public safety agencies at the Federal, State, and local levels arrived on site and at nearby staging areas and emergency operations centers. Their decades of joint planning, training, exercising, and operations had built the foundations of a regional homeland security community, which ensured a universal understanding of roles and responsibilities and allowed for a near-seamless integration of multiple agencies into a unified and effective response.

before, during, and immediately after disasters is a key component of societal resilience. In today's environment of speed-of-light communications and pervasive social networking technologies, homeland security partners must take full advantage of cutting-edge tools and capabilities to promote widespread situational awareness. As such, information sharing and public alert and warning must be viewed as mutually supportive efforts in seeking to combine the networked power of new media and "Web 2.0" technologies with existing homeland security information-sharing capabilities such as fusion centers, emergency operations centers, and joint terrorism task forces. Moreover, emergency information must be accessible through as many pathways as

possible, to include multiple languages, through social networks in low-income areas, and to those with special needs.

- **Conduct effective disaster response operations: Respond to disasters in an effective and unified manner.** An effective response requires that incident management organizations at all levels of government embrace common doctrine, undertake joint planning and training, and work to establish interoperable communications and equipment capabilities across jurisdictions, providing the flexibility, adaptability, and scalability necessary to match the complexity of many modern disasters. This cohesion will allow responders to improvise effectively in the face of unforeseen circumstances. First responders must be able to use the on-scene command, resource management, and communications and information management elements of the *National Incident Management System*. Jurisdictions across the Nation must have the ability to accurately characterize incidents and track the status of personnel and resources responding to major disasters and emergencies.

- **Provide timely and appropriate disaster assistance: Improve governmental, nongovernmental, and private-sector delivery of disaster assistance.** Effectively delivering disaster assistance requires improved coordination and preparedness among governmental, nongovernmental, and private-sector resources, including local businesses and faith-based and community organizations. Humanitarian relief services such as emergency sheltering and individual financial assistance must be efficiently and effectively administered. Effective operations during disasters require integration of nongovernmental assets in planning, training, and exercises.

Goal 5.4: Rapidly Recover

Improve the Nation's ability to adapt and rapidly recover. Major disasters and catastrophic events produce changes in habitability, the environment, the economy, and even in geography that can often preclude a return to the way things were. We must anticipate such changes and develop appropriate tools, knowledge, and skills to adapt, improve sustainability, and maintain our way of life in the aftermath of disaster. Recent events have highlighted the challenges we face in dealing with disaster recovery. From sheltering and rehousing displaced survivors to reconstituting critical infrastructure and reestablishing the economic base of devastated areas, the challenges are profound. Individuals, businesses, nonprofit organizations, local, tribal, State, and Federal governments all have responsibilities

in disaster recovery, underscoring the need to improve coordination and unity of effort.

Objectives

- **Enhance recovery capabilities: Establish and maintain nationwide capabilities for recovery from major disasters.** Nationwide—at all levels of government and in nongovernmental organizations—sufficient capabilities for disaster recovery must be developed and maintained. While no government program can make communities and individuals whole, we must do a better job with the limited resources we have. This requires the development of a national strategic approach for disaster recovery and the use of standards for enhanced recovery capabilities. Federal roles and responsibilities must be clarified, and all jurisdictions must maintain and exercise recovery plans.

- **Ensure continuity of essential services and functions: Improve capabilities of families, communities, private-sector organizations, and all levels of government to sustain essential services and functions.** Communities, government entities, and private-sector organizations must develop and exercise continuity plans. Business continuity standards and practices must continue to gain acceptance. During a disaster, families and communities, as well as businesses and governmental entities, must be able to sustain critical capabilities and restore essential services in a timely manner.

VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

The strategic aims and objectives for maturing and strengthening the homeland security enterprise are drawn from the common themes that emerge from each of the mission areas. Ensuring a shared awareness and understanding of risks and threats, building capable communities, creating unity of effort, and enhancing the use of science and technology underpin our national efforts to prevent terrorism and enhance security, secure and manage our borders, enforce and administer our immigration laws, safeguard and secure cyberspace, and ensure resilience to disasters.

Enhance Shared Awareness of Risks and Threats

Establish a comprehensive system for building and sharing awareness of risks and threats. The engine behind a distributed homeland security effort is a shared awareness of the risks and threats among all key stakeholders. To be effective, the homeland security enterprise requires a comprehensive information strategy that respects the privacy and civil liberties of individuals, as well as the diversity of information needs across the different missions. Although much has been done to improve information sharing since the 9/11 attacks, more work remains. Toward that end, the following key objectives are a priority: national-level homeland security risk assessments; tools and institutional arrangements for effective and timely sharing of information and analysis; a robust approach to screening and identification verification that safeguards individual privacy and civil rights; enhanced knowledge management tools; improved domain awareness, including the expanded use of sensors, detectors, and other unmanned systems across a wide range of homeland security activities; and aggressive activities to identify and defeat efforts by adversaries to conduct surveillance against homeland targets and exploit any weaknesses. These objectives must culminate in a common understanding of security as a shared responsibility.

VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

Objectives

- **Establish an approach to national-level homeland security risk assessments: Develop and implement a methodology to conduct national-level homeland security risk assessments.** Constructing a nationwide approach to homeland security requires a deliberate analytic method to evaluate the risks posed by various hazards and threats to national strategic interests and establish strategic guidance for homeland security prioritization. Given limited resources and the prospect of a seemingly infinite possibility of threats and vulnerabilities to consider, we must make difficult decisions about how to prioritize homeland security efforts. A national homeland security risk assessment will provide the Nation's homeland security leaders with an assessment of risks to our strategic interests from the full range of threats, hazards, challenges, and long-term trends. Understanding the risks and the ability of DHS and partners and stakeholders across the homeland security enterprise to reduce and manage these risks is a fundamental step toward informing our priorities and the allocation of resources. The Federal Government should develop a methodology for a homeland security national-level risk assessment. This national-level risk assessment should include threat assessments produced by the Intelligence Community, as well as the information and expertise concerning vulnerabilities and consequences resident across Federal departments and agencies and the homeland security enterprise. National-level homeland security risk assessments will enable DHS and homeland security partners and stakeholders to take the next step toward truly risk-informed decisionmaking.

> **A Homeland Security National Risk Assessment** will provide the Nation's homeland security leaders with an assessment of homeland security risks to our national strategic interests from challenges that include weapons of mass destruction, global terrorism, mass cyber attacks, pandemics, major accidents and natural disasters, illegal trafficking and related transnational criminal activity, and smaller scale attacks. Such a risk assessment will help homeland security decisionmakers determine the most promising strategic opportunities to manage risks across the homeland security enterprise.

VI. Maturing and Strengthening the Homeland Security Enterprise

- **Share information and analysis: Enhance critical tools and institutionalize arrangements for timely access and effective sharing of information and analysis.** The ability to more effectively share information among local, tribal, territorial, State, and Federal homeland security practitioners is critical to improving collaboration and decisionmaking during day-to-day operations and large-scale emergencies. Integrating existing technologies and using tools such as State and major urban area fusion centers provide critical delivery vehicles for homeland security intelligence and information. We must continue to strengthen baseline capabilities and analytic capacity to operate consistently, rapidly identify and disseminate information, and support and enhance a State and urban area intelligence platform for risk-based, information-driven decisionmaking by homeland security stakeholders.

> **Effective, timely sharing of information and analysis** is essential to homeland security. Fusion centers are the State and major city entities that were recommended in the Implementing the 9/11 Commission Recommendations Act of 2007 as the best way for Federal, State, local, tribal, and territorial governments and the owners and operators of critical infrastructure to share information and intelligence about terrorist threats, criminal activity, and other hazards. Since 2006, States and major cities have stood up some 70 fusion centers across the country, with the Federal Government contributing personnel, financial, and technical support.

- **Screen and verify identity: Establish a robust approach to identity verification that safeguards individual privacy and civil rights.** Robust procedures to screen and verify identities are critical to helping accurately identify people and assess risk. Future systems will need to be increasingly secure, efficient, easy to use, and flexible. Ongoing research into emerging technologies will help to expand screening and verification capabilities. At the same time, we must adhere to privacy standards and ensure that we fully respect individual rights and liberties. Information needed to achieve homeland security objectives must be collected and used consistent with applicable law and policy. Training, audits, and other oversight mechanisms are essential to ensuring information is used lawfully and appropriately.

VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

- **Enhance domain awareness: Ensure shared situational awareness in the air, land, and maritime domains.** Homeland security activities depend upon having shared situational awareness across a range of complex and dynamic operational environments. Awareness of aircraft, vehicles, and vessels in U.S. airspace and the air, land, and maritime approaches to the United States, along with Federal, State, local, tribal, territorial, and international resources to address threats and hazards, is critical to our ability to take effective action. Sensors, detectors, and other unmanned systems can play a vital role in supporting decisions about whether threats are present and when to intervene. Numerous unmanned systems are in use or development across the homeland security enterprise, including systems for monitoring the integrity of shipping containers from the point of consolidation to the point of deconsolidation; a "lab-in-a-box" capable of aerosol collection, molecular identification, and reporting on biological threats; imaging and radar systems designed to detect, track, and classify contacts; sensors to monitor the vital signs and establish the physical health of first responders; and a first responder locating system to enable incident commanders to visually track personnel. We must increase our domain awareness efforts consistent with our core interests of privacy and civil liberties.

> **Hybrid Capabilities and Complementary Activities.** Hybrid capabilities—assets and resources capable of performing multiple missions—are a hallmark of homeland security. In some cases, the same assets and personnel that patrol our borders, enforce our immigration laws, and respond to major oil spills, for example, also enforce safety regulations, assist travelers, and safeguard natural resources. These complementary activities are critical to fulfilling other national interests, and are often intertwined and mutually supporting with homeland security activities. Homeland security partners and stakeholders—both within DHS and across the homeland security enterprise—often maintain hybrid capabilities to fulfill multiple missions.

- **Integrate counterintelligence: Use and integrate counterintelligence in all aspects of homeland security to thwart attacks against the homeland.** The foreign intelligence threat to the United States—from states, non-state actors, and terrorist groups—is pervasive, intricate, far reaching, and growing. Globalization has made communication technology widely available, which our enemies can manipulate to gain advantages in the international marketplace and against the homeland, including our critical infrastructure. Because terrorists or

other adversaries often employ intelligence tradecraft to identify targets and prepare their attacks, counterintelligence can provide a critical means to understanding current and evolving threats. Counterintelligence also provides a suite of tools and skills to identify, deceive, exploit, or disrupt these preparations and operations. Efforts to prevent terrorism and enhance the security of the homeland rely, in part, on effective counterintelligence. We must disrupt hostile cyber activities, identify hostile intelligence collection activities, detect insider threats, and expand awareness of our adversaries' intelligence threats and capabilities.

- **Establish a common security mindset: Promote a common understanding of security as a shared responsibility.** Homeland security is a shared responsibility for which all elements of society—from individuals and communities, to the private sector, to State, local, tribal, and territorial governments, to nongovernmental organizations, to the Federal Government— have a vital role to play. The Federal Government cannot be everywhere, nor can it alone ensure resilience or thwart every threat, despite best efforts. Private individuals, communities, and other nongovernmental actors must be empowered to take action. The American people hold a strong sense of community, a belief in collective responsibility, and a willingness to do what is required of them to contribute to our common security and sustain our way of life. The highest calling of the homeland security enterprise is to empower Americans to contribute to our country's security—to embrace a unity of purpose. Empowered individuals with a mindset of shared responsibility are uniquely capable of disrupting threats and ensuring the security of the interdependent systems that make up society. Individuals and communities are the focal point of societal resilience, enhancing public preparedness and thus diminishing the effectiveness of terrorist tactics.

Build Capable Communities

Foster communities that have information, capabilities, and resources to prevent threats, respond to disruptions, and ensure their own well-being. Individuals, families, and communities are essential partners in the homeland security enterprise. Building and sustaining capability at the community level is essential to meeting homeland security strategic aims and realizing our vision for a secure homeland.

VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

Objectives

- **Set capability and capacity standards:** **Identify core capability and capacity targets to guide homeland security investments and activities across the enterprise.** We must focus on building and maintaining capabilities to address challenges across all homeland security missions. To do this, we must jointly, through cross-governmental collaborative mechanisms, set clear, measurable target levels of capability and capacity for enterprise partners across all missions and develop a system for assessing progress toward these targets. In order to succeed, we must focus our efforts on concrete, specific, and measurable objectives, setting clear, measurable target levels of capability and capacity for enterprise partners. Commitment to such a process is essential to our ability to "spend smarter" in an environment of tightening resources.

- **Enhance systems for training, exercising, and evaluating capabilities.** Training provides first responders, homeland security officials, emergency management officials, nongovernmental and private-sector partners, and other personnel with the knowledge, skills, and abilities needed to perform key tasks required by specific capabilities. Exercises provide a vital tool for homeland security personnel, from first responders to senior officials, to practice operational activities and decisionmaking processes in a realistic but risk-free environment. We must build on current efforts to coordinate and integrate exercises nationally, and emphasize the importance of exercising both steady-state and contingency-based mission activities in order to achieve measurable improvement. Exercises must also be valuable tools for assessing and improving performance, while demonstrating community resolve to prepare for major incidents. We must strive for assessments of

> **State, local, tribal, and territorial governments** are on the front lines of our efforts to secure our homeland, and are the first responders to incidents of all types. A coordinated approach that promotes unity of effort will provide the strongest foundation for the homeland security enterprise's efforts to combat current, emerging, and future threats to the homeland. To achieve unity of effort, partners will need clearly defined roles and responsibilities, access to information, and a shared understanding of how risks are managed and prioritized to inform the allocation of limited resources. In addition, Federal, State, local, tribal, and territorial partners will need a common framework to understand threats, assess risks, and share information.

capabilities across all levels that minimize the volume of reporting requirements and more efficiently collect necessary data on homeland security capabilities.

- **Maintain and sustain equipment and capabilities: Promote smart investment in operational capabilities.** Homeland security equipment and capabilities are critically important yet resource-intensive investments for stakeholders across the enterprise. In a resource-constrained environment, it is critical that the maintenance and sustainment of capabilities is done in the most cost-effective manner possible. We must promote and support long-term investments in capabilities through our grant programs and other funding mechanisms. Our goal is to help create capable communities, and we should promote the most efficient and prudent means of achieving and sustaining that goal.

Foster Unity of Effort

Foster a broad national culture of cooperation and mutual aid. Unity of effort is the ultimate goal for maturing and strengthening the homeland security enterprise. Cooperation and mutual aid are cornerstones of success for effective joint activity. A coordinated approach that promotes unity of effort will provide the strongest foundation to combat current, emerging, and future threats to the homeland. To achieve unity of effort, partners will need clearly defined roles and responsibilities, access to information, and a shared understanding of how risks are managed and prioritized to inform the allocation of limited resources. In addition, public-sector agencies and their private-sector partners will need an integrated framework to share information, understand threats, and assess and manage risks.

Objectives

- **Build a homeland security professional discipline: Develop the homeland security community of interest at all levels of government as part of a cadre of national security professionals.** A well-documented need within the national security community is a professional development program that fosters a stable and diverse community of professionals with the proper balance of relevant skills, attributes, experiences, and comprehensive knowledge. Executive Order 13434, "National Security Professional Development," initiated a program for developing interagency national security professionals through access to an integrated framework of training, education, and professional experience opportunities. We must work together with our national security partners in bringing that important idea to fruition. As part of that effort, we must take steps to create a homeland security community of interest across the

enterprise. Three elements of professional development are education, training, and experience via developmental assignments. State, local, tribal, and territorial governments, DHS and other Federal agencies, and academic institutions have taken important steps to build programs to support these key areas and will continue to emphasize enterprise-wide approaches to enhancing homeland security professional development.

- **Promote regional response capacity: Promote mutual aid agreements for response requirements that exceed local capacity.** As previously mentioned, disasters rarely recognize jurisdictional boundaries and often overwhelm local response capabilities. For these situations, regional plans should be developed to address operational interdependencies and local, regional, and interstate mutual aid agreements must be in place. To ensure interoperability, incident management organizations at all levels of government should employ elements of the *National Incident Management System* and conduct regional joint assessments, planning, and training. This objective builds on the foundation established in Mission 5: Ensuring Resilience to Disasters.

- **Institutionalize homeland security planning: Develop a planning system to execute homeland security activities.** A homeland security planning system is essential and indispensible to homeland security. Current planning systems address only portions of overall homeland security activities, and require better integration across all levels of government and with nongovernmental entities. Through fully considered interagency and intergovernmental discussions, we must integrate current planning practices and, drawing from best practices across the homeland security enterprise, create a planning system that allows homeland security partners and stakeholders to plan collaboratively and ensure that homeland security activities achieve our shared goals.

> **Unity of effort** is the key to operational success in homeland security. Jointness and multiagency coordination principles underpin both military and civilian mechanisms for achieving unity of effort. The *National Response Framework* and *National Incident Management System* facilitate unity of effort for disaster response and emergency services activity. The *Maritime Operational Threat Response Plan* and the Joint Interagency Task Force concept are used to achieve unity of effort for preventing terrorism, securing cyberspace, and effectively controlling U.S. land, air, and sea borders.

- **Further enhance the military-homeland security relationship: Strengthen unity of effort between military and civilian activities for homeland**

VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

security. We must work together to develop and expand models of coordination and cooperation between military and civilian authorities, and revise strategy and doctrine accordingly. The *National Response Framework* and the *National Incident Management System* provide mechanisms to ensure unity of effort between civilian and military authorities for disaster response. We must continually refine and enhance the framework for providing defense support to civil authorities for all homeland security mission activities. In addition, Federal departments and agencies should jointly conduct planning and analysis for homeland security and related defense activities, including developing joint strategic planning and analytic tools for determining capability requirements, as well as conducting joint national-level risk assessments in areas of shared interest. Federal departments and agencies must also explore ways to jointly develop capabilities necessary for both defense and homeland security.

- **Strengthen the ability of Federal departments and agencies to support homeland security missions.** While some Federal departments and agencies have broad homeland security responsibilities, others have smaller, but still critical, homeland security roles or capabilities associated within their own statutorily authorized programs, which may be leveraged for homeland security purposes. Federal departments and agencies with smaller, but critical, homeland security roles must be adequately resourced to meet homeland security mission requirements.

- **Expand and extend governmental and private-sector international partnerships: Transform how government and the private sector interact.** International partners are key participants in the homeland security enterprise. The interconnected nature of world economies and international infrastructure means that seemingly isolated events often have transnational origins and global consequences. The acceleration of the flows of ideas, goods, and people around the world and across U.S. borders generally advances America's interests, but also creates security challenges that are increasingly borderless and unconventional. International partners are critical to the effort to secure the homeland against threats that transcend jurisdictional and geographic boundaries. International engagement enhances the transparency of threat trajectories and increases our capacity to understand, investigate, and interdict threats at the earliest possible point, ideally before they become manifest, reach our shores, or disrupt the critical networks on which we depend. The United States must work with its international partners to increase global security

VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

against terrorism and violent extremism, the spread of infectious diseases, and the consequences of natural disasters.

- **Mature the Department of Homeland Security: Improve DHS's organizational and programmatic alignment and its management systems and processes.** DHS must lead by example. Ensuring unity of effort across the homeland security enterprise requires unity of effort within the Department. Critical to unifying DHS is improved organizational alignment, particularly among DHS headquarters components, enhanced programmatic alignment to the homeland security missions, and more efficient and effective management processes, including strategic planning, performance management, and accounting structure. DHS must complete a thorough review of its own organizational structures and programmatic activities, align programs and budgets to homeland security missions, and strengthen its management processes. This work began during the QHSR process and continues through the Department's bottom-up review.

Foster Innovative Approaches and Solutions Through Leading-Edge Science and Technology

Ensure scientifically informed analysis and decisions are coupled to innovative and effective technological solutions. We must be able to address a highly dynamic, broad, and ever-changing spectrum of threats, vulnerabilities, and disaster scenarios and to design and implement cost-effective operational and technological solutions across a wide array of operational contexts, in a manner that protects American values. Although many of the security threats now confronting the United States are driven by the global diffusion of technology, science and technology can also provide new and more effective methods for preventing and mitigating these threats, as well as natural disasters. The Federal Government must have a robust research effort in homeland security that is grounded in sound science, and a rigorous and disciplined approach to technology development, acquisition, and deployment.

Objectives

- **Scientifically study threats and vulnerabilities: Pursue a rigorous scientific understanding of current and future threats to homeland security and the possible means to their prevention and mitigation.** A comprehensive and vivid understanding of the probability and potential consequences of homeland security threats and hazards and the relative risk they pose forms the strategic foundation of the homeland security enterprise. Ongoing analyses of threats,

vulnerabilities, and the efficacy of our countermeasures by both the public and private sectors will inform homeland security priorities and help ensure that investments and operations focus on the most urgent problems and the most effective means for addressing them.

- **Develop innovative approaches and effective solutions: Encourage and enable innovative approaches to critical homeland security challenges, fostering collaborative efforts involving government, academia, and the private sector.** Achieving the goals of the core homeland security missions will require scientific research to discover new knowledge and methods that can be applied to homeland security challenges, and the creation of new technologies and new ways of thinking about problems and possible solutions. Technological feasibility, operational requirements, training needs, and financial sustainability must all be considered in developing and deploying new technologies. We must seek to foster a rich and wide-ranging capacity to identify and think through complex and unfamiliar problems and to formulate

> **DHS and the Department of Energy—including the National Laboratories—have established a partnership on aviation security** in order to develop new and more effective technologies to deter and disrupt known threats and proactively anticipate and protect against new ways by which terrorists could seek to board an aircraft.

effective and inventive solutions spanning many difficult and varied operational contexts. We must engage a wide range of stakeholders in this endeavor, including government labs, universities, federally funded research and development centers, and the private sector.

This page intentionally left blank.

VII. CONCLUSION: THE PATH FORWARD

The Quadrennial Homeland Security Review report sets forth a broad vision for homeland security. We have learned that our Nation's security is more than building protections, securing our borders, or preventing terrorism, although these measures are all central to homeland security. Homeland security is also about protecting the American way of life and ensuring our resilience in a challenging world.

The QHSR process (elaborated at **Appendix B**) and resulting report were designed to serve as a catalyst to spur the continued evolution and maturation of our Nation's homeland security enterprise—the diverse and distributed set of public and private actors from all corners of this Nation. Through this effort, we seek to foster a greater understanding of our shared responsibility and growing capability to protect ourselves from a range of threats and hazards.

In the years ahead, the world will be filled with breathtaking technological changes, social advances, and an accelerating flow of ideas, goods, and people around the world. These advancements and global interactions will enrich and improve our lives, but they may also be exploited by or may contribute to violent extremism, terrorist attacks, health threats, proliferation concerns, natural disasters, and cyber attacks—with many of these occurring, perhaps, at the same time.

The QHSR has set the stage for detailed analyses of homeland security capabilities and requirements across the homeland security enterprise. Stakeholders must now work to prioritize and identify the capabilities needed to achieve the goals, objectives, and outcomes identified in the QHSR, tie these requirements to resource allocation priorities, set performance criteria, and validate the allocation of roles and responsibilities.

The division of operational roles and responsibilities among Federal departments and agencies for various homeland security mission goals and objectives emerged as a major area requiring further study following the QHSR. Going forward, an analysis of roles and responsibilities across the homeland security missions would help resolve gaps or unnecessary redundancies between departments and agencies. Meaningful engagement by representative stakeholders from across the homeland security enterprise, including State, local, tribal, and territorial governments, must be part of the process.

VII. CONCLUSION: THE PATH FORWARD

The Department of Homeland Security has begun a comprehensive examination of the Department's activities and resources. This bottom-up review is a major step forward in DHS's ongoing effort to systematically link strategy to program to budget. The objective of this sequence of reviews is a linked strategy, set of programs, and budget that will strengthen the Department. The QHSR, the bottom-up review, and the budget proposals that will follow are important steps in maturing DHS into a truly strategy-driven organization. Additionally, the bottom-up review will advance the Department's functionality in three ways:

1. Increased comparability of programs, activities, and resources within and across components;
2. Improved measurement of desired mission outcomes and the contribution of programs, activities, and resources to these mission outcomes; and
3. Better cost estimating of programs and activities.

This exercise entails mapping existing activities to QHSR missions, identifying gaps and overlaps in these activities, improving the Department's ability to analytically relate activities to mission outcomes, and reassessing how to organize and group these activities into programs.

The path forward following the QHSR is clear—we must move with a sense of urgency and purpose to achieve our shared interest and common vision of a safer, more secure and resilient America. Each of us—government, business enterprise, and individual alike—has a role to play, contributing to the collective strength of this country. The message is clear: This Nation can protect itself. But we must all play a role—and in the commitment of each, we will secure the homeland for all.

APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

Homeland security spans the authorities and responsibilities of Federal departments and agencies, State, local, tribal and territorial governments, the private sector, as well as private citizens and communities. For this reason, coordination and cooperation are essential to successfully carrying out and accomplishing the homeland security missions. Documents such as the *National Infrastructure Protection Plan* (NIPP) and *National Response Framework* (NRF), as well as documents produced by the National Counterterrorism Center, spell out roles and responsibilities for various aspects of homeland security. The following discussion highlights key current roles and responsibilities of the many actors across the homeland security enterprise. They are derived largely from statutes, Presidential directives, and other authorities, as well as from the NIPP and NRF.

- 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 National Security and Homeland Security Councils and the National Security Staff, provides overall homeland security policy direction and coordination. As a result of Presidential Study Directive 1 (2009), which directed an examination of ways to reform the White House organization for counterterrorism and homeland security, the White House merged the staffs of the National Security Council and the Homeland Security Council into a single new integrated National Security Staff.

- The **Secretary of Homeland Security** leads the Federal agency as defined by statute charged with homeland security: preventing terrorism and managing risks to critical infrastructure; securing and managing the border; enforcing and administering immigration laws; safeguarding and securing cyberspace; and ensuring resilience to disasters.

- The **Attorney General** has lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at United States citizens or institutions abroad, as well as for related intelligence collection activities within the United States. Following a terrorist threat or an actual incident that falls within the criminal jurisdiction of the United States, the Attorney General identifies the perpetrators and brings them to justice. The Attorney General leads the Department of Justice, which also includes the **Federal Bureau of Investigation**, **Drug Enforcement Administration**, and **Bureau of Alcohol, Tobacco, Firearms, and Explosives**, each of which has key homeland security responsibilities.

- The **Secretary of State** has the responsibility to coordinate activities with foreign governments and international organizations related to the prevention,

preparation, response, and recovery from a domestic incident, and for the protection of U.S. citizens and U.S. interests overseas. The Department of State also adjudicates and screens visa applications abroad.

- The **Secretary of Defense** leads the Department of Defense (DOD), whose military services, defense agencies, and geographic and functional commands defend the United States from direct attack, deter potential adversaries, foster regional stability, secure and assure access to sea, air, space, and cyberspace, and build the security capacity of key partners. DOD also provides a wide range of support to civil authorities at the direction of the Secretary of Defense or the President when the capabilities of State and local authorities to respond effectively to an event are overwhelmed.

- The **Secretary of Health and Human Services** leads the coordination of all functions relevant to Public Health Emergency Preparedness and Disaster Medical Response. Additionally, the Department of Health and Human Services (HHS) incorporates steady-state and incident-specific activities as described in the National Health Security Strategy. HHS is the coordinator and primary agency for Emergency Support Function (ESF) #8 – Public Health and Medical Services, providing the mechanism for coordinated Federal assistance to supplement State, local, tribal, and territorial resources in response to a public health and medical disaster, potential or actual incident requiring a coordinated Federal response, and/or during a developing potential health and medical emergency. HHS is also the Sector-Specific Agency for the Healthcare and Public Health Sector.

- The **Secretary of the Treasury** works to safeguard the U.S. financial system, combat financial crimes, and cut off financial support to terrorists, WMD proliferators, drug traffickers, and other national security threats.

- The **Secretary of Agriculture** 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 of Agriculture (USDA) is the Sector-Specific Agency for the Food and Agriculture Sector, a responsibility shared with the Food and Drug Administration with respect to food safety and defense. In addition, USDA is the coordinator and primary agency for two Emergency Support Functions: ESF #4 – Firefighting and ESF #11 – Agriculture and Natural Resources. USDA, together with the Department of the Interior, also operates the National Interagency Fire Center.

APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

- The **Director of National Intelligence** serves as the head of the Intelligence Community (IC), acts as the principal advisor to the President and National Security Council for intelligence matters relating to national security, and oversees and directs implementation of the National Intelligence Program. The IC, composed of 16 elements across the U.S. Government, functions consistent with law, Executive order, regulations, and policy to support the national security-related missions of the U.S. Government. It provides a range of analytic products that assess threats to the homeland and inform planning, capability development, and operational activities of homeland security enterprise partners and stakeholders. In addition to IC elements with specific homeland security missions, the Office of the Director of National Intelligence maintains a number of mission and support centers that provide unique capabilities for homeland security partners, including the **National Counterterrorism Center (NCTC)**, National Counterproliferation Center, and National Counterintelligence Executive. NCTC serves as the primary U.S. government organization for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism, and conducts strategic operational planning for integrated counterterrorism activities.

- The **Secretary of Commerce**, supportive of national economic security interests and responsive to Public Law and Executive direction, is responsible for promulgating Federal information technology and cybersecurity standards; regulating export of security technologies; representing U.S. industry on international trade policy and commercial data flow matters; security and privacy policies that apply to the Internet's domain name system; protecting intellectual property; conducting cybersecurity research and development; and assuring timely availability of industrial products, materials, and services to meet homeland security requirements.

- The **Secretary 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 is a supporting Federal agency in the response and management of emergencies under the *National Response Framework*.

- The **Secretary of Energy** maintains stewardship of vital national security capabilities, from nuclear weapons to leading edge research and development programs. The Department of Energy (DOE) is the designated Federal agency to provide a unifying structure for the integration of Federal critical infrastructure and key resources protection efforts specifically for the Energy

Sector. It is also responsible for maintaining continuous and reliable energy supplies for the United States through preventive measures and restoration and recovery actions. DOE is the coordinator and primary agency for ESF #12 – Energy when incidents require a coordinated Federal response to facilitate the restoration of damaged energy systems and components.

- The **Administrator of the Environmental Protection Agency (EPA)** leads the EPA, which is charged with protecting human health and the environment. For certain incidents, EPA is the coordinator and primary agency for ESF #10 – Oil and Hazardous Materials Response, in response to an actual or potential discharge and/or uncontrolled release of oil or hazardous materials. EPA is the Sector-Specific Agency for securing the Water Sector.

- The **Secretary of Housing and Urban Development** is the coordinator and primary agency for ESF #14 – Long-Term Community Recovery, which provides a mechanism for coordinating Federal support to State, tribal, regional, and local governments, nongovernmental organizations (NGOs), and the private sector to enable community recovery from the long-term consequences of extraordinary disasters.

- The **Secretary of the Interior** develops policies and procedures for all types of hazards and emergencies that impact Federal lands, facilities, infrastructure, and resources; tribal lands; and insular areas. The Department of the Interior (DOI) is also a primary agency for ESF #9 – Search and Rescue, providing specialized lifesaving assistance to State, tribal, and local authorities when activated for incidents or potential incidents requiring a coordinated Federal response. DOI, together with the Department of Agriculture, also operates the National Interagency Fire Center.

- The **Secretary of Transportation** collaborates with DHS on all matters relating to transportation security and transportation infrastructure protection and in regulating the transportation of hazardous materials by all modes (including pipelines). The Secretary of Transportation is responsible for operating the national airspace system.

- **Other Federal Agencies** are also part of the homeland security enterprise and contribute to the homeland security mission in a variety of ways. This includes agencies with responsibilities for regulating elements of the Nation's critical infrastructure to assure public health, safety, and the common defense, developing and implementing pertinent public policy, supporting efforts to

assure a resilient homeland, and collaborating with those departments and agencies noted above in their efforts to secure the homeland.

- **Critical Infrastructure and Key Resource (CIKR) Owners and Operators** develop protective programs and measures to ensure that systems and assets, whether physical or virtual, are secure from and resilient to cascading, disruptive impacts. Protection includes actions to mitigate the overall risk to CIKR assets, systems, networks, functions, or their interconnecting links, including actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident. CIKR owners and operators also prepare business continuity plans and ensure their own ability to sustain essential services and functions.

- **Major and Multinational Corporations** operate in all sectors of trade and commerce that foster the American way of life and support the operation, security, and resilience of global movement systems. They take action to support risk management planning and investments in security as a necessary component of prudent business planning and operations. They contribute to developing the ideas, science, and technology that underlie innovation in homeland security. During times of disaster, they provide response resources (donated or compensated)—including specialized teams, essential service providers, equipment, and advanced technologies—through public-private emergency plans/partnerships or mutual aid and assistance agreements, or in response to requests from government and nongovernmental-volunteer initiatives.

- **Small Businesses** contribute to all aspects of homeland security and employ more than half of all private-sector workers. They support response efforts by developing contingency plans and working with local planners to ensure that their plans are consistent with pertinent response procedures. When small businesses can survive and quickly recover from disasters, the Nation and economy are more secure and more resilient. They perform research and development, catalyze new thinking, and serve as engines of innovation for development of new solutions to key challenges in homeland security.

- **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, including the State's chief communicator

and primary source of information on the need for evacuations, the scope of the disaster, and the availability of assistance. Governors are commanders of their National Guards and are able to call them up 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** coordinate the activity of cities, counties, and intrastate regions. States administer Federal homeland security grants to local and tribal (in certain grant programs) 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. States 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 decisionmakers 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 capabilities with neighboring jurisdictions, and establish mutual aid agreements with other tribal governments, local jurisdictions, and State governments. Depending on location, land base, and resources, tribal governments provide law enforcement, fire, and emergency services as well as public safety to their members.

- **Mayors** and other local elected and appointed officials (such as city managers) 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 ensuring their governments are able to carry out emergency response activities. They serve as

both key decisionmakers and trusted sources of public information during incidents.

- **Local Governments** provide front-line leadership for local law enforcement, fire, public safety, environmental response, public health, and emergency medical services for all manner of hazards and emergencies. Through the Urban Areas Security Initiative (UASI) program, cities (along with counties in many cases) address multijurisdictional planning and operations, equipment support and purchasing, and training and exercises in support of high-threat, high-density urban areas. UASI grants assist local governments in building and sustaining homeland security capabilities. Local governments coordinate resources and capabilities during disasters with neighboring jurisdictions, NGOs, the State, and the private sector.

- **County Leaders** serve as chief operating officers of county governments, both rural and urban. This includes supporting and enabling the county governments to fulfill their responsibilities to constituents, including public safety and security. In some States, elected county officials such as sheriffs or judges also serve as emergency managers, search and rescue officials, and chief law enforcement officers.

- **County Governments** provide front-line leadership for local law enforcement, fire, public safety, environmental response, public health, and emergency medical services for all manner of hazards and emergencies. In many cases, county government officials participate in UASIs with other urban jurisdictions to assist local governments in building and sustaining capabilities to prevent, protect against, respond to, and recover from threats or acts of terrorism. County governments coordinate resources and capabilities during disasters with neighboring jurisdictions, NGOs, the State, and the private sector.

- The **American Red Cross** is a supporting agency to the mass care functions of ESF #6 – Mass Care, Emergency Assistance, Housing, and Human Services under the NRF. As the Nation's largest mass care service provider, the American Red Cross provides sheltering, feeding, bulk distribution of needed items, basic first aid, welfare information, and casework, among other services, at the local level as needed. In its role as a service provider, the American Red Cross works closely with local, tribal, and State governments to provide mass care services to victims of every disaster, large and small, in an affected area.

APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

- **National Voluntary Organizations Active in Disaster (National VOAD)** is a consortium of approximately 50 national organizations and 55 State and territory equivalents that typically send representatives to the Federal Emergency Management Agency's National Response Coordination Center to represent the voluntary organizations and assist in response coordination. Members of National VOAD form a coalition of nonprofit organizations that respond to disasters as part of their overall mission.

- **Nongovernmental Organizations (NGOs)** provide sheltering, emergency food supplies, counseling services, and other vital support services to support response and promote the recovery of disaster victims. They often provide specialized services that help individuals with special needs, including those with disabilities, and provide resettlement assistance and services to arriving refugees. NGOs also play key roles in engaging communities to integrate lawful immigrants into American society and reduce the marginalization or radicalization of these groups.

- **Communities** and community organizations foster the development of organizations and organizational capacity that act toward a common goal (such as Neighborhood Watch, Community Emergency Response Teams, or providing emergency food or shelter). These groups may possess the knowledge and understanding of the threats, local response capabilities, and special needs within their jurisdictions and have the capacity necessary to alert authorities of those threats, capabilities, or needs. Additionally, during an incident these groups may be critical in passing along vital incident communications to individuals and families, and to supporting critical response activities in the initial stages of a crisis.

- **Individuals and Families** take 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 pets and service animals), monitoring emergency communications carefully, volunteering with established organizations, mobilizing or helping to ensure community preparedness, enrolling in training courses, and practicing what to do in an emergency. These individual and family preparedness activities strengthen community resilience and mitigate the impact of disasters. In addition, individual vigilance and awareness can help communities remain safer and bolster prevention efforts.

APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

**Figure A-1. Emergency Support Functions and ESF Coordinators
(Source: National Response Framework)**

ESF #1 – Transportation **ESF Coordinator: Department of Transportation**	**ESF #8 – Public Health and Medical Services** **ESF Coordinator: Department of Health and Human Services**
• Aviation/airspace management/control • Transportation safety • Restoration and recovery of transportation infrastructure • Movement restrictions • Damage and impact assessments	• Public health • Medical • Mental health services • Mass fatality management
ESF #2 – Communications **ESF Coordinator: DHS (National Communications System)**	**ESF #9 – Search and Rescue** **ESF Coordinator: DHS (FEMA)**
• Coordination with telecommunications and information technology industries • Restoration and repair of telecommunications infrastructure • Protection, restoration, and sustainment of national cyber and information technology resources • Oversight of communications within the Federal incident management and response structures	• Life-saving assistance • Search and rescue operations
	ESF #10 – Oil and Hazardous Materials Response **ESF Coordinator: Environmental Protection Agency**
	• Oil and hazardous materials response • Environmental short- and long-term cleanup
ESF #3 – Public Works and Engineering **ESF Coordinator: Department of Defense (USACE)**	**ESF #11 – Agriculture and Natural Resources** **ESF Coordinator: Department of Agriculture**
• Infrastructure protection and emergency repair • Infrastructure restoration • Engineering services and construction management • Emergency contracting support for life-saving and life-sustaining services	• Nutrition assistance • Animal and plant disease and pest response • Food safety and security • Natural and cultural resources and historic properties protection • Safety and well-being of household pets
ESF #4 – Firefighting **ESF Coordinator: Department of Agriculture (U.S. Forest Service)**	**ESF #12 – Energy** **ESF Coordinator: Department of Energy**
• Coordination of Federal firefighting activities • Support to wildland, rural, and urban firefighting operations	• Energy infrastructure assessment, repair, and restoration • Energy industry utilities coordination • Energy forecast
ESF #5 – Emergency Management **ESF Coordinator: DHS (FEMA)**	**ESF #13 – Public Safety and Security** **ESF Coordinator: Department of Justice**
• Coordination of incident management and response efforts • Issuance of mission assignments • Resource and human capital • Incident action planning • Financial management	• Facility and resource security • Security planning and technical resource assistance • Public safety and security support • Support to access, traffic, and crowd control
ESF #6 – Mass Care, Emergency Assistance, Housing, and Human Services **ESF Coordinator: DHS (FEMA)**	**ESF #14 – Long-Term Community Recovery** **ESF Coordinator: DHS (FEMA)**
• Mass care • Emergency assistance • Disaster housing • Human services	• Social and economic community impact assessment • Long-term community recovery assistance to States, tribes, local governments, and the private sector • Analysis and review of mitigation program implementation
ESF #7 – Logistics Management and Resource Support **ESF Coordinator: General Services Administration and DHS**	**ESF #15 – External Affairs** **ESF Coordinator: DHS**
• Comprehensive, national incident logistics planning, management, and sustainment capability • Resource support (facility space, office equipment and supplies, contracting services, etc.)	• Emergency public information and protective action guidance • Media and community relations • Congressional and international affairs • Tribal and insular affairs

APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

Figure A-2. Sector-Specific Agencies
(Source: National Infrastructure Protection Plan)

Sector-Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture (a) Department of Health and Human Services(b)	Agriculture and Food
Department of Defense (c)	Defense Industrial Base
Department of Energy	Energy (d)
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water (e)

Department of Homeland Security
    Office of Infrastructure Protection
 	
    Federal Protective Service
	Chemical
	Commercial Facilities
	Critical Manufacturing
	Dams
	Emergency Services
	Nuclear Reactors, Materials, and Waste
	Government Facilities (f)

Office of Cybersecurity and Communications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration U.S. Coast Guard (h)	Transportation Systems (g)

a The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

b The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.

c Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

d The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

e The Water Sector includes drinking water and wastewater systems.

f The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector.

g As stated in Homeland Security Presidential Directive 7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

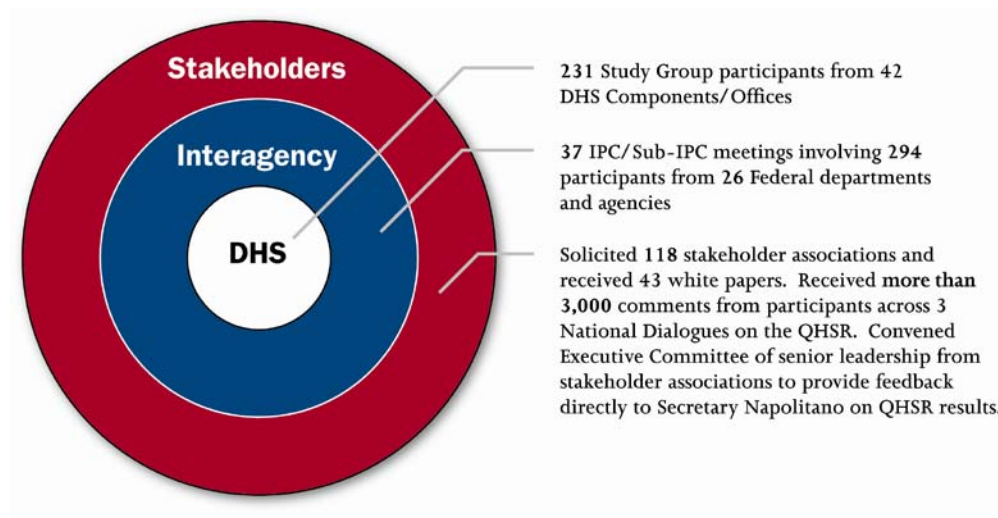h The U.S. Coast Guard is the SSA for the maritime transportation mode.

APPENDIX B: QUADRENNIAL HOMELAND SECURITY REVIEW PROCESS

Review Approach: Engagement Through Transparency and Collaboration

Section 2401 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* amends Title VII of the *Homeland Security Act of 2002* to require the Secretary of Homeland Security to conduct a Quadrennial Homeland Security Review (QHSR) every 4 years beginning in 2009. In doing so, the Department of Homeland Security (DHS) was directed to consult 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.

As noted in the QHSR report, homeland security is a distributed and diverse national enterprise. The term "enterprise" refers to the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities. It recognizes the diverse risks, needs, and priorities of these different stakeholders, and connotes a broad-based community with a common interest in the public safety and well-being of America and American society. Substantive and consistent engagement of stakeholders across the enterprise was therefore a requirement of conducting the first QHSR.

Figure B-1. Constituency Participation in the QHSR

Stakeholders

Interagency

DHS

231 Study Group participants from 42 DHS Components/Offices

37 IPC/Sub-IPC meetings involving 294 participants from 26 Federal departments and agencies

Solicited 118 stakeholder associations and received 43 white papers. Received **more than 3,000** comments from participants across 3 National Dialogues on the QHSR. Convened Executive Committee of senior leadership from stakeholder associations to provide feedback directly to Secretary Napolitano on QHSR results.

APPENDIX B: QUADRENNIAL HOMELAND SECURITY REVIEW PROCESS

In preparing the QHSR, the Department has benefited from the constructive engagement of thousands of dedicated individuals from across the country and, indeed, around the globe, including the key officials of DHS, the heads of other Federal agencies, and other relevant governmental and nongovernmental entities, including State, local, tribal, and territorial governments, as well as the broader public at large. Although numbers alone cannot capture the depth and vibrancy of the debates and discussions that occurred throughout the process of preparing the QHSR, the last 8 months engaged more than 100 stakeholder associations and more than 500 experts from government at all levels, as well as academia and the private sector. Our online National Dialogues had over 20,000 visits, with over 3,000 comments submitted.

Department of Homeland Security

The core of the QHSR approach was the formation of seven study groups that consisted of representatives from across DHS. The study groups were each led by a DHS official and facilitated by an independent subject-matter expert, both of whom ensured that all viewpoints were aired and that divergent opinions were brought forward. Consensus was not the object of the study group process; rather, it was to define the nature and purpose of the homeland security missions, describe the primary national tools required to enable those missions, *and identify and bring forward any major divergent points of view regarding the mission areas or national tools*. Specifically, the mission area study groups defined major goals, objectives, and key strategic outcomes for each of the homeland security mission areas. Three additional study groups examined homeland security national risk assessment, homeland security planning and capabilities, and DHS strategic management.

- **Study Groups:** In keeping with the inclusive approach of the review, over 200 participants from 42 DHS directorates, components, and offices made up the bulk of the study groups. The work of the DHS study group participants was supported by 35 subject-matter experts and research analysts from the Homeland Security Studies and Analysis Institute (HSSAI), the Department's federally funded research and development center. The study groups conducted their analysis over a 5-month period, with work products being consistently shared with the other stakeholder groups via different collaboration processes.

- **Steering Committee:** A Steering Committee, chaired by the Deputy Assistant Secretary for Policy (Strategic Plans) and composed of the DHS leads and independent facilitators of each of the study groups, as well as the Director of Program Analysis and Evaluation and representatives from the DHS Office of Intergovernmental Affairs, the Science and Technology Directorate, the Office of International Affairs, the Office of General Counsel, and the Office of

Intelligence and Analysis, convened weekly in person and by teleconference to ensure integration and consistency across the various studies. In addition, the Steering Committee held formal monthly in-progress reviews, during which each study group presented its progress towards developing its recommendations and brought forward unresolved questions and issues that required leadership consideration and decision.

- **DHS Senior Leadership Meetings:** More than a dozen DHS Deputy Secretary-led senior leadership meetings were held at the end of the study group deliberation period to review and concur on study group recommendations. Final decisions on the recommendations reflected departmental acknowledgement of the major themes around which the QHSR report was written.

Other Federal Departments and Agencies

DHS engaged with the White House National Security Staff to ensure robust interagency engagement and involvement with the QHSR. Specifically, interagency input was garnered through the following:

- **Sub-Interagency Policy Committees (Sub-IPCs):** Six special sub-IPCs were established by the National Security Staff to align with six of the QHSR study groups (the seventh study group, on DHS Strategic Management, was internally focused on DHS and therefore did not require a special sub-IPC) (see Figure B-2). The sub-IPCs were not venues for interagency *decisionmaking* on key issues; rather, they provided a forum for study groups to gather interagency input as study group content was developed. Over the course of the review, study groups held over 35 meetings that included approximately 294 Federal participants from 26 Federal departments and agencies through the special sub-IPCs, thereby ensuring interagency perspectives were solicited and represented in final study group recommendations.

- **Strategy Coordination Group:** In addition to the sub-IPCs, a special interagency Strategy Coordination Group was created to provide strategy and policy planners from across the interagency community an opportunity to share their feedback and perspectives on the review. Meeting monthly, the forum also allowed participants to identify issues being raised across multiple, similar strategic reviews and to share lessons learned and best practices on their respective reviews and planning processes.

APPENDIX B: QUADRENNIAL HOMELAND SECURITY REVIEW PROCESS

- **Interagency Processes:** The final QHSR report required vetting by interagency principals prior to delivery to Congress. Several Deputies Committee meetings were convened by the National Security Staff to discuss QHSR findings prior to the formal Office of Management and Budget (OMB) clearance process, allowing DHS to address major concerns before final interagency review. The OMB review process allowed Federal departments and agencies to formally comment on the QHSR report.

Figure B-2. Sub-Interagency Policy Committees and Interagency Participation
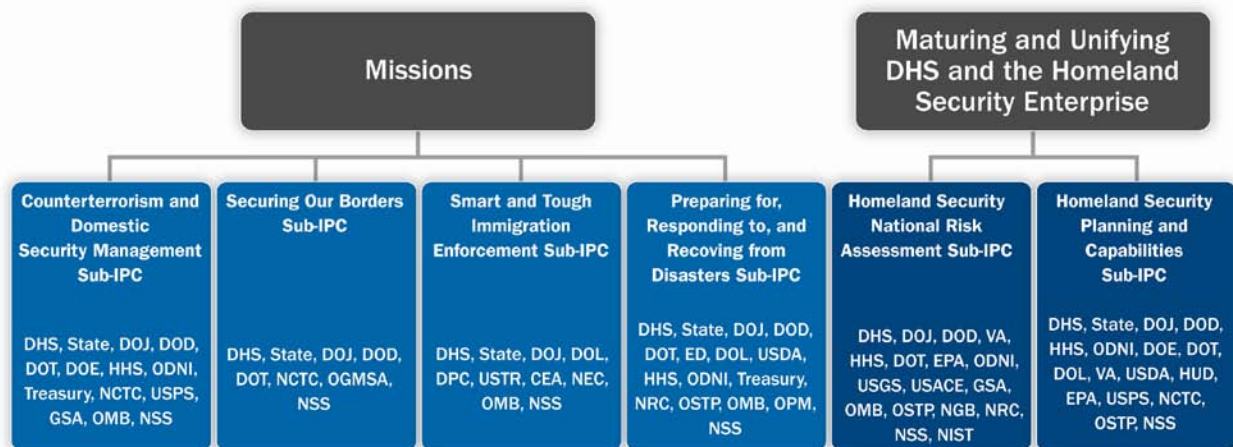
Congressional Engagement

Congressional engagement began during the preparatory phases of the QHSR and continued throughout the study period. DHS submitted an initial QHSR Resource Plan to Congress in early 2008, and the Deputy Assistant Secretary for Policy (Strategic Plans) testified before the House Homeland Security Committee, Subcommittee on Management, Investigations, and Oversight in July 2008. The DHS Office of Policy, together with the DHS Office of Program Analysis and Evaluation, also briefed staff from the House Homeland Security Committee, the Senate Homeland Security and Government Affairs Committee, and the House and Senate Appropriations Subcommittees on Homeland Security in 2008 regarding QHSR preparations.

In 2009, the DHS Office of Policy, together with the DHS Office of Program Analysis and Evaluation, conducted 17 briefings to congressional staff on QHSR status and process, including multiple briefings to staff from the House Homeland Security Committee, the Senate Homeland Security and Government Affairs Committee, and the House and Senate Appropriations Subcommittees on Homeland

APPENDIX B: QUADRENNIAL HOMELAND SECURITY REVIEW PROCESS

Security, as well as briefings to staff from the House Energy and Commerce Committee, the House Judiciary Committee, the House Transportation and Infrastructure Committee, the Senate Commerce Committee, and the Senate Judiciary Committee.

State, Local, Tribal, and Territorial Partners and Other Stakeholders

Several mechanisms were established to ensure the broadest possible outreach to critical State, local, and tribal partners as well as the general public.

- **Stakeholder Call for Comment:** The Secretary of Homeland Security began the QHSR study period with a letter to 118 homeland security stakeholder organizations representing State, local, tribal, territorial, nongovernmental, private-sector, and professional interests having roles and responsibilities in homeland security activities, inviting these organizations to submit papers and other materials relating to the QHSR study areas. Over 40 position papers were received and disseminated to study groups, and these papers helped to frame and inform the deliberations of the study groups. This *early engagement* of homeland security stakeholders at the beginning of the review process was a critical element of the QHSR.

- **National Dialogue on the QHSR:** *Sustained engagement* of the stakeholder community was another critical element of the QHSR. In a groundbreaking initiative, DHS held three online, collaborative "National Dialogue on the QHSR" sessions to capture the direct input and perspectives of a wide array of participants in the homeland security enterprise. Each National Dialogue presented study group materials that were posted for a period of 7 to 10 days for dialogue participants to rate and provide comment. The National Dialogues were open to anyone who wanted to provide input on QHSR content, although the Department engaged in deliberate outreach to several hundred organizations with interests in homeland security. Over the course of 3 dialogues, more than 20,000 visits were logged, resulting in over 3,000 comments on study group material. National Dialogue comments and content ratings were provided to the study groups who used the information to inform their iterative deliberations throughout the analytic period of the review. Revised study group materials were posted on each subsequent dialogue, demonstrating how materials evolved over the course of the review and showing participants how their comments informed study group work.

- **Executive Committee:** It would not have been possible to meaningfully convene representatives from all individual States, counties, cities, tribes, and territories to discuss QHSR findings. Therefore, DHS invited the leadership of

APPENDIX B: QUADRENNIAL HOMELAND SECURITY REVIEW PROCESS

10 key stakeholder associations that are broadly representative of State, local, tribal, and territorial governments to form the "virtual" QHSR Executive Committee. The Executive Committee consisted of the leaders of the following organizations: the National Governors Association, the Council of State Governments, the U.S. Conference of Mayors, the National League of Cities, the National Association of Counties, the National Council of State Legislatures, the National Congress of American Indians, the International City/County Management Association, the National Emergency Management Association, and the International Association of Emergency Managers. DHS held monthly teleconferences with the participating organizations throughout the analytic phase of the review to keep these organizations appraised of review progress. These organizations also participated in the collaborative events DHS held throughout the review, such as the Secretary's call for comment at the beginning of the review and the three National Dialogue sessions. Finally, on November 19, 2009, the Secretary of Homeland Security met in person with leadership representatives of the Executive Committee organizations to share key findings and recommendations of the QHSR. This in-person meeting provided key stakeholder associations the opportunity to comment on QHSR findings and recommendations in a similar manner to, and at a similar time as, Federal department and agency leadership.

APPENDIX C: ACRONYM LIST

CBRN   Chemical, Biological, Radiological, and Nuclear

CEA   Council of Economic Advisors

CERT   Community Emergency Response Team

CIKR   Critical Infrastructure and Key Resource

DHS   Department of Homeland Security

DOD   Department of Defense

DOE   Department of Energy

DOJ   Department of Justice

DOL   Department of Labor

DOT   Department of Transportation

DPC   Domestic Policy Council

ED   Department of Education

EPA   Environmental Protection Agency

ESF   Emergency Support Function

FEMA   Federal Emergency Management Agency

GSA   General Services Administration

HHS   Department of Health and Human Services

HSSAI   Homeland Security Studies and Analysis Institute

HUD   Department of Housing and Urban Development

IC   Intelligence Community

IPC   Interagency Policy Committee

NCTC   National Counterterrorism Center

NEC   National Economic Council

NGB   National Guard Bureau

NGO   Nongovernmental Organization

NIPP   National Infrastructure Protection Plan

NIST   National Institute of Standards and Technology

APPENDIX C: ACRONYM LIST

NRC   Nuclear Regulatory Commission

NRF   National Response Framework

NSS   National Security Strategy

ODNI   Office of the Director of National Intelligence

OGMSA   Office of Global Maritime Situational Awareness

OMB   Office of Management and Budget

OPM   Office of Personnel Management

OSTP   Office of Science and Technology Policy

QHSR   Quadrennial Homeland Security Review

SSA   Sector-Specific Agency

UASI   Urban Areas Security Initiative

USACE   U.S. Army Corps of Engineers

USDA   Department of Agriculture

USGS   U.S. Geological Survey

USPS   U.S. Postal Service

USTR   U.S. Trade Representative

VA   Department of Veterans Affairs

[National] Voluntary Organizations Active in Disaster
VOAD

WMD   Weapon(s) of Mass Destruction