

## Strategic Foundations of the Homeland Security Research Program

From distinct vantage points, several strategic plans guide the Homeland Security Research Program. Below, the most pertinent plans are introduced and the relevant portions of the plans are attached.

***National Strategy for Homeland Security (2007)***: This document presents the national view on how the United States will prepare for and respond to homeland security challenges. It states,

*“The purpose of our Strategy is to guide, organize, and unify our Nation’s homeland security efforts. It provides a common framework by which our entire Nation should focus its efforts on the following four goals:*

- 1. Prevent and disrupt terrorist attacks;*
- 2. Protect the American people, our critical infrastructure, and key resources;*
- 3. Respond to and recover from incidents that do occur; and*
- 4. Continue to strengthen the foundation to ensure our long-term success.”* (page 1).

The HS Research Program enhances the capability of the EPA to address the “critical infrastructure” component of Goal 2, and much of Goal 3’s mission of response and recovery. Goal 4 commits the nation to a science and technology program to address HS issues,

*“We will continue to build upon this foundation of scientific and technological advancement and support funding for research and development to further strengthen the security of the Homeland....Our collaborative S&T efforts should continue to explore existing or emerging technologies used for multiple or non-security specific purposes and develop rapid prototyping methods to adapt them to fill critical homeland security needs. Research in systems and operations science that will allow the integration of technology into functional capability is of equal importance....By promoting the evolution of current technologies and fielding new, revolutionary capabilities, S&T will remain an essential and enduring enabler of our Strategy.”* (pages 48-49).

The entire strategy is attached.

***EPA Strategic Plan (2006)***: In this document, EPA establishes five broad goals for protection of human health and the environment:

1. Clean Air and Global Climate Change,
2. Clean and Safe Water,
3. Land Preservation and Restoration,
4. Healthy Communities and Ecosystems, and
5. Compliance and Environmental Stewardship.

In Goals 1–3, consistent with the *National Homeland Security Strategy*, the Agency commits to carrying out its homeland security responsibilities regarding radiological

contamination, water security, and contaminated buildings and outdoor areas, respectively. In Goal 4, EPA supports the homeland security science needs of Goals 1-3 by establishing Homeland Security Research Program.

Relevant excerpts from the Plan are attached with the pertinent text highlighted in yellow. The entire Plan is available at: <http://www.epa.gov/ocfo/plan/plan.htm>

***EPA Homeland Security Strategy (2004)***: In this strategy, which supports the more general *EPA Strategic Plan*, the Agency establishes five broad mission-critical areas for EPA homeland security activities, two of which emphasize the requirements for research and development activities. Below, the mission-critical areas and the research-associated tactics included in the strategy are listed:

1. *Critical Infrastructure Protection*

- EPA will develop tools to better prevent, detect, mitigate, and/or recover from potential physical, cyber, chemical, biological, and radiological attacks to water utilities. EPA will prioritize the development of technical support based on the water sector's top vulnerabilities.
- EPA will work with stakeholders to identify the research and development needs in the areas of water security and rapid risk assessments to enhance the security of water and wastewater utilities.
- EPA will work with stakeholders to identify the necessary research and development in the areas of building security and rapid risk assessments to reduce the vulnerability of indoor air environments to chemical, biological and radiological incidents.

2. *Preparedness, Response, and Recovery*

- EPA will undertake research, development, testing, and communication/implementation of enhanced methods for detection and containment of biological and chemical warfare agents and bulk industrial chemicals intentionally introduced into large buildings/structures and for decontamination of building surfaces, furnishings, and equipment, with safe disposal of residual materials.
- EPA will undertake research, development, testing, and communication/implementation of enhanced methods for detection, treatment, and containment of biological and chemical warfare agents and bulk industrial chemicals intentionally introduced into drinking water systems.
- EPA will develop technical information, including practices and procedures for developing rapid assessments to aid decision-makers and response personnel in emergency situations.

3. *Communication and Information*

4. *Protection of EPA Personnel and Infrastructure*

5. *Evaluation*

The entire document is attached.

The *Homeland Security Research Multi-Year Plan* is built on the foundation of these strategies, as well as the National Infrastructure Protection Plan (NIPP), the water sector NIPP, Homeland Security Presidential Directives, the National Response Framework, and the Bioterrorism Act, among others.

NATIONAL STRATEGY FOR  
**HOMELAND  
SECURITY**



HOMELAND SECURITY COUNCIL  
OCTOBER 2007



NATIONAL STRATEGY FOR  
**HOMELAND  
SECURITY**



HOMELAND SECURITY COUNCIL  
OCTOBER 2007





## THE WHITE HOUSE

WASHINGTON

My fellow Americans,

More than 6 years after the attacks of September 11, 2001, we remain at war with adversaries who are committed to destroying our people, our freedom, and our way of life. In the midst of this conflict, our Nation also has endured one of the worst natural disasters in our history, Hurricane Katrina. As we face the dual challenges of preventing terrorist attacks in the Homeland and strengthening our Nation's preparedness for both natural and man-made disasters, our most solemn duty is to protect the American people. The *National Strategy for Homeland Security* serves as our guide to leverage America's talents and resources to meet this obligation.

Despite grave challenges, we also have seen great accomplishments. Working with our partners and allies, we have broken up terrorist cells, disrupted attacks, and saved American lives. Although our enemies have not been idle, they have not succeeded in launching another attack on our soil in over 6 years due to the bravery and diligence of many.

Just as our vision of homeland security has evolved as we have made progress in the War on Terror, we also have learned from the tragedy of Hurricane Katrina. We witnessed countless acts of courage and kindness in the aftermath of that storm, but I, like most Americans, was not satisfied with the Federal response. We have applied the lessons of Katrina to this *Strategy* to make sure that America is safer, stronger, and better prepared.

To best protect the American people, homeland security must be a responsibility shared across our entire Nation. As we further develop a national culture of preparedness, our local, Tribal, State, and Federal governments, faith-based and community organizations, and businesses must be partners in securing the Homeland.

This *Strategy* also calls on each of you. Every one of us should develop our own personal and family readiness plans to help protect us in the event of a natural or man-made disaster, enabling emergency responders and resources to be focused on those in greatest need.

Many of the threats we face – pandemic diseases, the proliferation of weapons of mass destruction, terrorism, and natural disasters – also demand multinational effort and cooperation. To this end, we have strengthened our homeland security through foreign partnerships, and we are committed to expanding and increasing our layers of defense, which extend well beyond our borders, by seeking further cooperation with our international partners.

As we secure the Homeland, however, we cannot simply rely on defensive approaches and well-planned response and recovery measures. We recognize that our efforts also must involve offense at home and abroad. We will disrupt the enemy's plans and diminish the impact of future disasters through measures that enhance the resilience of our economy and critical infrastructure before an incident occurs.

Today, our Nation is safer, but we are not yet safe. Since September 11, 2001, we have made great progress in confronting new challenges and refining our approach to homeland security. As acknowledged in 2002 in the first *National Strategy for Homeland Security*, we will not achieve all of our goals overnight, but we will achieve them. By the very nature of this struggle, many of our victories will be unheralded and achieved in silence.

Despite the difficult challenges ahead, we will fulfill our responsibility to safeguard America just as generations of Americans have before us. Together, guided by this *National Strategy for Homeland Security*, we will continue working to protect our families and communities, our liberty, and our way of life.

GEORGE W. BUSH

THE WHITE HOUSE

October 5, 2007

# CONTENTS

Overview of America's <i>National Strategy for Homeland Security</i> . . . . .	1
Today's Realities in Homeland Security . . . . .	3
Today's Threat Environment . . . . .	9
Our Vision and Strategy for Homeland Security . . . . .	13
Prevent and Disrupt Terrorist Attacks. . . . .	15
Protect the American People, Critical Infrastructure, and Key Resources . . . . .	25
Respond to and Recover from Incidents . . . . .	31
Ensuring Long-Term Success . . . . .	41
Conclusion . . . . .	53



---

## OVERVIEW OF AMERICA'S *NATIONAL STRATEGY FOR HOMELAND SECURITY*

America is at war with terrorist enemies who are intent on attacking our Homeland and destroying our way of life. The lives and livelihoods of the American people also remain at risk from natural catastrophes, including naturally occurring infectious diseases and hazards such as hurricanes and earthquakes, and man-made accidents. Our *National Strategy for Homeland Security* recognizes that while we must continue to focus on the persistent and evolving terrorist threat, we also must address the full range of potential catastrophic events, including man-made and natural disasters, due to their implications for homeland security.

The purpose of our *Strategy* is to guide, organize, and unify our Nation's homeland security efforts. It provides a common framework by which our entire Nation should focus its efforts on the following four goals:

- Prevent and disrupt terrorist attacks;
- Protect the American people, our critical infrastructure, and key resources;
- Respond to and recover from incidents that do occur; and
- Continue to strengthen the foundation to ensure our long-term success.

While the first three goals help to organize our national efforts, the last goal entails creating and transforming our homeland security principles, systems, structures, and institutions. This includes applying a comprehensive approach to risk management, building a culture of preparedness, developing a comprehensive Homeland Security Management System, improving incident management, better utilizing science and technology, and leveraging all instruments of national power and influence.

Homeland security requires a truly national effort, with shared goals and responsibilities for protecting and defending the Homeland. Our *Strategy* leverages the unique strengths and capabilities of all levels of government, the private and non-profit sectors, communities, and individual citizens. Mindful that many of the threats we face do not recognize geographic boundaries, we also will continue to work closely with our international partners throughout the world.

This updated *Strategy*, which builds directly from the first *National Strategy for Homeland Security* issued in July 2002, reflects our increased understanding of the terrorist threats confronting the United States today, incorporates lessons learned from exercises and real-world catastrophes – including Hurricane Katrina – and proposes new initiatives and approaches that will enable the Nation to achieve our homeland security objectives. This *Strategy* also complements both the *National Security Strategy* issued in March 2006 and the *National Strategy for Combating Terrorism* issued in September 2006.

Our first and most solemn obligation is to protect the American people. The *National Strategy for Homeland Security* will guide our Nation as we honor this commitment and achieve a more secure Homeland that sustains our way of life as a free, prosperous, and welcoming America.



---

# TODAY'S REALITIES IN HOMELAND SECURITY

## EVOLUTION OF THE PARADIGM

**T**he terrorist attacks on September 11, 2001, were acts of war against the United States and the principles of freedom, opportunity, and openness that define the American way of life. The severity and magnitude of the attacks were unprecedented, and that dark day became a watershed event in the Nation's approach to protecting and defending the lives and livelihoods of the American people.

Despite previous acts of terror on our Nation's soil – most notably the 1993 attack on the World Trade Center and the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City – homeland security before September 11 existed as a patchwork of efforts undertaken by disparate departments and agencies across all levels of government. While segments of our law enforcement and intelligence communities, along with our armed forces, assessed and prepared to act against terrorism and other significant threats to the United States, we lacked a unifying vision, a cohesive strategic approach, and the necessary institutions within government to secure the Homeland against terrorism.

### **Homeland Security Defined**

Homeland Security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.

The shock of September 11 transformed our thinking. In the immediate aftermath of history's deadliest international terrorist attack, we developed a homeland security strategy based on a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. In order to help implement that strategy, we enhanced our homeland security and counterterrorism architecture at the Federal, State, local, Tribal, and community levels.

Our understanding of homeland security continued to evolve after September 11, adapting to new realities and threats. As we waged the War on Terror both at home and abroad, our Nation endured Hurricane Katrina, the most destructive natural disaster in U.S. history. The human suffering and staggering physical destruction caused by Katrina were a reminder that threats come not only from terrorism, but also from nature. Indeed, certain non-terrorist events that reach catastrophic levels can have significant implications for homeland security. The resulting national consequences and possible cascading effects from these events might present potential or perceived vulnerabilities that could be exploited, possibly eroding citizens' confidence in our Nation's government and ultimately increasing our vulnerability to attack. This *Strategy* therefore recognizes that effective preparation for catastrophic natural disasters and man-made disasters, while not homeland security *per se*, can nevertheless increase the security of the Homeland.

---

## SHARED RESPONSIBILITY

Throughout the evolution of our homeland security paradigm, one feature most essential to our success has endured: the notion that homeland security is a shared responsibility built upon a foundation of partnerships. Federal, State, local, and Tribal governments, the private and non-profit sectors, communities, and individual citizens all share common goals and responsibilities – as well as accountability – for protecting and defending the Homeland.

The Federal Government as a united whole – and not simply one or two departments or agencies – has a critical role in homeland security and leads in those areas where it has a constitutional mandate or where it possesses the unique capabilities to address the most catastrophic or consequential scenarios. Those areas include, for example, border security; intelligence missions; and detecting, tracking, and rendering safe weapons of mass destruction (WMD). The Federal Government also is responsible for developing national strategies as well as promulgating best practices, national standards for homeland security, and national plans, as appropriate. It also uses targeted funding based on a risk management approach to help ensure that homeland security partners are capable of working together effectively and efficiently – in a truly national effort.

### **State and Local Governments**

This *Strategy* defines “State” to mean any State of the United States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, or the trust territory of the Pacific Islands. This *Strategy* also defines “local government” as any county, city, village, town, district, or other political subdivision of any State, and includes any rural community or unincorporated town or village or any other public entity for which an application for assistance is made by a State or political subdivision thereof.

America’s constitutional foundations of federalism and limited government place significant trust and responsibility in the capabilities of State and local governments to help protect the American people. State, local, and Tribal governments, which best understand their communities and the unique requirements of their citizens, provide our first response to incidents through law enforcement, fire, public health, and emergency medical services. They will always play a prominent, frontline role in helping to prevent terrorist attacks as well as in preparing for and responding to a range of natural and man-made emergencies.

The private and non-profit sectors also must be full partners in homeland security. As the country’s principal providers of goods and services, and the owners or operators of approximately 85 percent of the Nation’s critical infrastructure, businesses have both an interest in and a responsibility for ensuring their own security. The private sector plays key roles in areas as diverse as supply chain security, critical infrastructure protection, and research and development in science, technology, and other innovations that will help secure the Homeland. The non-profit sector, including volunteer and relief groups and faith-based organizations, provides important support services for the Nation, including meals and shelter, counseling, and compassion and comfort to Americans, particularly in the aftermath of an incident.

In order to complete this truly national effort, we also must encourage and draw upon an informed and active citizenry. For instance, citizens should each understand what to do if they observe suspicious behavior in their community and what to do in the event of an attack

---

or natural disaster – this will reduce the threat to lives and property as well as the burden on emergency managers and first responders.

Partnerships in homeland security also extend beyond our Nation's borders. International cooperation continues to be an enduring feature of our approach to terrorism and violent extremism, infectious diseases, and other threats that transcend jurisdictional and geographic boundaries. The United States will continue to develop and strengthen foreign partnerships and the homeland security capabilities of our friends and allies. Security at home ultimately is related to security abroad: as partners protect and defend their homelands, the security of our own Homeland increases.

## PROGRESS IN HOMELAND SECURITY AND BEYOND

We recognize that to the American people, progress should be measured not simply in terms of published plans or increased budgets; rather, it must be measured by the results that we achieve. Since September 11, we have made extraordinary progress, with most of our important successes in the War on Terror and in the full range of homeland security activities having been achieved through effective national and international partnerships. Our work, however, is far from over.

- We have greatly increased worldwide counterterrorism efforts since September 11, which has constrained the ability of al-Qaida to attack the Homeland and has led terrorist groups to find that the Homeland is a harder target to strike. These measures have helped disrupt multiple potentially deadly plots against the United States since September 11.
- We have instituted an active, multi-layered approach to securing the Homeland that integrates the capabilities of local, Tribal, State, and Federal governments, as well as those of the private and non-profit sectors, in order to secure the land, maritime, air, space, and cyber domains.
- We have made our borders more secure and developed an effective system of layered defense by strengthening the screening of people and goods overseas and by tracking and disrupting the international travel of terrorists.
- We have strengthened our ability to protect the American people by enhancing our homeland security and counterterrorism architecture through the creation of the Department of Homeland Security, the Office of the Director of National Intelligence, the Homeland Security Council, the National Counterterrorism Center, and U.S. Northern Command, a Department of Defense combatant command focused on homeland defense and civil support.
- The Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ) have made the prevention of terrorist attacks their highest priority, as evidenced by the creation of the FBI's new National Security Branch and DOJ's new National Security Division. We also have more effectively leveraged State, local, and Tribal law enforcement efforts as part of our national homeland security enterprise.
- Through the targeted risk-based delivery of Federal grant funding and technical assistance, we have enhanced State, local, and Tribal homeland security training and equipment, emergency management capabilities, and the interoperability of communications.

- 
- We have taken a series of historic steps to address biological threats, both deliberate and natural. These steps include unprecedented efforts to develop and procure medical countermeasures against bioterrorism and pandemic threats, improve capabilities for the detection of and response to biological attacks, and support State, local, and Tribal preparedness efforts through funding and explicit guidance.
  - We have worked with the Congress to create, implement, and renew key legal reforms – such as the USA PATRIOT Act, the Intelligence Reform and Terrorism Prevention Act of 2004, and the Protect America Act of 2007 – which promote security and help to implement both the 9/11 Commission and the WMD Commission recommendations while protecting our fundamental liberties. Furthermore, with the Military Commissions Act of 2006, the United States can prosecute captured terrorists for war crimes through full and fair trials.
  - Since September 11, the Administration has worked with the Congress to establish the Privacy and Civil Liberties Oversight Board as an integral part of the Executive Branch, and we have further established privacy officers in departments and agencies across the Federal Government – all to ensure that the rights of American citizens are considered and respected in our counterterrorism efforts.
  - We have created a full-scale, comprehensive National Exercise Program to increase our preparedness to respond to the consequences of terrorist attacks and natural disasters.

## CHALLENGES IN HOMELAND SECURITY AND BEYOND

While America is safer, we are not yet safe. Because of determined terrorist enemies and nature's unyielding power, significant challenges remain, including:

- The War on Terror remains a generational struggle, and our entire Nation must be engaged and prepared to participate in this effort.
- Terrorists have declared their intention to acquire and use weapons of mass destruction (WMD) to inflict catastrophic attacks against the United States and our allies, partners, and other interests.
- Our vast land and maritime borders make it difficult to completely deny terrorists and their weapons access to the Homeland.
- The United States is not immune to the emergence of homegrown radicalization and violent Islamic extremism.
- We must counter potential waning in the sense of urgency and levels of international cooperation as September 11 becomes a more distant memory and perceptions of the terrorist threat diverge.
- We must guard against complacency and balance the sense of optimism that is fundamental to the American character with the sober recognition that despite our best efforts, future catastrophes – natural and man-made – will occur, and thus we must always remain a prepared Nation.
- Although we have substantially improved our cooperation and partnership among all levels of government, private and non-profit sectors, communities, and individual citi-

---

zens, we must continue to strengthen efforts to achieve full unity of effort through a stronger and further integrated national approach to homeland security.

- Although we have improved our ability to manage the risks that we face in the 21<sup>st</sup> century global security environment, we must enhance our ability to measure risk in a consistent and commonly accepted fashion and allocate finite resources accordingly.
- We must make additional reforms to the Foreign Intelligence Surveillance Act (FISA) and ensure that the statute is permanently amended so that our intelligence professionals continue to have the legal tools they need to gather information about the intentions of our enemies while protecting the civil liberties of Americans.
- While our information sharing capabilities have improved significantly, substantial obstacles remain. We must continue to break down information barriers among Federal, State, local, and Tribal partners and the private sector.
- The Congress must better align its oversight and committee structure in order to reflect the need for streamlined and effective legislative action that supports a unified approach to securing the Nation.



---

## TODAY'S THREAT ENVIRONMENT

Our Nation faces complex and dynamic threats from terrorism. In addition, other threats from catastrophic events – including natural disasters, accidents, and other hazards – exist and must be addressed. We will continue to advance our understanding of these threats so we are better able to safeguard the American people.

### TERRORISM

Despite concerted worldwide efforts in the aftermath of September 11 that have disrupted terrorist plots and constrained al-Qaida's ability to strike the Homeland, the United States faces a persistent and evolving terrorist threat, primarily from violent Islamic terrorist groups and cells.

Currently, the most serious and dangerous manifestation of this threat remains al-Qaida, which is driven by an undiminished strategic intent to attack our Homeland. Although earlier efforts in the War on Terror deprived al-Qaida of its safe haven in Afghanistan and degraded its network by capturing or killing most of those responsible for September 11, the group has protected its top leadership, replenished operational lieutenants, and regenerated a safe haven in Pakistan's Federally Administered Tribal Areas – core capabilities that would help facilitate another attack on the Homeland.

Al-Qaida likely will continue to enhance its ability to attack America through greater cooperation with regional terrorist groups, particularly al-Qaida in Iraq – currently the group's most visible and capable affiliate and the only one known to have expressed a desire to attack us here. Moreover, although we have discovered only a handful of individuals in the United States with ties to al-Qaida senior leadership, the group likely will intensify its efforts to place operatives here in the Homeland. We also must never lose sight of al-Qaida's persistent desire for weapons of mass destruction, as the group continues to try to acquire and use chemical, biological, radiological, or nuclear material.

In addition to al-Qaida, a host of other groups and individuals also use terror and violence against the innocent in pursuit of their objectives and pose potential threats to the security of the United States. These include Lebanese Hizballah, which has conducted anti-U.S. attacks outside the United States and, prior to September 11, was responsible for more American deaths than any other terrorist organization. Hizballah may increasingly consider attacking the Homeland if it perceives the United States as posing a direct threat to the group or Iran, its principal sponsor.

The United States also is not immune to the emergence of homegrown radicalization and violent Islamic extremism within its borders. The arrest and prosecution inside the United States of a small number of violent Islamic extremists points to the possibility that others in the Homeland may become sufficiently radicalized to view the use of violence within the United States as legitimate. While our constitutional protection of freedom of religion, history of welcoming and assimilating new immigrants, strong economic opportunities, and equal-opportunity protections may help to mitigate the threat, drivers of radicalization still exist.

---

We will continue efforts to defeat this threat by working with Muslim American communities that stand at the forefront of this fight.

The terrorist threat to the Homeland is not restricted to violent Islamic extremist groups. We also confront an ongoing threat posed by domestic terrorists based and operating strictly within the United States. Often referred to as “single-issue” groups, they include white supremacist groups, animal rights extremists, and eco-terrorist groups, among others.

## CATASTROPHIC NATURAL DISASTERS

Our *National Strategy for Homeland Security* recognizes that the lives and livelihoods of the American people also are at risk from natural catastrophes. Our vast Nation, with its varied population, geography, and landscape, will continue to endure a range of natural hazards and disasters.

Naturally occurring infectious diseases pose a significant and ongoing hazard. Increasing human contact with domesticated and wild animals (from which many human diseases emerge), the growing speed and volume of global travel and commerce, and a decline in the development of new infectious disease therapeutics complicate this challenge. In 2003, Severe Acute Respiratory Syndrome (SARS) demonstrated the potential for a global impact of a novel infectious disease. Originating in rural China, SARS resulted in more than 8,000 infections and 800 deaths worldwide and significant economic and social disruptions. The emergence of another novel disease without a known countermeasure, or a new influenza pandemic, could have dramatically greater consequences. Influenza pandemics have occurred intermittently over the centuries. The last three pandemics – in 1918, 1957, and 1968 – killed approximately 40 million, two million, and one million people worldwide, respectively. Although the timing cannot be predicted, history and science suggest that we will face one or more pandemics in this century.

Natural disasters also encompass a variety of meteorological and geological hazards. Hurricanes, for example, account for seven of the ten most costly disasters in U.S. history, including Hurricane Katrina – the Nation’s most destructive natural disaster. While experts differ on the predicted intensity and frequency of future storms, history suggests the question is not if, but when, a devastating hurricane will reach our shores again. Earthquakes also will continue to be part of the hazard landscape. Although major advances have been achieved in understanding and mitigating earthquake hazards, Americans in 39 States face significant risk from earthquakes. Additionally, although each incident is often less significant than major hurricanes and earthquakes, floods are the most frequently occurring natural disaster and the leading cause of property damage and death from natural disasters in the Homeland over the past century. In an average year, more than 800 tornadoes are reported nationwide, resulting in 80 deaths and more than 1,500 injuries. In addition, wildfires remain a persistent hazard throughout many regions of the country.

## CATASTROPHIC ACCIDENTS AND OTHER HAZARDS

We also remain vulnerable to catastrophic domestic accidents involving industrial hazards and infrastructure failures. These include the thousands of chemical spills that occur each year with the potential for significant public health and environmental impacts. In addition,

---

incidents that pose potential threats to our Nation's critical infrastructure can lead to significant cascading effects across multiple systems. For example, an estimated 50 million people across eight States and the Canadian province of Ontario were left without electrical power in August 2003 when a utility in Ohio experienced problems that began a chain reaction of events leading to power outages lasting, in some places, several days. This incident, known as the "Northeast Blackout of 2003," cost roughly \$6 billion and caused at least 265 power plants to shut down.



---

## OUR VISION AND STRATEGY FOR HOMELAND SECURITY

**W**e are a Nation blessed with unprecedented liberty, opportunity, and openness – foundations of the American way of life. Our principal terrorist enemies – al-Qaida, its affiliates, and those inspired by them – seek to destroy this way of life. Al-Qaida’s plotting against our Homeland, for instance, focuses on prominent political, economic, and infrastructure targets designed to produce mass casualties, visually dramatic destruction, significant economic damage, fear, and loss of confidence in government among our population. Catastrophic events, including natural disasters and man-made accidents, also can produce similar devastating consequences that require an effective and coordinated national effort.

The United States, through a concerted national effort that galvanizes the strengths and capabilities of Federal, State, local, and Tribal governments; the private and non-profit sectors; and regions, communities, and individual citizens – along with our partners in the international community – will work to achieve a secure Homeland that sustains our way of life as a free, prosperous, and welcoming America.

In order to realize this vision, the United States will use all instruments of national power and influence – diplomatic, information, military, economic, financial, intelligence, and law enforcement – to achieve our goals to prevent and disrupt terrorist attacks; protect the American people, critical infrastructure, and key resources; and respond to and recover from incidents that do occur. We also will continue to create, strengthen, and transform the principles, systems, structures, and institutions we need to secure our Nation over the long term.

This is our strategy for homeland security.



---

## PREVENT AND DISRUPT TERRORIST ATTACKS

In the aftermath of the September 11 attacks, the United States, together with partners across the globe, has waged an unrelenting War on Terror both to hold the perpetrators accountable and to prevent the recurrence of similar atrocities on any scale, whether at home or abroad.

The updated *National Strategy for Combating Terrorism*, released in September 2006, articulates our strategy for winning the War on Terror. Over the short term we are working to prevent attacks by terrorist networks, deny weapons of mass destruction (WMD) to rogue states and terrorists who seek to use them, deny terrorists the support and sanctuary of rogue states, and deny terrorists control of any nation they would use as a base and launching pad for terror. From the beginning, however, we recognized that the War on Terror is a different kind of war – not only a battle of arms but also a battle of ideas. Accordingly, we are advancing effective democracy as the antidote to the ideology of our terrorist enemies and the long-term solution for winning the War on Terror.

This *National Strategy for Homeland Security* is a companion to the *National Strategy for Combating Terrorism*, and the sections in both on preventing and disrupting terrorist attacks are complementary and mutually reinforcing. In order to prevent and disrupt terrorist attacks in the United States, we are working to deny terrorists and terrorist-related weapons and materials entry into our country and across all international borders, disrupt their ability to operate within our borders, and prevent the emergence of violent Islamic radicalization in order to deny terrorists future recruits and defeat homegrown extremism.

### Preventing WMD Terrorism

The intent of our principal terrorist enemies to inflict catastrophic damage on the United States, coupled with their demonstrated contempt for human life, has fueled their desire to acquire WMD. Among our most important missions in denying entry to terrorists, their weapons, and other implements of terror is to detect, disrupt, and interdict the movement of WMD-related materials into the Homeland. This is one objective in our comprehensive strategy to prevent WMD terrorism, which is fully discussed in the *National Strategy for Combating Terrorism*. By integrating the operational and intelligence efforts of all levels of government, the private sector, and our foreign partners, and enabled by an international framework and domestic institutions supporting its implementation, our strategy involves simultaneous action to:

- Determine terrorists' intentions, capabilities, and plans to develop or acquire WMD;
- Deny terrorists access to the material, expertise, and other enabling capabilities required to develop WMD;
- Deter terrorists from employing WMD;
- Detect and disrupt terrorists' attempted movement of WMD-related materials, weapons, and personnel;
- Prevent and respond to a WMD-related terrorist attack; and
- Define the nature and source of a terrorist-employed WMD device.

WMD in the hands of terrorists is one of the gravest threats we face, and we cannot permit the world's most dangerous terrorists to threaten us with the world's most destructive weapons.

---

## DENY TERRORISTS, THEIR WEAPONS, AND OTHER TERROR-RELATED MATERIALS ENTRY TO THE HOMELAND

Denying our terrorist enemies the ability to travel internationally and, particularly, across and within our borders, severely inhibits their effectiveness. By preventing terrorists and their implements of destruction from entering the United States, we hinder their ability to identify and surveil possible targets, conduct planning, and launch an attack within our Homeland. Our *National Strategy to Combat Terrorist Travel*, *National Strategy for Maritime Security*, and *National Strategy for Aviation Security* are helping to guide our efforts. While we have strengthened travel and document security, improved information sharing with our domestic and international partners, and enhanced the screening of all visitors and cargo to the United States, our principal terrorist enemies are determined to infiltrate operatives and attack us on our soil. They also remain adaptive, exploiting perceived weaknesses in our dynamic travel system and using illicit means to circumvent our border and transportation security. We will defeat terrorists' efforts to infiltrate our Homeland while continuing to promote the reliable and efficient flow of people, goods, and services across our borders that is essential to American openness and economic prosperity.

- ***Prevent terrorist exploitation of legitimate pathways into the Homeland.*** Continuing to strengthen our layered system of protections that start overseas and continue along our borders, at our ports, on our roadways and railways, and in our skies is fundamental to preventing terrorists, their weapons, and related materials from entering our country through exploitation of legitimate pathways. In order to do this, we must continue to act deliberately on several fronts. A critical component of screening people is travel document security, because official documents are the key enablers for screening all people at ports of entry. The Western Hemisphere Travel Initiative and

### **Border Security and Interior Enforcement**

As part of our broader effort for comprehensive immigration reform, we will work to further secure the Homeland and disrupt terrorist and other criminal activity in the United States. This includes improving our ability to detain and remove criminal and fugitive aliens and visa violators. We will continue to hire, train, and deploy additional Border Patrol agents, Customs and Border Protection officers, and Immigration and Customs Enforcement officers, as well as to build on the substantial improvements to the infrastructure and technology deployed at our borders. Additionally, we will expand detention bed space for aliens subject to detention and removal.

At the same time, we will enhance interior enforcement efforts, including worksite enforcement programs. Employers should be required to verify the work eligibility of all employees, preventing illegal immigrants from obtaining jobs through fraud or the use of stolen identification, including Social Security numbers. In order to accomplish this, we must expand the use of an electronic employment eligibility verification system that is timely, accurate, and easy for employers to use. We also will continue to crack down on employers who knowingly hire illegal immigrants by applying criminal penalties to those who circumvent the law. In addition, we will continue to step up efforts to verify the status of non-immigrants studying in the United States through the Student and Exchange Visitor Information System (SEVIS) and have appropriate follow-up where there may be violations. Taken together, these efforts will reinforce significantly enhanced border and interior security and help deny employment to those who are present in our country illegally, including criminals and potential terrorists.

the REAL ID Act are additional efforts to improve the integrity of documents used for entry into the United States. Enhancing international security standards through the use of biometrics, including in passports and visas, has made it increasingly difficult to counterfeit travel documents, and we must encourage those countries not in the Visa Waiver Program to adopt biometric passports. In the face of resourceful terrorists, however, we must continue to expand the US-VISIT program's biometric enrollment from two fingerprints to ten fingerprints, as well as leverage science and technology to enable more advanced multi-modal biometric recognition capabilities in the future that use fingerprint, face, or iris data. In order to further enhance travel document security, we will continue to press our international partners to strengthen and fully enforce laws criminalizing the counterfeiting, alteration, and misuse of identification and travel documents, and

to report lost and stolen passports in a timely manner. These efforts build on the Department of State's screening for fraudulent passports and other documents through the visa interview process and U.S. Customs and Border Protection's examination of passports and visas for evidence of fraud during the admissions process.

By improving the screening of visa applicants, we also can help control access through ports of entry. Improved screening means enhancing our ability to more effectively identify prospective travelers who pose security threats through improved interview techniques, background checks, and the collection and comparison of biometrics. This includes expanding the use of security personnel abroad who are focused on assessing security threats and fraudulent documents used in the visa application process. It also means that we will continue to work with our foreign partners to share terrorist watchlists and to ensure other relevant electronic databases are accurate, up-to-date, and well-managed.

### Screening People

- The **REAL ID Act** establishes Federal standards for State-issued driver's licenses and non-driver's identification cards.
- **Secure Flight** will require airlines to submit passenger information to DHS for flights that operate to, from, and within the United States, as well as those that fly over the continental United States.
- The **Student and Exchange Visitor Information System (SEVIS)** is an internet-based system that is improving America's ability to track and monitor foreign students and exchange visitors.
- The **United States Visitor and Immigrant Status Indicator Technology (US-VISIT)** program, when fully implemented, will create an entry and exit system that matches foreign travelers' arrival and departure records using biometrics to screen applicants for admission to the United States.
- The **Western Hemisphere Travel Initiative (WHTI)** reduces the number of identification and citizenship documents that may be used by persons entering or re-entering the United States, from more than 8,000 documents, to a few dozen secure documents. This expedites document review at ports of entry while combating fraudulent documents.
- The **Visa Waiver Program (VWP)** enables nationals of over two dozen countries to travel to the United States for tourism or business for stays of 90 days or less without obtaining a visa.

Terrorists also can exploit the global supply chains through which cargo enters the United States to smuggle their tools of terror, including possibly WMD. To counter this potential infiltration, and particularly to prevent the introduction of nuclear and radiological material into the Homeland, we will continue to expand the type of information we collect and improve cargo screening, scanning, and detection procedures and systems at foreign ports. Enhancing the Container Security Initiative, Megaports Initiative, and Secure Freight Initiative, among other international, multilateral, and bilateral efforts, is an important step toward developing a more robust global inspection and detection architecture for the 21st century. We will combine these efforts with strengthened interdiction measures for all types of cargo and all modes of transport to further constrain the mobility of terrorists, their weapons, and other material. We also will continue to strengthen and enhance screening, scanning, and detection capabilities at all U.S. maritime ports and land ports of entry for cargo entering, leaving, and moving within the country.

Additionally, in order to improve the security of international commercial systems and supply chains, the United States will enhance the Customs-Trade Partnership Against Terrorism to further develop public-private partnerships with the full range of partners involved in commerce and transportation. The private sector is central to improving security along the entire supply chain – from the factory floor to foreign vendors, at seaports, and across borders. This integrated public-private partnership also will be important in stimulating the development and implementation of best practices, risk management approaches, and industry codes of conduct. Risk assessment is a critical element of corporate valuations, so companies that minimize risk will be rewarded by the market.

- ***Prevent terrorist use of illicit pathways into the Homeland.*** While some terrorists will continue to exploit legitimate channels to move personnel and weapons into and within our country, others might attempt to infiltrate our land, maritime, and air borders by car, truck, rail, foot, boat, or aircraft. In order to disrupt the use of illicit pathways into the Homeland, we will continue to implement an integrated system of people, technology, and tactical infrastructure through the Secure Border Initiative to detect, identify,

### Screening Cargo

- The **Container Security Initiative** (CSI) creates a security regime to prescreen and evaluate maritime containers – before they are shipped from foreign ports – through automated targeting tools, ensuring that high-risk cargo is examined or scanned.
- The **Customs-Trade Partnership Against Terrorism** (C-TPAT) is a voluntary U.S. Customs and Border Protection program whereby participating businesses undergo a review of security procedures and adopt enhanced security measures in order to expedite shipping.
- The **Megaports Initiative** is a Department of Energy program in which the United States collaborates with foreign trade partners to enhance their ability to scan cargo for nuclear and other radiological materials at major international seaports.
- The **Secure Freight Initiative** is a comprehensive model for securing the global supply chain that seeks to enhance security while keeping legitimate trade flowing. It leverages shipper information, host country government partnerships, and trade partnerships to scan cargo containers bound for the United States.

---

respond to, and resolve illegal entry attempts at our land borders. We also will enhance and improve the coordination of surveillance of watercraft and general aviation. We will work with our neighbors and international partners to shrink the illicit travel networks used by human smugglers, narco-traffickers, and other transnational criminals whose activities foster continued exploitation of our borders.

## DISRUPT TERRORISTS AND THEIR CAPACITY TO OPERATE IN THE UNITED STATES

The United States and our partners and allies are attacking terrorists and their networks in a campaign of direct and continuous action to deny them what they need to operate and survive overseas. We are on the offense at home, too – taking the fight to an enemy that exploits our open and diverse society, hides among us, and tries to attack us from within. Leveraging our Nation’s foundation of homeland security partnerships, as well as our relationships with committed friends across the globe, we will work to uncover terrorists and terrorist activity within our borders and take swift and effective action to preempt and disrupt their activities and enterprises. The Federal Government must ensure that we have the necessary and appropriate legal tools to accomplish these objectives while at the same time preserving the rights and civil liberties of all Americans.

- **Identify and locate terrorists and uncover terrorist activity.** In order to uncover terrorists and terrorist activity against the backdrop of our highly mobile, dynamic, and diverse society, we must attain domain awareness of the actions, events, and trends that occur throughout our land, maritime, air, space, and cyber domains. This is a multifaceted process. First, partners throughout the entire law enforcement community must continue to enhance their baseline understanding of their operating environments – the people, the geography, and the daily and weekly rhythm of activities and events. By understanding trend lines, we can better identify anomalies and deviations that could indicate terrorist activity. The reporting of unusual or suspicious activity by private sector partners and a vigilant public also is essential to this effort. Identifying terrorists and detecting terrorist activity and plotting also require a greater understanding of how suspect activities at the local level relate to the strategic environment. Our law enforcement and intelligence communities must have detailed knowledge of our Homeland adversaries, including their identities, sources of support, intentions, capabilities, and *modi operandi*. This information must be assessed against a current strategic threat picture that continues to integrate national intelligence.

In order to enhance our domain awareness as well as improve our understanding of how terrorist enemies are likely to operate in the Homeland, the law enforcement community, along with the intelligence community, must work to develop and imple-

### Intelligence-Led Policing

Intelligence-Led Policing (ILP) is a management and resource allocation approach to law enforcement using data collection and intelligence analysis to set specific priorities for all manner of crimes, including those associated with terrorism. ILP is a collaborative approach based on improved intelligence operations and community-oriented policing and problem solving, which the field of law enforcement has considered beneficial for many years. Today it is being adopted by a variety of law enforcement entities.

---

ment national information requirements – developing a process for identifying information gaps, determining critical information requirements, and meeting those requirements collaboratively. We also must encourage the implementation of Intelligence-Led Policing by State, local, and Tribal law enforcement – after all, they best understand their communities, citizens, and current trend lines. Working in a collaborative environment, the Federal Government will recommend priorities for State, local, and Tribal homeland security activities that focus resources on the most pressing problems, adopt a formal intelligence process with requirements generation and tasking of information collection, and analyze and disseminate the information. Underlying our efforts to achieve domain awareness and identify and locate terrorists and terrorist activity in the Homeland is a fully developed and integrated Information Sharing Environment (see the chapter titled “Ensuring Long-Term Success”) that supports the vertical and horizontal distribution of terrorism-related information among Federal, State, local, Tribal, and foreign governments and the private sector, as appropriate.

- ***Disrupt terrorists and their activities and networks.*** As we achieve domain awareness throughout our communities, our Federal, State, local, and Tribal law enforcement authorities will collaborate to investigate, disrupt, and preempt terrorist activity and deny terrorists the capacity to operate effectively within our borders. This means targeting all elements of a network that terrorists need to operate and survive. For instance, we will investigate, arrest, and prosecute or, where appropriate, remove terrorist leaders, operatives, facilitators, and trainers. We also will freeze or seize terrorist funds, disrupt funding sources, and interdict their financing transfer mechanisms. Furthermore, we will focus on criminal behavior and other terrorist financing methodologies that terrorist groups or cells may use to finance or otherwise facilitate their activities.

#### **Improvised Explosive Devices**

Over the past several years, al-Qaida – our principal terrorist enemy – has demonstrated its ability and intent to employ innovative weapons against U.S. interests, including in the Homeland, and our friends and allies overseas. The disrupted 2006 U.K.-based plot to blow up multiple trans-Atlantic commercial airliners with liquid explosives is especially noteworthy. We remain particularly concerned about the employment of improvised explosive devices (IEDs) in an attack against the Homeland, given the ready availability of IED components and the relative technological ease with which they can be fashioned. In conjunction with an array of activities to deny terrorists the weapons and tools they use to kill the innocent, our *National Strategy for Combating Terrorist Use of Explosives*, which is being developed pursuant to Homeland Security Presidential Directive-19 (issued February 12, 2007), will help guide our efforts.

We also will work with domestic and international partners to deny terrorists what they need to operate in the Homeland, including the weapons and tools they use to kill the innocent. These include missiles, rockets, explosives, and small arms acquired through a variety of means, including theft, fraud, state sponsor support, and black market purchases. Terrorists and their state sponsors also may exploit dual-use technologies, including technologies that are being used for great benefit in medicine, agriculture, and industry. We will stringently enforce our export control laws as a means of denying rogue actors – including terrorist groups – access to restricted dual-use items. We will

---

work with our private sector and international partners to ensure the presence of industry standards, national systems of oversight, and penalties for misuse of such items while preserving the advancement of science and technology to save lives and improve our quality of life.

Defeating terrorist activity in the Homeland also requires preventing terrorist exploitation of our financial, cyber, and legal systems. Terrorists use financial systems to raise, store, and transfer funds that serve as the lifeblood of their operations. We have hardened U.S. financial systems against terrorist abuse by building upon our anti-money laundering system and broadening and deepening safeguards in the international financial system while taking steps to deter and disrupt specific terrorist funding. We have done this in large part by building strong international law enforcement alliances and effective public-private partnerships committed to preventing the flow of illicit capital through formal and informal financial mechanisms. We will continue to strengthen this approach and use intelligence, law enforcement, and regulatory steps, such as our targeted financial sanctions, to identify and isolate actors involved in terrorist financing.

Terrorists also seek sanctuary in the cyber domain, particularly the Internet, an inexpensive, geographically unbounded, and largely unconstrained virtual haven for our enemies. Terrorists use the Internet to create and disseminate propaganda, recruit new members, raise funds, and plan operations. The Internet has become a training ground, with terrorists acquiring instruction once possible only through physical training camps. In addition to discrediting their terrorist propaganda on the Internet with the promotion of truthful messages, we will seek to deny the Internet to our terrorist enemies as an effective safe haven for their recruitment, fund-raising, training, and operational planning.

### **Foreign Intelligence Surveillance Act Modernization**

Since its enactment in 1978, the Foreign Intelligence Surveillance Act (FISA), as amended, has provided a legal framework through which the Intelligence Community lawfully collects foreign intelligence information of value to our Nation's security, while simultaneously protecting the civil liberties of Americans. Revolutionary changes in technology since 1978 had the effect of expanding the scope of FISA's coverage to include foreign intelligence collection efforts that Congress did not intend to subject to the statute's requirements. This unintended expansion of FISA's scope meant that our intelligence professionals, in a significant number of cases, needed to obtain a court order to collect foreign intelligence information against a target located overseas. This circumstance created an unnecessary obstacle to our Intelligence Community's ability to gather real-time information about the intent of our enemies overseas and diverted scarce resources that would be better spent safeguarding the civil liberties of people in the United States, not foreign terrorists who wish to do us harm. The Protect America Act of 2007, which passed with bipartisan support in the House and the Senate, was an important interim step in modernizing FISA to account for modern changes in technology and the threats that we face in the 21<sup>st</sup> century. Working with Congress, we must make additional reforms to FISA and ensure that the statute is permanently amended so that our intelligence professionals continue to have the legal tools they need to gather information about the intentions of our enemies while protecting the civil liberties of Americans – now and in the future.

---

The United States has a domestic legal system that supports the investigation and prosecution of terrorist activities while simultaneously protecting individual privacy, the First Amendment rights of association, religious freedom, and free speech, and other civil liberties. We are a Nation built on the rule of law, and we will apply our laws to defeat terrorism while always preserving our liberties. Toward that end, not only must we guard against any gaps in our system that would offer terrorists a virtual haven to exploit, but we also must ensure that our law enforcement community has the necessary and proper mix of tools and authorities to defeat the threats of the 21<sup>st</sup> century.

## PREVENT VIOLENT ISLAMIC EXTREMIST RADICALIZATION IN THE UNITED STATES

The arrest and prosecution inside the United States of a small number of violent Islamic extremists demonstrates that we are not immune to the emergence of homegrown violent Islamic extremism. Potential catalysts for radicalization within Muslim American communities include feelings or perceptions of social discrimination that generate a sense of alienation from society and distrust of the government; perceptions of political and economic inequalities; and dissatisfaction with foreign and domestic U.S. policies viewed as hostile to Muslims. Preventing and disrupting radicalization requires concerted, focused action in the near term. While our *Strategy* focuses on preventing homegrown violent Islamic extremism – the ideology underpinning the principal terrorist threat confronting the United States today – we recognize that terrorists and violent extremists can arise in many other faiths, communities, or persuasions. Accordingly, our *Strategy* can be appropriately tailored to address a variety of domestic communities and groups whose members may be susceptible to radicalization.

- ***Engage key communities as partners in the War on Terror.*** Our *Strategy* recognizes the centrality of the very people our terrorist enemies most want to exploit: the faithful followers of Islam. The fact that our country has not experienced the level of homegrown violent Islamic extremism that has begun to plague other Western democracies is, in large measure, a tribute to American society, which values free expression and encourages all to engage politically and economically. As the primary targets of radicalization who stand at the forefront of the struggle against violent extremism, Muslim Americans are uniquely situated to offer insights and solutions. More broadly, community engagement and public-private partnerships across American society are essential to our success. We will continue to strengthen grassroots dialogue and interaction among Muslim communities and all levels of government, as well as with non-Muslim sectors of our society, because Americans of all religions, races, and ethnicities have a stake and role to play in the War on Terror. Engagement, taking place through public-private task forces and forums, includes work to ensure the preservation of liberty and religious pluralism and the enforcement of civil rights and hate crimes laws, discussions about U.S. foreign and domestic policy concerns, and addressing the ability of Muslim Americans to fulfill obligations of charitable giving, international travel, and religious practice.
- ***Identify and counter the sources of radicalization.*** The purveyors of violent extremism rely upon access to targeted communities to inculcate and spread their ideology. Law enforcement officials, therefore, must continue to identify and address sources of violent extremist radicalization in the Homeland. One place where we have already witnessed radicalization is in our prison system, but we must continue to identify other places vio-

---

lent propagators exploit within the United States, overseas, and on the Internet. In order to counter sources of radicalization, we will continue to support community and grassroots initiatives that publicly condemn the use of violence in general and specific acts of terror whenever and wherever they occur, debunk the claim of our terrorist enemies that the United States is at war with Islam, and counter all forms of propaganda that distort and misrepresent U.S. policy by clearly communicating U.S. policies – what they mean, how and why they are carried out, and how they affect all Americans. We also will support community and grassroots efforts to promote the values of citizenship, democracy, integration, religious tolerance, and the protection of civil rights, as well as increase cooperation among Tribal, State, and Federal prison officials and Muslim communities to counter radicalization in prisons.

- ***Enhance Federal, State, local, and Tribal government capacities to address radicalization.*** All levels of our government must strengthen institutions and human resources in a way that increases our ability to prevent violent Islamic extremism within our borders, identify when it is occurring, and spot new trends and developments in the radicalization process. To that end, we will continue to educate and train law enforcement and other U.S. Government personnel on Islamic cultural and community norms as well as prioritize the recruitment and retention of those having relevant language skills and cultural backgrounds; educate Federal, State, local, and Tribal government personnel on radicalization, expand current training programs on cultural proficiency, and encourage interagency training and career opportunities to facilitate the development and sharing of expertise; and improve interagency cooperation and information sharing at all levels of government.
- ***Continue to advance our understanding of radicalization.*** As we achieve success in preventing homegrown violent Islamic extremism, we should expect our adaptive enemies to create new methods for spreading their ideology of hate and murder. In order to identify and preempt new trends and developments, we will continue to advance our knowledge and understanding of radicalization by supporting relevant public and private research, including with regard to the vulnerabilities or susceptibility of individuals to violent Islamic extremism. Furthermore, we will keep working with Muslim communities to improve our understanding of the sources and evolving trends of radicalization and identify how changing technologies could affect radicalization.



---

## PROTECT THE AMERICAN PEOPLE, CRITICAL INFRASTRUCTURE, AND KEY RESOURCES

**W**hile protecting the lives and livelihoods of the American people demands that we work to prevent and disrupt terrorist attacks in the Homeland, it also requires that we undertake measures to deter the threat of terrorism, mitigate the Nation's vulnerabilities, and minimize the consequences of an attack or disaster should it occur. Our efforts include, among other things, protecting our population from infectious diseases and catastrophic public health threats, as well as reducing the effects and consequences of all hazards through improved systems to notify, alert, and warn the public.

Safeguarding the American people also includes the preservation of the Nation's critical infrastructure and key resources (CI/KR). As set forth in the 2006 *National Infrastructure Protection Plan* (NIPP), critical infrastructure includes the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. Key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government. By protecting CI/KR, we further protect the American people and build a safer, more secure, and more resilient Nation.

### Protection and Risk Management

Despite our best efforts, achieving a complete state of CI/KR protection is not possible in the face of the numerous and varied catastrophic possibilities that could challenge the security of America today. Recognizing that the future is uncertain and that we cannot envision or prepare for every potential threat, we must understand and accept a certain level of risk as a permanent condition. Managing homeland security risk requires a disciplined approach to resource prioritization and the diversification of protective responsibilities across the full spectrum of our Nation's homeland security partners. Applying a risk-based framework to all homeland security efforts will help to ensure our success over the long term and is discussed in detail in the chapter titled "Ensuring Long-Term Success."

### DETER THE TERRORIST THREAT

We seek to deter state sponsors of terrorism, terrorist groups, and other non-state actors who support or facilitate terrorism by undertaking various actions to decrease their likelihood of success as well as alter their motivational calculus.

- ***Decreasing likelihood of success.*** Terrorist actors can be deterred and dissuaded from conducting attacks if they perceive that they are not likely to achieve their objectives or that the costs of their efforts are too high. The counterterrorism and homeland security activities outlined in the chapter titled "Prevent and Disrupt Terrorist Attacks" are part of our deterrent strategy – making it increasingly difficult for our enemies to achieve their objective of an attack in the Homeland by denying them and their weapons entry to the United States, denying them the ability to operate effectively within our borders, and denying them future recruits by preventing homegrown radicalization.

As a protective function, this concept of “deterrence through denial” requires additional actions, including increased defensive postures at potential sites of attack. Prominent political, economic, and infrastructure targets are attractive to our enemies, as are large places of public gatherings and symbolic targets, such as national monuments. In order to deny terrorists access to potential targets and decrease their likelihood of success, the Federal Government, in full collaboration with State, local, Tribal, and private sector partners, will continue to harden sites, as appropriate, and strengthen security through the presence of security forces, reinforcement of defensive barriers, and enhancement of access control measures. The continued targeted provision of Federal assistance to State, local, and Tribal governments and the private sector – through risk- and performance-based criteria – will ensure that these entities receive the dollars and training necessary to effectively implement these measures. Additionally, the use of both active and passive countermeasures as well as their unpredictable application will help ensure greater effectiveness. We also must promote public awareness of our increased security practices so terrorists understand that we are increasing the likelihood that they will not succeed.

### **The National Infrastructure Protection Plan**

Guiding our efforts to protect the Nation’s CI/KR is the 2006 *National Infrastructure Protection Plan* (NIPP) and its supporting Sector-Specific Plans, which were developed pursuant to Homeland Security Presidential Directive-7, issued on December 17, 2003. The NIPP sets forth a comprehensive risk management framework and provides a coordinated approach to CI/KR protection roles and responsibilities for Federal, State, local, and private sector security partners. It sets national priorities, goals, and requirements for the effective distribution of funding and resources that will help ensure that our government, economy, and public services continue to function in the event of a man-made or natural disaster. In accordance with HSPD-7, the NIPP includes an augmented focus on the protection of CI/KR from the unique and potentially catastrophic effects of terrorist attacks. However, the NIPP framework supports a larger all-hazard approach to CI/KR protection.

Hardening sites against external threats is only one side of the deterrence equation. Terrorists also may seek to infiltrate or recruit an individual with privileged access to a hardened site. These insiders can offer our terrorist enemies information on exploitable vulnerabilities or even provide terrorist operatives access to sensitive or controlled areas. We must therefore continue to work with our State, local, Tribal, and private sector partners to review workforce surety programs and standards for screening and background checks, where appropriate. Finally, we must continue to conduct threat and vulnerability assessments and calibrate our defensive measures accordingly to account for changes in terrorists’ strategic targeting, tactics, techniques, and procedures, as well as changes in the larger operating environment.

- ***Changing motivational calculus.*** Terrorist actors also can be deterred or dissuaded from conducting attacks if they fear potential consequences for their actions. Since September 11, the United States has made it clear that we and our partners in the War on Terror make no distinction between those who commit acts of terror and those who support and harbor them. Any government that chooses to be an ally of terror has chosen to be

---

an enemy of freedom, justice, and peace, and we, along with our international partners, will hold our terrorist enemies to account.

Altering the calculus of our terrorist enemies – including all elements of the terrorist network – so that they fear the consequences of their actions requires credibility. We will continue to communicate and demonstrate our will to take action, both to our enemies in order to raise their awareness and to the American people so that they remain confident in our resolve. Maintaining our credibility also requires that we not only demonstrate our will to hold terrorists, their sponsors, and facilitators accountable, but that we also retain the capabilities and flexibility to do so. This includes enhancing our ability to respond to acts of terror using all instruments of national power, as well as refining our ability to define the nature, source, and perpetrator of an attack. To further strengthen the potential consequences our terrorist enemies face, we will continue to isolate and discredit those who support or facilitate terrorism, bring to justice terrorist actors, build a moral counterweight to undermine the perceived legitimacy of terrorism and the targeting of innocents, and ultimately create a global environment inhospitable to terrorists, violent extremists, and all who support them.

## MITIGATE VULNERABILITIES

We will not be able to deter all terrorist threats, and it is impossible to deter or prevent natural catastrophes. We can, however, mitigate the Nation's vulnerability to acts of terrorism, other man-made threats, and natural disasters by ensuring the structural and operational resilience of our critical infrastructure and key resources and by further protecting the American people through medical preparedness.

- ***Ensuring CI/KR structural resilience.*** While the devastation of even one sector of our critical infrastructure or key resources would have a debilitating effect on our national security and possibly damage the morale and confidence of the American people, interdependencies make the protection of CI/KR particularly essential. A failure in one area, such as our water supply system, can adversely affect not only public health but also the ability of first responders to provide emergency services. Accordingly, ensuring the survivability of our CI/KR assets, systems, and networks requires that we continue to accurately model their interdependencies and better assess and understand the potential

### **Critical Infrastructure and Key Resources**

Our Nation has identified 17 sectors of critical infrastructure and key resources, each with cross-cutting physical, cyber, and human elements:

Agriculture and Food  
Banking and Finance  
Chemical  
Commercial Facilities  
Commercial Nuclear Reactors, Materials, and Waste  
Dams  
Defense Industrial Base  
Drinking Water and Water Treatment Systems  
Emergency Services  
Energy  
Government Facilities  
Information Technology  
National Monuments and Icons  
Postal and Shipping  
Public Health and Health Care  
Telecommunications  
Transportation Systems

---

cascading effects that could impact and impede operations in interconnected infrastructures.

For each CI/KR sector, we must collectively work to ensure the ability of power, communications, and other life sustaining systems to survive an attack by terrorists, a natural disaster, and other assessed risks or hazards. In the past, investments in redundant and duplicative infrastructure were used to achieve this objective. We must now focus on the resilience of the system as a whole – an approach that centers on investments that make the system better able to absorb the impact of an event without losing the capacity to function. While this might include the building of redundant assets, resilience often is attained through the dispersal of key functions across multiple service providers and flexible supply chains and related systems. Resilience also includes the protection and physical survivability of key national assets and structures.

Additionally, an important aspect of promoting resilience includes seismic retrofitting and adherence to stricter building codes, as appropriate. Flood mitigation activities are also important and include the maintenance of flood plains. We also must increase participation in the National Flood Insurance Program and base that program on actuarial rates.

While the Federal Government provides overarching leadership and coordination for protecting and mitigating the vulnerabilities of our Nation's CI/KR, all partners in homeland security have important roles to play. This is especially true of the private sector, which owns and operates approximately 85 percent of the Nation's critical infrastructure and is the first line of defense for those assets. We will continue to strengthen our partnerships with State, local, and Tribal governments and the private sector so that we collectively can fulfill our responsibilities, as outlined in the NIPP, to protect and ensure the resilience of our Nation's most critical assets. Our partnerships also extend to our international neighbors. Many of our CI/KR assets are intertwined with a global infrastructure that has

### **Cyber Security: A Special Consideration**

Many of the Nation's essential and emergency services, as well as our critical infrastructure, rely on the uninterrupted use of the Internet and the communications systems, data, monitoring, and control systems that comprise our cyber infrastructure. A cyber attack could be debilitating to our highly interdependent CI/KR and ultimately to our economy and national security.

A variety of actors threaten the security of our cyber infrastructure. Terrorists increasingly exploit the Internet to communicate, proselytize, recruit, raise funds, and conduct training and operational planning. Hostile foreign governments have the technical and financial resources to support advanced network exploitation and launch attacks on the informational and physical elements of our cyber infrastructure. Criminal hackers threaten our Nation's economy and the personal information of our citizens, and they also could pose a threat if wittingly or unwittingly recruited by foreign intelligence or terrorist groups. Our cyber networks also remain vulnerable to natural disasters.

In order to secure our cyber infrastructure against these man-made and natural threats, our Federal, State, and local governments, along with the private sector, are working together to prevent damage to, and the unauthorized use and exploitation of, our cyber systems. We also are enhancing our ability and procedures to respond in the event of an attack or major cyber incident. The *National Strategy to Secure Cyberspace* and the NIPP's Cross-Sector Cyber Security plan are guiding our efforts.

---

evolved to support modern economies. While this global system brings efficiencies and benefits, it also creates vulnerabilities and challenges, and we must continue to work with our partners across the globe to protect the structural resilience of what has become a system of systems at home and abroad.

- ***Ensuring operational resilience.*** Mitigating the vulnerability of government and private sector operations to man-made or natural disasters depends not only on the structural resilience of our assets, systems, and networks but also on operational resilience. First, we will continue to maintain comprehensive and effective continuity programs, including those that integrate continuity of operations and continuity of government programs, to ensure the preservation of our government under the Constitution and the continuing performance of national essential functions – those government roles that are necessary to lead and sustain the Nation during and following a catastrophic emergency. A national approach to continuity also requires that State, local, and Tribal governments work to ensure that they are able to maintain or rapidly resume effective functioning during and after catastrophic incidents and are able to interact effectively with each other and the Federal Government. Likewise, we strongly encourage the private sector to conduct business continuity planning that recognizes interdependencies and complements governmental efforts – doing so not only helps secure the United States, but also makes good long-term business sense for individual companies. Such integrated and comprehensive planning is essential to protecting and preserving lives and livelihoods and maintaining our robust economy during crises.
- ***Protecting the American people through medical preparedness.*** As we protect our Nation’s critical infrastructure and key resources by working to deter terrorist threats and mitigate vulnerabilities through structural and operational resilience, we are helping to protect the American people. Our population, however, requires additional protective measures. We must reduce the vulnerability of the American populace to intentional dissemination of harmful biological agents, detonation of a nuclear or radiological device, the intentional or accidental release of toxic chemicals, naturally occurring infectious disease such as an influenza pandemic, and meteorological or geological events such as hurricanes or earthquakes.

Reducing the Nation’s vulnerability to public health threats requires that we continue to build sustainable systems for prevention, detection, reporting, investigation, control, and recovery. We must continue to expand the capabilities of the public health and medical communities to identify and assess threats and to determine if an attack or outbreak has occurred – all in a rapid and reliable manner. In order to facilitate our efforts, we will continue to upgrade our systems for clinical surveillance and environmental monitoring, as well as ensure the effective and timely integration and sharing of data, conclusions, and other information with State, local, and Tribal authorities and other appropriate homeland security partners. Likewise, we will encourage the timely sharing of information learned at the State, local, and Tribal level with the Federal Government.

In order to further mitigate the vulnerability of the American people to natural or man-made health threats, we must ensure that we have access to the necessary medical countermeasures, appropriately enhancing and expanding our flexible medical toolkit against potential biological threats. We must facilitate States and local and Tribal communities

---

in establishing appropriate levels of medical stockpiles and the systems that can rapidly distribute medical countermeasures to large, at-risk populations. Finally, we must assist communities as they develop medical systems that are able to sustain delivery of situation-appropriate care in the setting of catastrophic events. Like other homeland security activities, protecting the health of citizens is a shared responsibility – one that starts at the individual and family level, involves government and the private sector, and relies heavily on local action. While the Federal Government possesses unique tools and resources to guide and assist efforts to protect the health of citizens from all disasters, collaborative community and regional planning is essential for the protection of the American people.

## MINIMIZE CONSEQUENCES

Despite our best deterrent and mitigation efforts, terrorist attacks and natural disasters will happen, and we must work to minimize the consequences of their occurrence. Several of our efforts to reduce our Nation's vulnerabilities necessarily reduce the consequences of a disaster. This is the mutually reinforcing nature of our integrated efforts to protect the American people, critical infrastructure, and key resources. Moreover, the core of our efforts to minimize consequences lies with our comprehensive approach for responding to and recovering from incidents, which is described in the next chapter.

There are, however, pre-incident steps that we can take that can help to further reduce the effects and consequences of those events that do occur and better protect the American people, particularly through improved notification, alert, and warning systems. We must continue to develop reliable, effective, and flexible national systems to warn Americans of impending threats, including acts of terrorism, natural disasters, acts of war, and other hazards to public security and well-being. Beyond press conferences and warnings through television and radio, these systems must leverage modern and changing technology to push vital information to citizens wherever they are. Pre-incident alerts and warnings should be geographically or functionally targeted and provide guidance and instruction so that governments, the private sector, and individual citizens can take necessary preparatory or protective actions. These messages should continue throughout and immediately after the event, providing situational updates and current directions, as appropriate.

---

## RESPOND TO AND RECOVER FROM INCIDENTS

**D**espite our comprehensive and steadfast efforts to prevent and disrupt terrorist attacks and protect the American people, critical infrastructure, and key resources, our terrorist enemies remain determined to destroy our way of life, and nature continues to release its destructive forces. Given the certainty of catastrophes on our soil – no matter how unprecedented or extraordinary – it is our collective duty to provide the best response possible. When needed, we will bring to bear the Nation’s full capabilities and resources to save lives, mitigate suffering, and protect property. As the Nation responds based on the scope and nature of the incident, we must begin to lay the foundation not only for a strong recovery over the short term but also for the rebuilding and revitalization of affected communities and regions over the long term. This is crucial to reducing the psychological, social, and economic effects of an incident. Ultimately, response, recovery, and rebuilding efforts are tightly intertwined, each tapping into the resilience of the American spirit and our determination to endure and become stronger in the face of adversity.

In order to respond effectively to an incident and initiate short-term recovery, we must have a system that can quickly adapt to the full range of catastrophic scenarios confronting the Nation today and seamlessly integrate capabilities and resources from all stakeholders – Federal, State, local, and Tribal governments and the private and non-profit sectors – to achieve common objectives. At the core of our efforts have been the National Response Plan (now referred to as the National Response Framework) and the National Incident Management System (NIMS), which were developed pursuant to Homeland Security Presidential Directive-5, issued on February 28, 2003. Building on best practices, lessons learned from exercises and real-world events, including our response to Hurricane Katrina, and the ongoing formal review and revision of the National Response Framework, we will continue to improve our all-hazards approach for responding to and recovering from incidents. Ultimately, our National Response Framework must help us strengthen the foundation for an effective national response, rapidly assess emerging incidents, take initial actions, expand operations as needed, and commence recovery actions to stabilize the area. This framework must be clearly written, easy to understand, and designed to be truly national in scope, meeting the needs of State, local, and Tribal governments and the private and non-profit sectors, as well as the Federal Government. We also will ensure that those communities devastated or severely affected by a catastrophic incident are set on a sustainable path for long-term rebuilding and revitalization.

### **Incident Management Versus Response**

The homeland security community has used the terms “incident management” and “response” in complementary and occasionally interchangeable manners. Within this *Strategy*, “response” refers to actions taken in the immediate aftermath of an incident to save lives, meet basic human needs, and reduce the loss of property. “Incident management,” however, is a broader concept that refers to how we manage incidents and mitigate consequences across all homeland security activities, including prevention, protection, and response and recovery. This concept, including the role of the National Incident Management System (NIMS), is discussed further in the chapter titled “Ensuring Long-Term Success.”

---

## STRENGTHEN THE FOUNDATION FOR AN EFFECTIVE NATIONAL RESPONSE

An effective all-hazards response effort must begin with a strong foundation based on clear roles and responsibilities across all levels of government and the private and non-profit sectors, strengthened doctrine to guide our national response, a joint planning process to improve response capabilities, and advance readiness activities to better prepare for an impending or emergent event. The effectiveness of our efforts will be determined by the people who fulfill key roles and how they carry out their responsibilities, including their commitment to develop plans and partnerships, conduct joint training and exercises, and achieve shared goals.

- ***Clarify how national roles and responsibilities are fulfilled across all levels of government and the private and non-profit sectors.*** Disaster response has traditionally been handled by State, local, and Tribal governments, with the Federal Government and private and non-profit sectors playing supporting and *ad hoc* roles, respectively. A lack of clarity regarding roles and responsibilities across these levels can lead to gaps and seams in our national response and delay our ability to provide life-saving support when needed. Accordingly, we must better articulate how roles, responsibilities, and lines of authority for all response stakeholders are fulfilled across all levels of government and among the private and nonprofit sectors so that each understands how it supports the broader national response. We will continue to base our Federal planning and response efforts on the premise that the vast majority of incidents will be handled at the lowest jurisdictional level possible, with the Federal Government anticipating needs and assisting State, local, and Tribal authorities upon request, when their capabilities are insufficient, or in special circumstances where Federal interests are directly implicated. Public-private partnerships also are essential, and we will work together to better define the roles that the private and non-profit sectors can play, particularly in their local communities, to achieve a more successful response.
- ***Strengthen doctrine to guide the national response.*** Incidents that begin with a single response discipline within one jurisdiction may quickly expand to multi-disciplinary, multi-jurisdictional incidents that require additional resources and capabilities. In order to ensure high-level organization and efficiency among multiple actors in these challenging and complex environments, the response community must rely on fundamental principles that guide the full range of response activities. NIMS forms the backbone of this doctrine and includes, among other things, an Incident Command System as the overall management structure for responding to an incident as well as the concept of Unified Command, which provides for and enables joint decisions and action based on mutually agreed-upon objectives, priorities, and plans among all homeland partners involved in the response effort without affecting individual agency authority, responsibility, or accountability. We will continue to expand and refine the full set of fundamental doctrinal principles underlying our National Response Framework. For example, we will incorporate and further emphasize the concept of readiness to act that is imperative for no-notice incidents as well as incidents that have the potential to expand rapidly in size, scope, or complexity. Through the framework, we will encourage engaged partnerships in which all organizations establish shared objectives, assess their capabilities, identify gaps, and work collaboratively to fill those gaps well in advance of an incident. We also

## Roles and Responsibilities

In today's dynamic threat environment, we must strive for a national response based on engaged partnerships at and across all levels that enable us to anticipate where we should increase or reduce support based on changing circumstances. Success starts with understanding the following fundamental roles:

**Community Response.** *One of the fundamental response principles is that all incidents should be handled at the lowest jurisdictional level possible.* The initial response to the majority of incidents typically is handled by local responders within a single jurisdiction and goes no further. When incidents exceed available resources, the local or Tribal government may rely on mutual aid agreements with nearby localities or request additional support from the State. It is worth noting that for certain types of Federal assistance, Tribal nations work with the State, but, as sovereign entities, they can elect to deal directly with the Federal Government for other types of assistance.

**State Response.** *State governments have the primary responsibility for assisting local governments to respond to and recover from disasters and emergencies.* When an incident expands to challenge the resources and capabilities of the State coordinate requests for additional support, the State may request support from the private and nonprofit sector, turn to other States for support through the Emergency Management Assistance Compact, or call upon the Federal Government for assistance. States also may collaborate with one another to ensure a broader, more effective regional response.

**Federal Response.** *The Federal Government maintains a wide array of capabilities and resources that may be made available to States and local governments.* Federal assistance is provided when needed to support State and local efforts or lessen or avert the threat of a catastrophe within the United States. Accordingly, Federal response efforts are designed to complement and supplement, rather than supplant, the State and local response. The Federal Government also maintains relationships with private and non-profit sector entities to aid in facilitating additional support.

**Private and Non-Profit Sector.** *The private and non-profit sectors fulfill key roles and work closely with communities, States, and the Federal Government.* The private sector plays an essential role implementing plans for the rapid restoration of commercial activities and critical infrastructure operations, which can help mitigate consequences, improve quality of life, and accelerate recovery for communities and the Nation. Non-profit organizations serve a vital role by performing essential services within communities in times of need, such as mass sheltering, emergency food supplies, counseling services, or other vital support services.

**Special Circumstances.** *There are special circumstances where the Federal Government exercises a larger, more proactive role.* This includes catastrophic incidents when local and State governments require significant support, and incidents where Federal interests are directly implicated, such as those involving primary Federal jurisdiction or authorities. For example, the Federal Government will lead response efforts to render safe weapons of mass destruction and coordinate related activities with State and local partners, as appropriate.

will underscore that our national response must be scalable, flexible, and adaptable to respond to the full range of potential incidents that our Nation could confront.

- **Develop and apply joint planning and training processes.** An effective, coordinated response begins with sound planning well before an incident occurs. The planning process will translate policy, strategy, doctrine, and capabilities into specific tasks and courses of action to be undertaken during a response. The resulting plans must repre-

---

sent collaborative efforts involving communities, States, and the Federal Government as well as private sector and non-profit partners to ensure we effectively bring to bear all instruments of national power in our response to an incident. The planning effort also must be based on a clear set of planning assumptions and guided by a full range of national planning scenarios, depicting a spectrum of catastrophic man-made and natural disasters that would test our Nation's response capabilities. Finally, because each incident is unique, our planning processes must be dynamic and flexible, ensuring we have the ability not only to produce deliberate plans but also the ability to adapt our plans at the operational and tactical levels in a compressed period of time to address the specific characteristics of each incident.

Complementing our process for joint planning is a joint training and exercise program that will help response professionals practice the application of those plans well in advance of an actual incident. Ultimately, a continuous cycle of joint training and exercises will ensure that all government, private sector, and non-profit stakeholders are capable of fulfilling their roles and responsibilities and can achieve unity of effort when responding to a real-world natural or man-made disaster. It is vital that best practices and lessons learned from exercises be applied to continually improve our Nation's response.

- **Conduct advance readiness activities.** There are times when we are able to anticipate impending or emergent events that will require a national response, such as an upcoming hurricane season, a potential pandemic, or a period of heightened terrorist threat. We must capitalize on this critical window of opportunity to increase readiness activities. For example, we can pre-identify needs and fill gaps in our current capabilities or resources that will be required to address the specific nature of the forthcoming incident. We also will pre-position commodities such as water, ice, emergency meals, tarps, and other disaster supplies so they will be readily available for use. Additional advance readiness activities include establishing contracts with the private sector prior to an incident and developing pre-negotiated agreements with Federal departments and agencies to ensure that appropriate Federal resources are available during a crisis.

## ASSESS SITUATION AND TAKE INITIAL ACTION

When an incident occurs, responders work to assess the situation – including possible causes, extent of affected population and geographic area, and the degree of damage – in order to take the initial actions that will save lives, mitigate suffering, and protect property. Our Nation must acknowledge the critical role of first responders to rapidly assess ongoing and emerging incidents. This includes effectively prioritizing and coordinating initial actions, mobilizing and deploying resources and capabilities, and anticipating additional support that may be needed.

### Situational Awareness

Maintaining situational awareness is essential to assessing emerging incidents as well as conducting operations and ultimately ensuring the effective management of incident response. It demands that we prioritize information and develop a common operating picture, both of which require a well-developed national information management system and effective multi-agency coordination centers to support decision-making during incidents. The concept of situational awareness, along with other fundamental principles of incident management, is detailed in the chapter titled "Ensuring Long-Term Success."

- **Prioritize and coordinate initial actions to mitigate consequences.** Since there will be a degree of confusion and turmoil in the initial hours of an incident, it is critical that our Nation use standardized incident response structures and procedures to prioritize and coordinate initial actions. Our framework must better integrate the National Incident Management System (NIMS), which enables a consistent approach and allows multiple organizations to work together effectively. For example, as first responders arrive at the affected area, they must quickly establish on-scene incident command to coordinate the activities of numerous responders under a single structure. Using NIMS, the incident command develops an Incident Action Plan, which outlines incident priorities, objectives, and initial actions and drives the development of supporting plans. These initial activities may include search and rescue, evacuations, communication of key information to the public, restoration of essential critical infrastructure, and provision of community law enforcement, fire, and emergency medical services, among others. As the incident unfolds, the incident command will revise plans and courses of action based on changing circumstances.

- **Effectively mobilize and deploy people, resources, and capabilities.** In response, every minute counts, and a failure to quickly surge people, resources, and capabilities can result in lives lost, increased property damage, and cascading consequences that can magnify the effects of the incident. To ensure rapid mobilization and deployment of response assets, our National Response Framework must describe how this process occurs across various levels

### Examples of Federal Field Teams

Since September 11, the Federal Government has strengthened deployable teams to help respond to natural and man-made disasters. These teams support the emergent needs of State, local, and Tribal jurisdictions or exercise Federal statutory responsibilities by providing specialized expertise and capabilities, establishing emergency response facilities, and supporting overall incident management.

- Emergency Response Teams (ERT) – to be replaced by the Federal Incident Response Support Teams (FIRST) and Incident Management Assistance Teams (IMAT)
- Damage Assessment Teams
- Nuclear Incident Response Team (NIRT)
- Disaster Medical Assistance Teams (DMATs)
- Department of Health and Human Services' Incident Response Coordination Team – formerly the Secretary's Emergency Response Team
- Department of Labor/Occupational Safety and Health Administration's Specialized Response Teams
- National Veterinary Response Teams (NVRT) – formerly the Veterinarian Medical Assistance Teams (VMATs)
- Disaster Mortuary Operational Response Teams (DMORTs)
- Medical Emergency Radiological Response Team (MERRT)
- National Medical Response Teams (NMRTs)
- Scientific and Technical Advisory and Response Teams (STARTs)
- Donations Coordination Teams
- Urban Search and Rescue (US&R) Task Forces
- Incident Management Teams (IMTs)
- Domestic Emergency Support Team (DEST)
- Domestic Animal and Wildlife Emergency Response Teams and Mitigation Assessment Team

---

of government and with the private and nonprofit sectors. In addition, all responders should be encouraged to maintain and regularly exercise notification systems and activation protocols. Activation and deployment should be a deliberate and informed – yet rapid – process that reflects the size, scope, nature, and complexity of an incident.

- ***Anticipate additional support that may be needed.*** Minute by minute, the scope and scale of an incident can rapidly evolve, such as when a hurricane changes course or it becomes apparent that a terrorist bombing is actually one in a series of attacks in multiple cities. Responders at all levels must be able to anticipate the course of an incident and associated requirements and work with their counterparts to surge or deescalate resources and capabilities as needed. While there is no substitute for experience, our National Response Framework must help drive joint planning and training programs that will help responders across all levels better anticipate alternative courses of action and work together effectively.

### **EXPAND OPERATIONAL CAPABILITIES, AS NEEDED**

While the vast majority of incidents are effectively handled at the community level, some require additional support from nearby jurisdictions or the State, including through mutual aid agreements with other States. If needed, the Federal Government also will provide support. In catastrophic or highly complex events, all who respond should provide assistance in an organized fashion within the existing response framework, anticipating needs and coordinating with their partners in advance as opposed to waiting to be asked. As the incident grows in severity and complexity, our national response operations must effectively coordinate requests for additional support and integrate resources and capabilities into ongoing operations. It is critical that our Nation continue to improve and clearly describe the processes used to coordinate requests for additional support and integrate resources and capabilities into ongoing operations.

- ***Effectively coordinate requests for additional support.*** If resources and capabilities beyond the immediate area are required, the on-scene incident command requests additional support, activating response structures and personnel to support and coordinate the overall response. In many cases, resources and capabilities are provided from surrounding areas. Our Nation must work together to clarify the processes to request and provide assistance and ensure we have the necessary awareness, training, and familiarization programs for responders to execute related plans and agreements. This includes familiarization with the processes that States use to request support through mutual aid agreements as well as from the Federal Government and how the Federal Government provides this support to States. Effective support requires that all organizations review and update their existing agreements and plans, meet with their partners, and verify their expectations and capabilities on a regular basis.
- ***Integrate resources and capabilities.*** During large-scale incidents, we establish response structures and facilities to effectively receive, stage, track, and integrate incoming resources and capabilities into ongoing operations. For example, personnel are deployed to staging areas to receive commodities that can then be integrated into operations in support of the State and then distributed to communities. For large, complex incidents, resources and capabilities might arrive from a diverse array of organizations – ranging

---

from multiple private-sector companies to non-governmental organizations to the Federal Government – through pre-arranged agreements and contracts. In order to assist with the full assimilation of resources and assets, we will continue to develop comprehensive and integrated logistics systems and procedures that enhance our Nation’s overall response capabilities. In addition, our National Response Framework must describe the policies and procedures for how to manage disaster assistance offered by our international partners, as well as clarify responsibilities and procedures for inquiries regarding affected foreign nationals.

### **COMMENCE SHORT-TERM RECOVERY ACTIONS TO STABILIZE THE AFFECTED AREA AND DEMOBILIZE ASSETS**

Even as the immediate imperatives for response to an incident are being addressed, the need to begin recovery operations emerges. In an almost imperceptible evolution, response efforts will transition to short-term recovery operations, such as the restoration of interrupted utility services, reestablishment of transportation routes, and the provision of food and shelter for those displaced by the disaster – actions that will help individuals, communities, and the Nation return to a general state of normalcy. While short-term recovery efforts are the primary responsibility of States and communities, they also involve significant contributions from all sectors of our society – Federal, State, local, and Tribal governments, the private sector, nonprofit partners, as well as individual citizens. As the priorities and needs of an incident evolve, people, assets, and resources will be reassigned or demobilized to provide a flexible and scalable response, evolving as needs evolve, changing as the incident priorities change. As immediate life-saving and life-sustaining activities subside, and short-term recovery decisions are made over a period of weeks or even months, we must recognize that these efforts are steps to an effective transition to long-term rebuilding and revitalization efforts.

### **ENSURE AN EFFECTIVE TRANSITION TO LONG-TERM REBUILDING AND REVITALIZATION EFFORTS**

Ensuring a successful transition from short-term recovery to rebuilding and revitalization efforts is vital and must include active participation and leadership by the breadth of political, economic, private, and non-profit actors that form the fiber of any community. Rebuilding and revitalization efforts are distinguished from shorter-term recovery efforts not only by the length of time involved, but also by the scope and nature of the incident, the complexity of efforts required to regenerate infrastructure, and the effect on the social fabric of the community and region.

Rebuilding and revitalizing those communities so devastated or severely affected by a catastrophic incident that a State or region is overwhelmed can take several months and sometimes years, depending on the severity and extent of destruction. Some cases might require the complete reconstruction of critical infrastructure and key resources, redevelopment of homes and long-term housing solutions, and the restoration of economic growth and vitality.

In the past, we have undertaken reconstruction operations for major catastrophes in an *ad hoc* and reactive fashion, developing large-scale disaster-specific rebuilding approaches and tools only after major crises arise. The resulting process of rebuilding has been slow, complex, and extremely expensive. Notwithstanding the tremendous efforts of the individuals involved, the

---

challenges of an *ad hoc* approach are reflected in the experiences in lower Manhattan after the September 11 attacks, in the southeastern United States during the 2004 hurricane season that witnessed landfall of four major hurricanes within six weeks, and in the Gulf Coast region after Hurricane Katrina.

Going forward, we must develop a comprehensive – but not bureaucratic or government-centric – framework wherein communities that are directly or indirectly affected by a large-scale disaster can flourish on a sustainable path to rebuilding and revitalization. This framework and accompanying plans must be closely guided by, and have at their core, the citizens, private sector, and faith-based and community organizations that are most severely and directly affected. After all, individual citizens and the private and non-profit sectors are our society’s wells of creativity, innovation, and resourcefulness, and they have the greatest stake in, and urgency for, revitalizing their community.

The majority of reconstruction efforts will occur beyond the Federal Government’s purview. However, the Federal Government, in collaboration with all stakeholders, will draw upon and apply the field’s most innovative thinking, lessons learned, and best practices to create a comprehensive framework for our Nation that fully appreciates free markets and the vast power of incentives and empowers individuals, businesses, and non-profit groups in the decisions about the future of their communities.

In order to develop this new framework, our Nation must continue to assess the challenges in this area and provide recommendations to improve our ability to rebuild and revitalize areas following a catastrophic natural or man-made disaster. We must determine how Federal, State, local, and Tribal governments, the private and non-profit sectors, and communities can improve collaboration and develop recommendations that further economic renewal and help stabilize and reconstruct communities.

In addressing these challenges, Federal, State, local, and Tribal governments, the private and nonprofit sectors, and communities must be focused on citizens – and not on bureaucracy or processes – and be guided by the concepts of compassion, speed, efficiency, common sense, and the devolution of as many decisions as reasonably possible to individual citizens, businesses, and communities. Specific areas of focus include:

- ***Restore community services and the economy.*** In the wake of a catastrophic event, all facets of society will need to work together to restore communities and the economy. This includes helping to facilitate the return of private, non-profit, and government operations to the affected area. Individuals, communities, and private sector and non-profit entities should strive to resume their services as quickly as possible, while government at all levels should carry out activities and investments that foster this rapid and orderly revitalization. Federal, State, local, and Tribal governments may consider a range of actions based on the circumstances and careful consideration of the situation and, in some cases, may temporarily reduce or waive regulations that could result in unintended consequences from large-scale incidents.
- ***Organize planning efforts among key players.*** The Nation should coalesce around public-private partnerships that can more effectively integrate and coordinate collective recovery efforts. This requires plans and policies that support basic needs such as housing, medical care, and the food service industry. In some circumstances, this will require

---

the creation of special purpose entities and unique, temporary tax or other financial incentives that foster cooperation and collective engagement in rebuilding of the affected communities. In addition, as warranted and in accordance with existing laws and regulations, the Federal Government can scale back select requirements that communities match Federal expenditures with certain percentage of funding from their own budgets.

- ***Facilitate long-term assistance for displaced victims.*** Ensuring the availability of medium-term housing and promotion of long-term housing solutions for the affected area are often important initial measures. Other focus areas must include care and treatment of affected persons in terms of sustained medical care and additional measures for social, political, environmental, and economic restoration. In order to be effective, long-term efforts to assist displaced victims must begin as soon as possible following response efforts, in conjunction with short-term recovery.
- ***Rebuild critical infrastructure.*** A key Federal role in long-term reconstruction involves both rebuilding the most essential critical infrastructure and providing economic incentives, when appropriate, to support the return of citizens and the private sector to the affected community. Because this is a very different problem from response and immediate recovery efforts, long-term rebuilding and revitalization must be addressed through tailored approaches that creatively engage the full spectrum of government, private sector, and non-profit entities. Furthermore, including mitigation measures in critical infrastructure designs during the restoration process also is important for reducing the consequences of future similar events.



---

## ENSURING LONG-TERM SUCCESS

**P**reventing and disrupting terrorist attacks; protecting the American people, critical infrastructure, and key resources; and responding to and recovering from those incidents that do occur are enduring homeland security responsibilities. In order to help fulfill those responsibilities over the long term, we will continue to strengthen the principles, systems, structures, and institutions that cut across the homeland security enterprise and support our activities to secure the Homeland. Ultimately, this will help ensure the success of our *Strategy* to secure the Nation.

### RISK MANAGEMENT

The assessment and management of risk underlies the full spectrum of our homeland security activities, including decisions about when, where, and how to invest in resources that eliminate, control, or mitigate risks. In the face of multiple and diverse catastrophic possibilities, we accept that risk – a function of threats, vulnerabilities, and consequences – is a permanent condition. We must apply a risk-based framework across all homeland security efforts in order to identify and assess potential hazards (including their downstream effects), determine what levels of relative risk are acceptable, and prioritize and allocate resources among all homeland security partners, both public and private, to prevent, protect against, and respond to and recover from all manner of incidents. A disciplined approach to managing risk will help to achieve overall effectiveness and efficiency in securing the Homeland. In order to develop this discipline, we as a Nation must organize and help mature the profession of risk management by adopting common risk analysis principles and standards, as well as a professional lexicon.

### CULTURE OF PREPAREDNESS

Our entire Nation shares common responsibilities in homeland security. In order to help prepare the Nation to carry out these responsibilities, we will continue to foster a Culture of Preparedness that permeates all levels of our society – from individual citizens, businesses, and non-profit organizations to Federal, State, local, and Tribal government officials and authorities. This Culture rests on four principles.

The first principle of our Culture of Preparedness is a shared acknowledgement that creating a prepared Nation will be an enduring challenge. As individual citizens we must guard against complacency, and as a society we must balance the sense of optimism that is fundamental to the American character with a sober recognition that future catastrophes will occur. The certainty of future calamities should inform and motivate our preparedness, and we will continue to emphasize the responsibility of the entire Nation to be flexible and ready to cope with a broad range of challenges.

The second principle is the importance of individual and collective initiative to counter fundamental biases toward reactive responses and approaches. Our Culture, therefore, must encourage and reward innovation and new ways of thinking as well as better align authority and responsibility so that those who are responsible for a mission or task have the authority to act.

---

The third principle is that individual citizens, communities, the private sector, and non-profit organizations each perform a central role in homeland security. Citizen and community preparedness are among the most effective means of securing the Homeland, and leadership must continue at all levels to promote and strengthen their preparedness, including through public dialogue and specialized programs such as the “Ready” campaign, the Nation’s public service initiative for individual and corporate preparedness (see [ready.gov](http://ready.gov) for more information). All Americans must share in the full range of homeland security activities, including prevention and protection, but it is particularly important that we all take responsibility for increasing the likelihood that we can survive an incident and care for our own basic needs in the immediate aftermath. As more Americans contribute to homeland security through self-reliance and mutual assistance, we reduce the burden on our emergency responders so they can focus on those most in need.

We also will continue to encourage the preparedness of other homeland security stakeholders, including private sector and non-profit groups such as non-governmental organizations and faith-based groups and, whenever appropriate, incorporate them as full partners into our national preparedness efforts across all homeland security disciplines. The private sector is particularly important in this endeavor. As highlighted throughout this *Strategy*, the private sector is the Nation’s primary provider of goods and services and the owner and operator of approximately 85 percent of our critical infrastructure. It is an essential partner in ensuring structural and operational resilience that protects the American people, establishing supply chain security to help deny terrorist weapons and material entry into the Homeland, and reporting suspicious activities at work sites that could uncover and ultimately help disrupt terrorist activity. The private sector also is a critical partner in rebuilding communities devastated or severely affected by a catastrophic incident as well as in fielding scientific and technological advancements that can help secure the Homeland. Due to the multiple and essential roles the private sector plays across all areas of homeland security, continued collaboration and engagement with the private sector to strengthen preparedness is imperative.

The fourth principle of our Culture of Preparedness is the responsibility of each level of government in fostering a prepared Nation. Although Federal, State, local, and Tribal governments will have roles and responsibilities unique to each, our Culture must continue to embrace the notion of partnership among all levels of government. Built upon a foundation of partnerships, common goals, and shared responsibility, the creation of our Culture of Preparedness is an enduring touchstone for homeland security.

## **HOMELAND SECURITY MANAGEMENT SYSTEM**

In order to continue strengthening the foundations of a prepared Nation, we will establish and institutionalize a comprehensive Homeland Security Management System that incorporates all stakeholders. Relevant departments and agencies of the Federal Government must take the lead in implementing this system, and State, local, and Tribal governments are highly encouraged to ultimately adopt fully compatible and complementary processes and practices as part of a full-scale national effort.

Our current approach to managing homeland security has focused on doctrine and planning through the National Preparedness Guidelines (NPG). Called for in Homeland Security Presidential Directive-8, issued on December 17, 2003, the NPG delineates readiness targets, pri-

---

orities, standards for preparedness assessments and strategies, and a system for assessing the Nation's overall level of preparedness to prevent, protect against, and respond to and recover from incidents. The NPG aligns national efforts by using national planning scenarios that represent a wide range of catastrophic terrorist attacks and natural disasters that would stretch the Nation's prevention, protection, and response capabilities. Those scenarios form the basis of the 37 essential capabilities, identified in the NPG and the accompanying Target Capabilities List, that must be developed or maintained, in whole or in part, by various levels of government across our homeland security efforts. In this manner, the NPG constitutes a capabilities-based preparedness process for making informed decisions about managing homeland risk and prioritizing homeland security investments across disciplines, jurisdictions, regions, and levels of government, helping us to answer how prepared we are, how prepared we need to be, and how we prioritize efforts to close the gap.

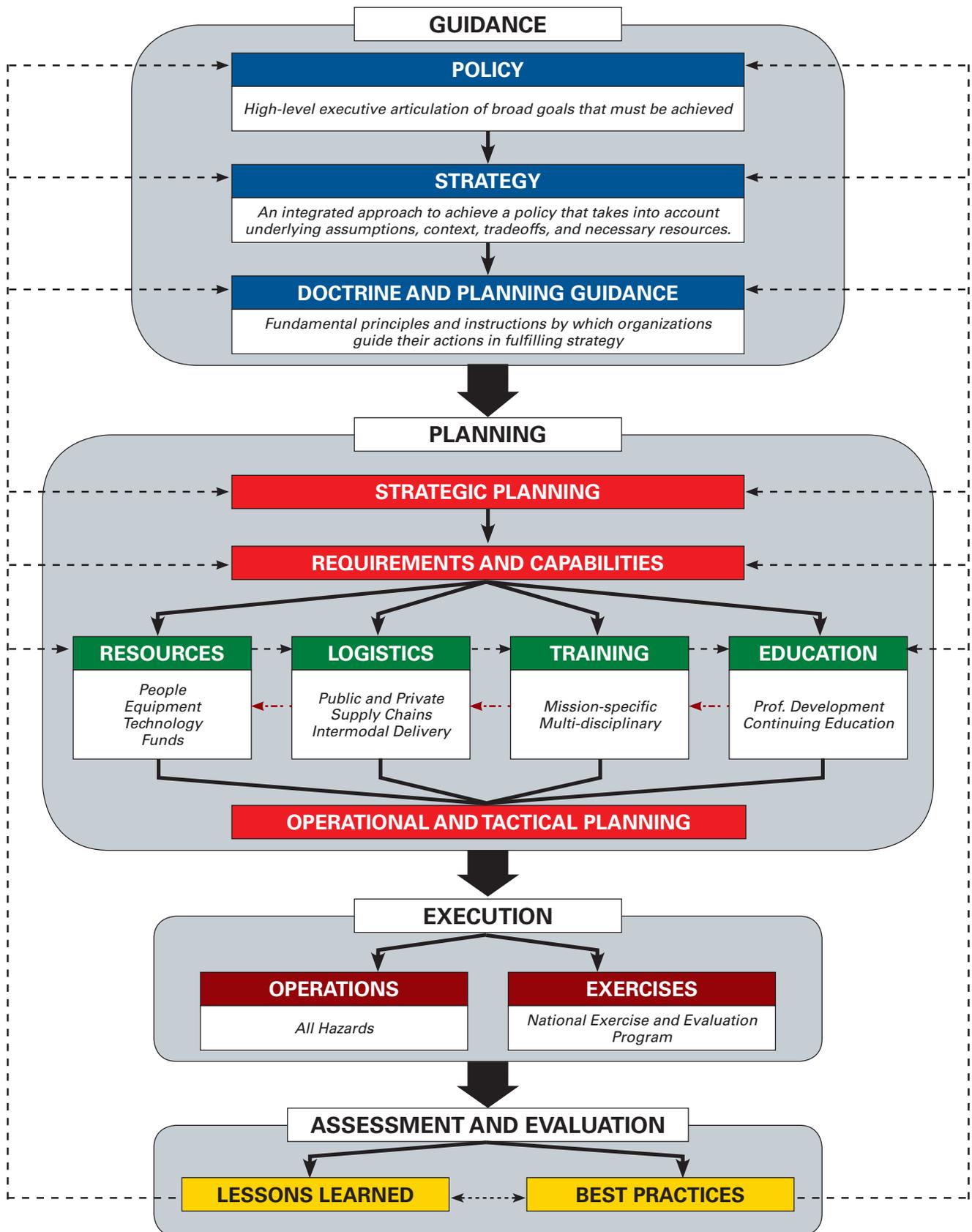
We must build on this current process in order to establish a more deliberate and comprehensive system that will ensure unity of effort and help maximize success as we work to prevent and disrupt terrorism, protect the American people, critical infrastructure and key resources, and respond to and recover from incidents that do occur. This new Homeland Security Management System (depicted in Figure 1) will involve a continuous, mutually reinforcing cycle of activity across four phases.

- **Phase One: Guidance.** The first phase in our Homeland Security Management System encompasses overarching homeland security guidance. It is the foundation of our system, and it must be grounded in clearly articulated and up-to-date homeland and relevant national security policies, with coordinated supporting strategies, doctrine, and planning guidance flowing from and fully synchronizing with these policies. Accordingly, we will update, clarify, and consolidate, where necessary, homeland and national security presidential directives and other key policies, all of which encompass high-level executive articulations of the broad homeland security goals we must achieve.
- **Phase Two: Planning.** The second phase is a deliberate and dynamic system that translates our policies, strategies, doctrine, and planning guidance into a family of strategic, operational, and tactical plans. These plans should be coordinated with relevant stakeholders, consistent with the fundamental roles and responsibilities of local, Tribal, State, and Federal governments bring to bear all appropriate instruments of national power and influence, assign activities to specific homeland security actors, and appropriately sequence these activities against a timeline for implementation.

Strategic plans educate and drive resource requirements and capabilities, laying the foundation for more detailed operational and tactical plans. Based on the resource and capability requirements identified in strategic plans, operational and tactical plans prescribe the actions of all applicable stakeholders arranged in time and space in order to achieve specific goals. For the Homeland Security Management System to be effective and address long-range challenges across multiple disciplines, all homeland security partners should develop a planning capability that may also be employed during times of crisis.

Figure 1

# HOMELAND SECURITY MANAGEMENT SYSTEM



---

Requirements and capabilities within the planning phase of our system also must place particular emphasis on training and education so that homeland security professionals not only acquire the specific functional skills that are needed to successfully execute operational plans but also understand the broader strategic context in which these plans will be executed. Leadership development must be emphasized in this education and training process, because planning and execution across a wide array of communities, organizational structures, and professions requires specific leadership skills. The second phase ultimately culminates in tactical plans by homeland security partners that describe the specific field-level activities they will undertake to fulfill the responsibilities assigned to them in the operational plan.

- **Phase Three: Execution.** The third phase in the Homeland Security Management System encompasses the execution of operational and tactical-level plans. This may occur as actual operations in response to real-world events or may happen as part of an exercise, including through the National Exercise Program, that allows us to practice the plan and ensure all actors fully understand their roles and responsibilities.

#### **Investing in Intellectual and Human Capital**

In order to ensure the success of the Homeland Security Management System, our Nation must further develop a community of homeland security professionals. This requires establishing multidisciplinary education in homeland and relevant national security policies and strategies; the planning process; execution of operations and exercises; and overall assessment and evaluation. Furthermore, this should include an understanding and appreciation of appropriate regions, religions, cultures, legal systems, and languages. Education must continue outside the classroom as well – in order to enhance knowledge and learning, build trust and familiarity among diverse homeland security practitioners, break down organizational stovepipes, and advance the exchange of ideas and best practices, we must continue to develop interagency and intergovernmental assignments and fellowship opportunities, tying them to promotions and professional advancement. Executive Order 13434 of May 17, 2007 (“National Security Professional Development”) and the resulting *National Strategy for the Development of Security Professionals* are essential steps forward in meeting these educational needs, and we will continue to build on these endeavors to ensure that we have the necessary depth and breadth of intellectual and human capital across all levels of homeland security partnerships and disciplines.

- **Phase Four: Assessment and Evaluation.** The fourth phase involves the continual assessment and evaluation of both operations and exercises. This phase of the system will produce lessons learned and best practices that must be incorporated back into all phases of the Homeland Security Management System. This sequence of activities ensures our highly adaptive system reflects current realities and remains responsive to a dynamic, changing homeland security environment.

Because homeland security is a shared responsibility, the Federal Government must provide leadership and guidance for non-Federal partners across the four phases of the Homeland Security Management System. For the Homeland Security Management System to succeed, Federal dollars must be allocated based on constantly improving risk assessments and on accountability for results; once allocated, funds must be used to support or develop operational plans and their derivative requirements and capabilities. In addition, our Nation still faces the challenge of developing tools for assessing our over-

---

all security posture and measuring the effectiveness of Federal assistance. We therefore must develop assessment tools that measure not only State, local, and Tribal response capabilities but also capabilities in support of our prevention and protection goals. These tools must recognize and reward partnership with and among neighboring jurisdictions and regions and all levels of government.

## INCIDENT MANAGEMENT

While our Homeland Security Management System provides a framework for integrating four essential phases in a deliberate process to secure the Homeland, there will be times when incidents force the homeland security community to compress this cycle of activity and assume a more crisis-oriented posture. Decision-making during crises and periods of heightened concern, however, is different from decision-making during a steady-state of activity, and we must develop a comprehensive approach that will help Federal, State, local, and Tribal authorities manage incidents across all homeland security efforts.

Our approach will build upon the current National Incident Management System (NIMS). An outgrowth of Homeland Security Presidential Directive-5 (HSPD-5), issued on February 28, 2003, NIMS focuses largely on stakeholders in the discipline of response. Incidents, however, are not limited to natural and man-made disasters that strike the Homeland. They also include, for example, threats developing overseas, law enforcement and public health actions and investigations, and even specific protective measures taken at critical infrastructure sites, for example. In order to realize the full intent of HSPD-5, our new approach to incident management must apply not only to response and recovery but also to the prevention and protection phases of an incident as well. Federal efforts must be directed toward coordination of resources across sectors (public, private, and non-profit), disciplines, and among Federal, State, local, and Tribal officials.

Incident management rests on a core set of common principles and requirements. The first of these is an Incident Command System, which provides the overall structure for managing an incident. Our current system for incident command has five major functional areas: command, operations, planning, logistics, and finance and administration. Although a sixth area – intelligence – is currently applied on an *ad hoc* basis, we must institutionalize this area throughout our new approach in support of prevention and protection activities. Unified Command is a second core principle. The Federal Government must fully adopt and implement this principle, which is commonly used at the State and local levels and provides the basis from which multiple agencies can work together effectively to manage an incident by ensuring that all decisions will be based upon mutually agreed upon objectives and plans, regardless of the number of entities or jurisdictions involved.

<b>Principles and Requirements of Incident Management</b>
Incident Command System
Unified Command
Crisis Action Planning Resources
Situational Awareness
Prioritization of Information
Multi-Agency Coordination Centers
Skilled Leaders and Partners
Training and Exercises

---

Crisis action planning is a third key principle in our approach to incident management. This planning process takes existing contingency plans and procedures and rapidly adapts them to address the requirements of the current crisis or event of concern in a compressed timeframe. We must ensure that all stakeholders across all homeland security disciplines have the ability to transition quickly from contingency planning to crisis action planning. They also must be able to provide resources – a fourth requirement – in support of their plans and activities, and we call on all stakeholders to have predetermined capabilities available on a short deployment timeline.

The maintenance of situational awareness through timely and accurate information is a fifth core principle integral to incident management. It requires continuous sharing, monitoring, verification, and synthesis of information to support informed decisions on how to best manage threats, potential threats, disasters, or events of concern. In order to help facilitate situational awareness and decision-making, we must prioritize incident information – a sixth requirement. While timely information is valuable, it also can be overwhelming. We must be able to identify what is required to assist decision makers and then rapidly summarize and prioritize the information we receive from multiple reporting systems. In order to be successful, our new approach to incident management also must have an information management system that integrates key information and defines national information requirements.

A seventh requirement of incident management consists of the various multi-agency coordination centers that exist throughout all levels of government. They are essential to maintaining situational awareness and overall incident management, and they assist in the flow of information, the reporting of actions and activities, and ultimately the development of a common operating picture, but they also are hubs for coordinating operational activities during an incident. Examples include State, local, and Tribal emergency operations centers; State, local, and Tribal fusion centers; the National Operations Center, National Infrastructure Coordination Center, and the Federal Emergency Management Agency's National Response Coordination Center (all part of the Department of Homeland Security); the Federal Bureau of Investigation's Strategic Information and Operations Center and National Joint Terrorist Task Force (both part of the Department of Justice); and the National Counterterrorism Center (part of the Office

### **Interoperable and Resilient Communications**

Our Nation continues to confront two distinct communications challenges: interoperability and survivability. Unimpeded and timely flow of information in varying degrees across multiple operational systems and between different disciplines and jurisdictions is critical to command, control, and coordination of operational activities. To achieve interoperability, we must have compatible equipment, standard operating procedures, planning, mature governance structures, and a collaborative culture that enables all necessary parties to work together seamlessly. Survivable communications infrastructure is even more fundamental. To achieve survivability, our national security and emergency preparedness communications systems must be resilient – either able to withstand destructive forces regardless of cause or sufficiently redundant to suffer damage and remain reliable. Without the appropriate application of interoperable communications technologies, standards, and governance structures, effective and safe incident management will be hindered. Although much progress has been made, effective communication during major disasters requiring multi-jurisdictional coordination depends on continued improvement to our Nation's communications systems.

---

of the Director of National Intelligence). We will continue to develop and strengthen these centers and systems to ensure that activities are better coordinated and related information is shared among multiple agencies.

People exist at the heart of our refocused incident management approach, and deploying people with the skills necessary to manage each incident is the eighth key principle. Building on the professional development initiatives that are part of our Homeland Security Management System, we will ensure that the most qualified professionals are identified in advance so that they may be quickly and efficiently activated and deployed during an incident. We will embrace and institute a continuous training cycle to ensure that leaders and partners at all levels of government are fully trained and well versed in the principles of incident management. Finally, we will conduct exercises, consistent with the National Exercise Program, so that all stakeholders can ensure they are fully capable of executing their incident management responsibilities.

## SCIENCE AND TECHNOLOGY

The United States derives much of its strength from its advantage in the realm of science and technology (S&T), and we must continue to use this advantage and encourage innovative research and development to assist in protecting and defending against the range of natural and man-made threats confronting the Homeland.

Over the past six years, focused partnerships with our Nation's vast and varied research enterprise, which includes businesses, research institutes, universities, government laboratories as well as Federal departments and agencies, have yielded significant capabilities that are helping us to better protect the lives and livelihoods of the American people. For instance, the focused application of the Nation's nuclear expertise has produced improved tools for countering the threat of nuclear terrorism against the Homeland. We also have applied biometric technologies and systems to enhance the security of travel documents and inhibit the movement of terrorists internationally and across our borders. The development and application of a variety of chemical, biological, radiological, and nuclear countermeasures are helping to prevent WMD terrorism and address the public health consequences that can stem from a range of natural and man-made disasters. We also have upgraded the technical capabilities of our first responders through the provision of decontamination equipment and protective gear; these advances serve not only to better protect our Nation's first responders but also to increase their ability to save the lives of others. Other improvements in the critical area of S&T include additional funding of independent analysis for homeland security S&T research and setting of standards for homeland security technology.

We will continue to build upon this foundation of scientific and technological advancement and support funding for research and development to further strengthen the security of the Homeland. We will streamline processes and reduce red tape in order to enhance our partnerships with the country's national research enterprise, including within and among Federal departments and agencies. Specifically, we will continue to engage in disciplined dialogue about the threats we face, our strategies to counter them, and how S&T can bridge gaps in approaches or facilitate the more effective and efficient achievement of our objectives. Our collaborative S&T efforts should continue to explore existing or emerging technologies used for multiple or non-security specific purposes and develop rapid prototyping methods to adapt

---

them to fill critical homeland security needs. Research in systems and operations science that will allow the integration of technology into functional capability is of equal importance. For example, a sound scientific knowledge base regarding health and medical response systems could improve our ability to manage the health consequences of disasters. By promoting the evolution of current technologies and fielding new, revolutionary capabilities, S&T will remain an essential and enduring enabler of our *Strategy*.

## LEVERAGING INSTRUMENTS OF NATIONAL POWER AND INFLUENCE

In the wake of both the September 11 terrorist attacks and lessons learned from our response to Hurricane Katrina, the United States has used its instruments of national power and influence – diplomatic, information, military, economic, financial, intelligence, and law enforcement – to prevent terrorism, protect the lives and livelihoods of the American people, and respond to and recover from incidents. For instance, we have enhanced our ability to analyze and integrate all intelligence pertaining to terrorism through the establishment of the Office of the Director of National Intelligence and the National Counterterrorism Center as well as the creation of an Information Sharing Environment. The general sharing of information, however, extends beyond terror-related intelligence, and we will continue to enhance our processes for sharing all relevant and appropriate information throughout our levels of government and with the private and non-profit sectors and our foreign partners on the full range of homeland security issues.

We are applying targeted financial sanctions to identify and isolate terrorist financiers and facilitators and using a restructured approach to economic assistance, both overseas to meet current and long-term challenges such as terrorism, and here at home to assist in the recovery of communities severely affected by catastrophic homeland security incidents. We also are building enduring public-private partnerships to leverage our Nation's economic power by driving improvements in global security practices, including measures relating to international air travel and global supply chains. We are engaging in transformational diplomacy within the international arena as well as leveraging our engagement with and among Federal, State, local, Tribal, and private sector partners here in the Homeland. We will continue to utilize our public diplomacy and strategic communications resources to offer a positive vision of hope and opportunity that is rooted in our most basic values; work with our partners to isolate and discredit those who espouse ideologies of hate and oppression; and nurture common interests and values between Americans and peoples of different countries, cultures, and faiths across the world.

### Information Sharing Environment

In December 2004, Congress passed and the President signed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). IRTPA calls for, among other things, the creation of the Information Sharing Environment (ISE) – a trusted partnership among all levels of government, the private sector, and our foreign partners to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States through the appropriate exchange of terrorism information.

In addition, IRTPA establishes a Program Manager for the ISE who is responsible for overseeing its implementation. With the enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, the ISE has been expanded further to include not only “terrorism information” as defined in IRTPA but also other categories of homeland security information and weapons of mass destruction information.

---

As we sustain the evolution underway in these areas, success in securing the Homeland requires that we prioritize the continued transformation of our law enforcement and military instruments of national power. Our Nation's law enforcement community – Federal, State, local, and Tribal authorities – collaborate to detect, prevent, and disrupt a range of threats to the public, including terrorism. Our Federal law enforcement community is composed of more than 100,000 full-time personnel who play a decisive leadership role with respect to terrorism and related homeland security matters, including collecting and analyzing significant terrorist and criminal information through more than 100 Federal Bureau of Investigation-led Joint Terrorism Task Forces. Moreover, the U.S. Attorney for each of our country's 94 Federal judicial districts leads an Anti-Terrorism Advisory Council that brings together a cross-section of investigators and prosecutors from all levels of government, as well as first responders and private security personnel, to coordinate counterterrorism initiatives and support the operational efforts of the Joint Terrorism Task Forces.

Our State, local, and Tribal law enforcement communities, representing more than one million personnel from coast to coast, also play an integral role in the all-hazards approach to homeland security. Their role includes active engagement in a broad array of activities that detect and investigate potential threats, protect the American people and critical infrastructures, and restore and maintain law and order in the wake of catastrophic incidents. We will continue to work with and enable State and local fusion centers to leverage their capabilities in the War on Terror and maximize the flow of information among Federal, State, local, and Tribal entities. State, local, and Tribal law enforcement and other first responders also are the leaders in maintaining public safety by performing other essential response services, such as conducting evacuations.

Given the significant overall demands of homeland security and the simultaneously increasing technological and organizational sophistication of terrorist and criminal elements, there is a growing need to better manage and more efficiently leverage all of our law enforcement resources. Specifically, we must build on six years of progress to further enhance collaboration among our numerous law enforcement entities, developing a common baseline for law enforcement activities (e.g., standardizing information collection and collation, reporting procedures, and data archiving across all jurisdictions in order to improve analysis and detection of emerging threats or patterns) so that they may work together seamlessly throughout the Nation. This common approach must be capable of tailoring activities at each level to support specific priorities of importance to their respective communities and, as necessary, be able to fulfill select requests for information as part of the broader national effort to secure the Homeland. The approach should be consciously designed to be all-crimes relevant so that investments in information technology, communications equipment, and other support structures are used to drive efficiencies across the full range of law enforcement activities. We also will continue to fund training and exercises as well as the development of a common baseline for reporting and requesting information requirements. By enabling seamless integration and true unity of effort among all Federal, State, local, and Tribal law enforcement entities, we will better protect and defend the Homeland and the American people.

Our Nation's armed forces are crucial partners in homeland security. Our active, reserve, and National Guard forces are integrated into communities throughout our country, and they bring to bear the largest and most diverse workforce and capabilities in government to pro-

---

tect the United States from direct attacks and conduct missions to deter, prevent, and defeat threats against our Nation.

Over the past several years, our armed forces have been preparing to meet a wider range of challenges to our Nation by restructuring their capabilities, rearranging their global force posture, and adapting forces to better fight the War on Terror. While defending the Homeland is appropriately a top priority for the Department of Defense, the country's active, reserve, and National Guard forces also must continue to enhance their ability to provide support to civil authorities, not only to help prevent terrorism but also to respond to and recover from man-made and natural disasters that do occur. Working with the Nation's Governors and State Adjutants General, the Department of Defense must develop operational plans based upon the national planning scenarios that will integrate and synchronize military forces to achieve unity of effort in support of homeland security missions across the Nation. These plans will determine specific military requirements and capabilities for accomplishing homeland security missions that will most effectively be met by the combined effort of active, reserve, and National Guard forces.

## LEGISLATIVE BRANCH

Homeland security at the Federal level is not the sole purview of the executive branch of government. The Congress also must take bold steps to fulfill its responsibilities in the national effort to secure the Homeland and protect the American people. The current committee structure, for example, creates competing initiatives and requirements and fails to establish clear and consistent priorities or provide optimal oversight. Accordingly, both houses of the Congress should take action to further streamline the organization and structure of those committees that authorize and appropriate homeland security-related funds and otherwise oversee homeland security missions. The Congress also should fully embrace a risk-based funding approach so that we best prioritize our limited resources to meet our most critical homeland security goals and objectives first, as opposed to distributing funds and making decisions based on political considerations. In addition, Congress should help ensure that we have the necessary tools to address changing technologies and homeland security threats while protecting privacy and civil liberties. Finally, in the same manner that Congress was an important partner in building an effective national security system during the Cold War and beyond, a strong partnership with Congress will be essential to help secure the Homeland in the years ahead.



---

## CONCLUSION

Since the turn of the millennium, our Nation has endured history's deadliest attack of international terrorism and the most destructive natural disaster to strike American soil. In the face of these challenges, America has responded courageously, with focus and clarity of purpose, and today we are safer, stronger, and better prepared to address the full range of catastrophic events, including man-made accidents and natural disasters, that threaten us. Our work, however, is far from over. We remain resolute in our commitment to prevent and disrupt terrorist attacks in the Homeland, protect the American people and the Nation's critical infrastructure and key resources, and effectively respond to and recover from those incidents that do occur. Working together, our Nation will secure the Homeland in order to sustain our way of life – now and for generations to come.

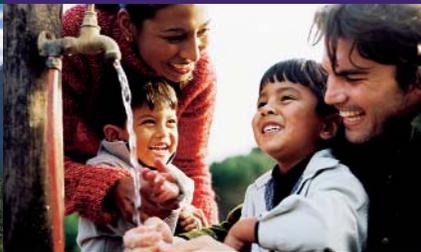




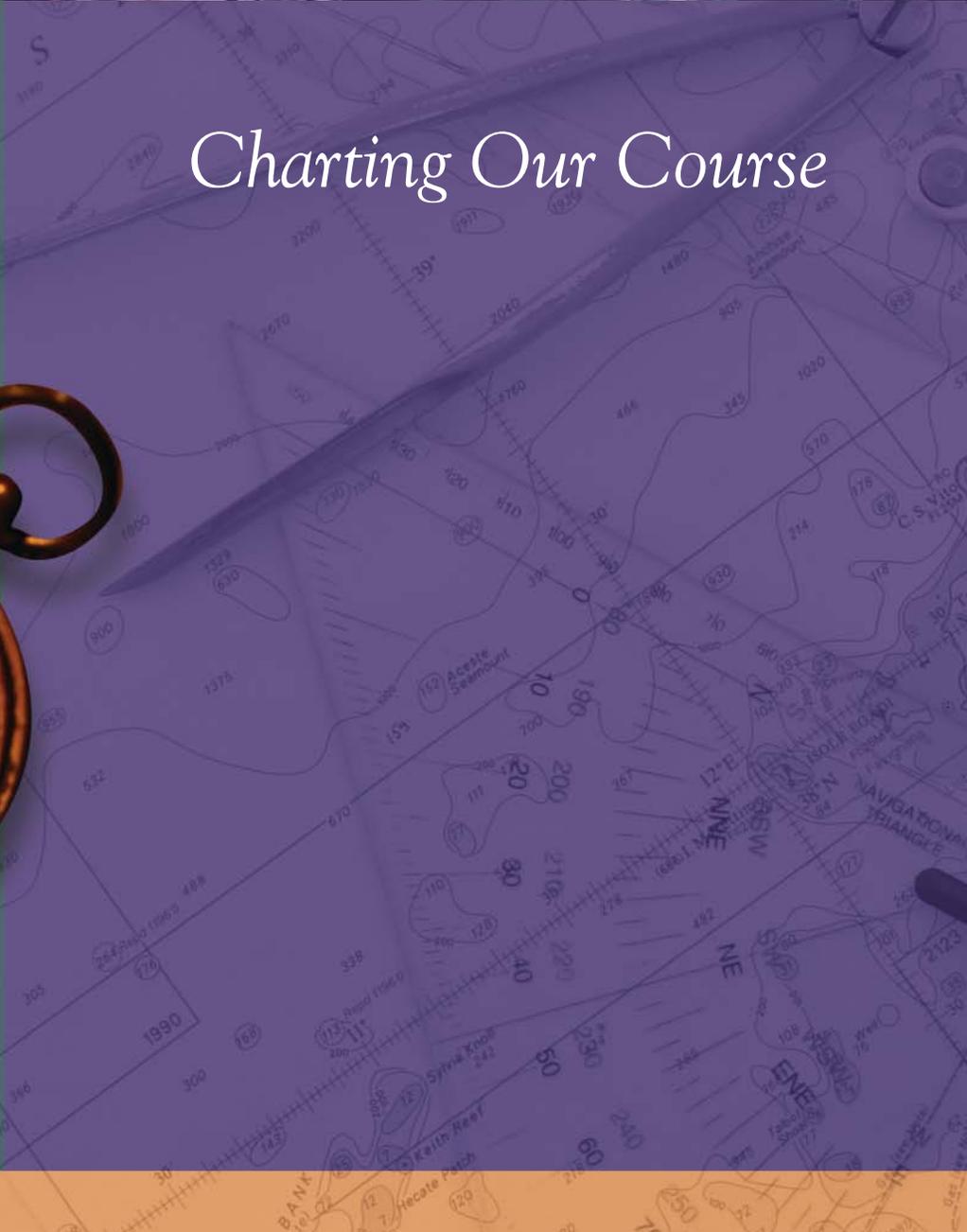


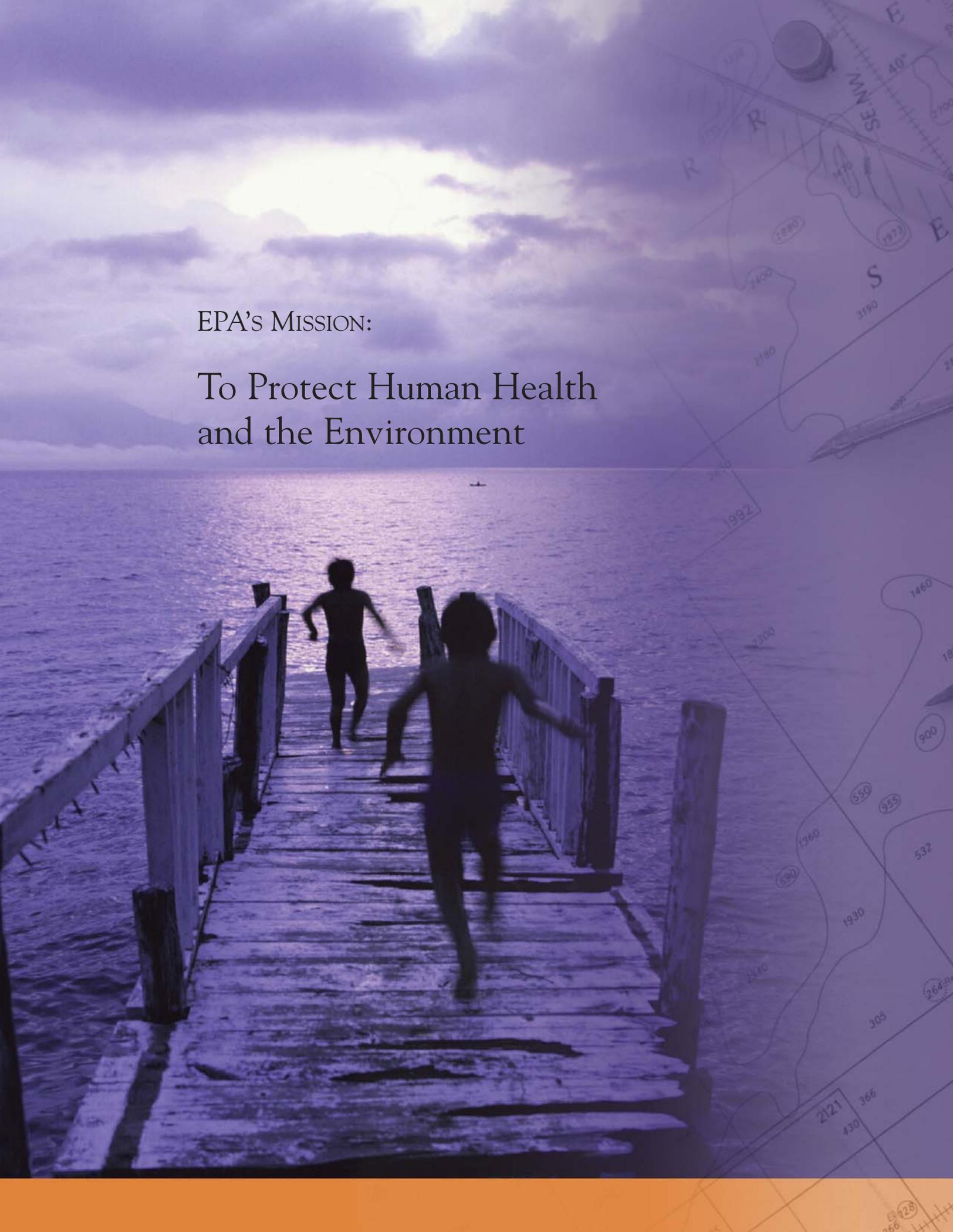


# 2006-2011 EPA Strategic Plan



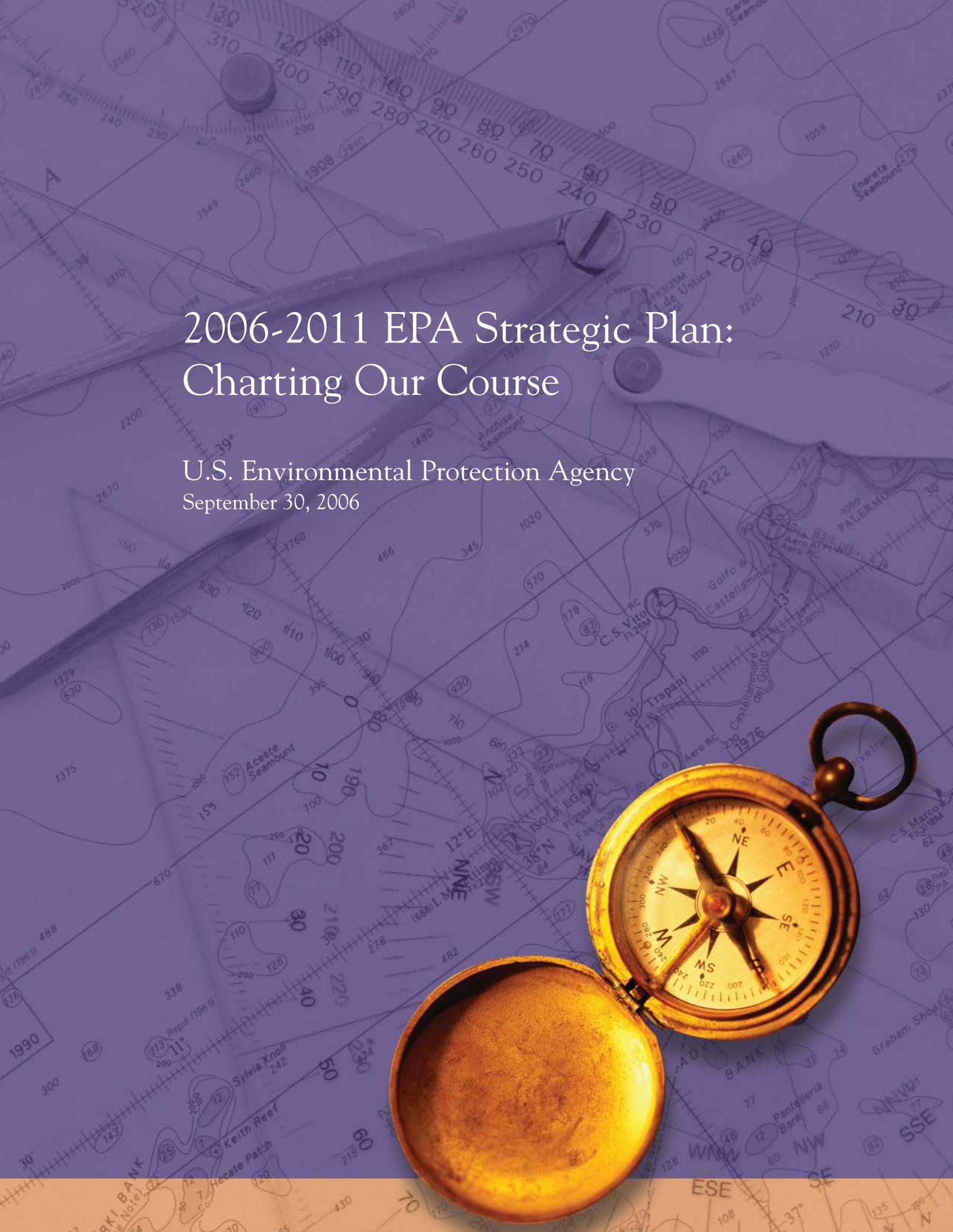
## *Charting Our Course*



The image is a composite. The background is a sunset over the ocean, with the sun low on the horizon and its light reflecting on the water. In the foreground, two children are running away from the viewer on a wooden pier that extends into the sea. The pier has a simple railing. On the right side of the image, there is a semi-transparent map overlay. The map shows contour lines with numerical values such as 1000, 1200, 1400, 1600, 1800, 1930, 1992, 2000, 2100, 2140, 2160, 2180, 2210, 2221, 2300, 2366, 2400, 2428, 2600, 2640, 2660, 2700, 2720, 2760, 2800, 2840, 2880, 2920, 2960, 3000, 3050, 3100, 3150, 3190, 3240, 3280, 3320, 3360, 3400, 3440, 3480, 3520, 3560, 3600, 3640, 3680, 3720, 3760, 3800, 3840, 3880, 3920, 3960, 4000, 4040, 4080, 4120, 4160, 4200, 4240, 4280, 4320, 4360, 4400, 4440, 4480, 4520, 4560, 4600, 4640, 4680, 4720, 4760, 4800, 4840, 4880, 4920, 4960, 5000. The map also shows some text like 'R R', 'S', 'SE NW', and '40°'.

EPA's MISSION:

To Protect Human Health  
and the Environment

A topographic map with a ruler and a compass. The map shows contour lines, elevation numbers, and various geographical features. A ruler is placed horizontally across the upper part of the map. A compass is in the lower right corner, showing cardinal and intercardinal directions. The background is a light blue color with a subtle grid pattern.

# 2006-2011 EPA Strategic Plan: Charting Our Course

U.S. Environmental Protection Agency  
September 30, 2006



# CONTENTS

Introduction .....	5
Goal 1—Clean Air and Global Climate Change .....	8
Objective 1.1: Healthier Outdoor Air .....	12
Objective 1.2: Healthier Indoor Air .....	19
Objective 1.3: Protect the Ozone Layer .....	20
Objective 1.4: Radiation .....	21
Objective 1.5: Reduce Greenhouse Gas Emissions .....	23
Objective 1.6: Enhance Science and Research .....	25
Goal 2—Clean and Safe Water .....	32
Objective 2.1: Protect Human Health .....	36
Objective 2.2: Protect Water Quality .....	43
Objective 2.3: Enhance Science and Research .....	50
Goal 3—Land Preservation and Restoration .....	58
Objective 3.1: Preserve Land .....	62
Objective 3.2: Restore Land .....	67
Objective 3.3: Enhance Science and Research .....	72
Goal 4—Healthy Communities and Ecosystems .....	78
Objective 4.1: Chemical, Organism, and Pesticide Risks .....	83
Objective 4.2: Communities .....	91
Objective 4.3: Restore and Protect Critical Ecosystems .....	97
Objective 4.4: Enhance Science and Research .....	109



Goal 5—Compliance and Environmental Stewardship .....	126
Objective 5.1: Achieve Environmental Protection Through Improved Compliance .....	130
Objective 5.2: Improve Environmental Performance Through Pollution Prevention and Other Stewardship Practices .....	133
Objective 5.3: Improve Human Health and the Environment in Indian Country .....	138
Objective 5.4: Enhance Society’s Capacity for Sustainability Through Science and Research .....	140
Cross-Goal Strategies .....	146
Results and Accountability .....	149
Innovation and Collaboration .....	152
Best Available Science .....	158
Appendix A: Social Costs and Benefits .....	163
Appendix B: Proposed Future Program Evaluations .....	165
Appendix C: Summary of Consultation Efforts .....	173
Appendix D: Areas of Coordination Between EPA and Other Federal Agencies .....	179



## INTRODUCTION

Since the U.S. Environmental Protection Agency (EPA) was established in 1970, we have worked with our federal, state, tribal, and local government partners to advance our mission to protect human health and the environment. Together, we have made tremendous progress in protecting and restoring the nation's air, water, and land.

But while we have achieved a great deal, we recognize that much work remains. The environmental problems we are facing in 2006 are more complex than those of 30 years ago, and implementing solutions is more challenging. Recent national and international events, such as the devastation left by Hurricane Katrina, the advance of Avian flu, threats to homeland security, and population growth and its associated resource consumption, are altering the environment in unprecedented ways. Scientific advances and emerging technologies offer new opportunities for protecting human health and the environment, but also pose new risks and challenges. We recognize that today's environmental problems cannot be solved by traditional regulatory controls alone; they will require the combined expertise, perspectives, and resources of many. More than ever before, we need to look toward the future to anticipate potential threats to human health and the environment, establish clear priorities, and prepare ourselves to address them.



### GOALS OF THE 2006-2011 STRATEGIC PLAN

- Clean Air and Global Climate Change
- Clean and Safe Water
- Land Preservation and Restoration
- Healthy Communities and Ecosystems
- Compliance and Environmental Stewardship

### CROSS-GOAL STRATEGIES

- Results and Accountability
- Innovation and Collaboration
- Best Available Science



### OUR GOALS AND STRATEGIES

EPA's 2006-2011 *Strategic Plan* sets out an ambitious road map for environmental protection over the next 5 years. In developing this *Plan*, we have sharpened our focus on achieving measurable environmental results. Our five strategic goals reflect the results we are striving to achieve: Clean Air and Global Climate Change, Clean and Safe Water, Land Preservation and Restoration, Healthy Communities and Ecosystems, and Compliance and Environmental Stewardship.

EPA Administrator Steve Johnson has established key principles to accelerate the pace of environmental protection, and these three principles are reflected in our “cross-goal” strategies—common themes for our work under each of our strategic goals:

- **Results and Accountability.** EPA is committed to being a good steward of our environment and a good steward of America’s tax dollars. To provide the public with the environmental results it expects and deserves, we must operate as efficiently and effectively as possible. Accountability for results is a key component of the President’s Management Agenda, designed to make government citizen-centered, results-oriented, and market-based.
- **Innovation and Collaboration.** Our progress depends both on our ability and continued commitment to identify and use innovative tools, approaches, and solutions to address environmental problems and to engage extensively with our partners, stakeholders, and the public. Under each of our goals, we are working to promote a sense of environmental stewardship and a shared responsibility for addressing today’s challenges.
- **Best Available Science.** EPA needs the best scientific information available to anticipate potential environmental threats, evaluate risks, identify solutions, and develop protective standards. Sound science helps us ask the right questions, assess information, and characterize problems clearly to inform Agency decision makers.



## GUIDING MANAGEMENT AND BUDGET DECISIONS

In setting out our goals for the coming 5 years and describing how we intend to achieve them, our *Strategic Plan* provides the foundation for all of EPA’s planning, budgeting, performance measurement, and accountability processes. We will design annual performance goals and measures, which are presented in the President’s budget request to Congress, to achieve the long-term strategic goals set out in this *Plan*. We will report on our performance against these annual goals and measures in our annual *Performance and Accountability Report* and

use this performance information as we establish priorities and develop future budget submissions. This process will come full circle as we evaluate these performance data to develop our 2009-2014 and future *Strategic Plans*. In addition, our strategic planning and decision making



benefit from information provided by new environmental indicators that we are developing, in particular for our forthcoming *Report on the Environment*. Information derived from these indicators help us better articulate and further improve the long-term measures contained in our *Strategic Plan*.

## IMPROVING OUR STRATEGIC PLAN

While EPA's 2006-2011 *Strategic Plan* retains the five-goal structure introduced in our 2003 *Plan*, it contains a number of improvements and additions. For example, under each goal we have provided a discussion of "Emerging Issues and External Factors"—important new challenges and opportunities that are likely to arise in the coming years. The goal chapters also include new information about developing the long-term measures included in the *Plan*, particularly their relationship to annual performance measures, measures provided in the Office of Management and Budget's Program Assessment Rating Tool, and the new environmental indicators being developed for EPA's *Report on the Environment*. This *Plan* also reflects our increased emphasis on activities and measures that address tribal environmental and health issues, environmental justice concerns, environmental stewardship, and strategic management of human capital.



We have prepared this *Strategic Plan* to present our vision for the future and to guide our work over the coming years to achieve these results. We hope that you will join with us to realize our common desire for a cleaner, healthier environment for all Americans.

Lyons Gray  
Chief Financial Officer



GOAL 1 :

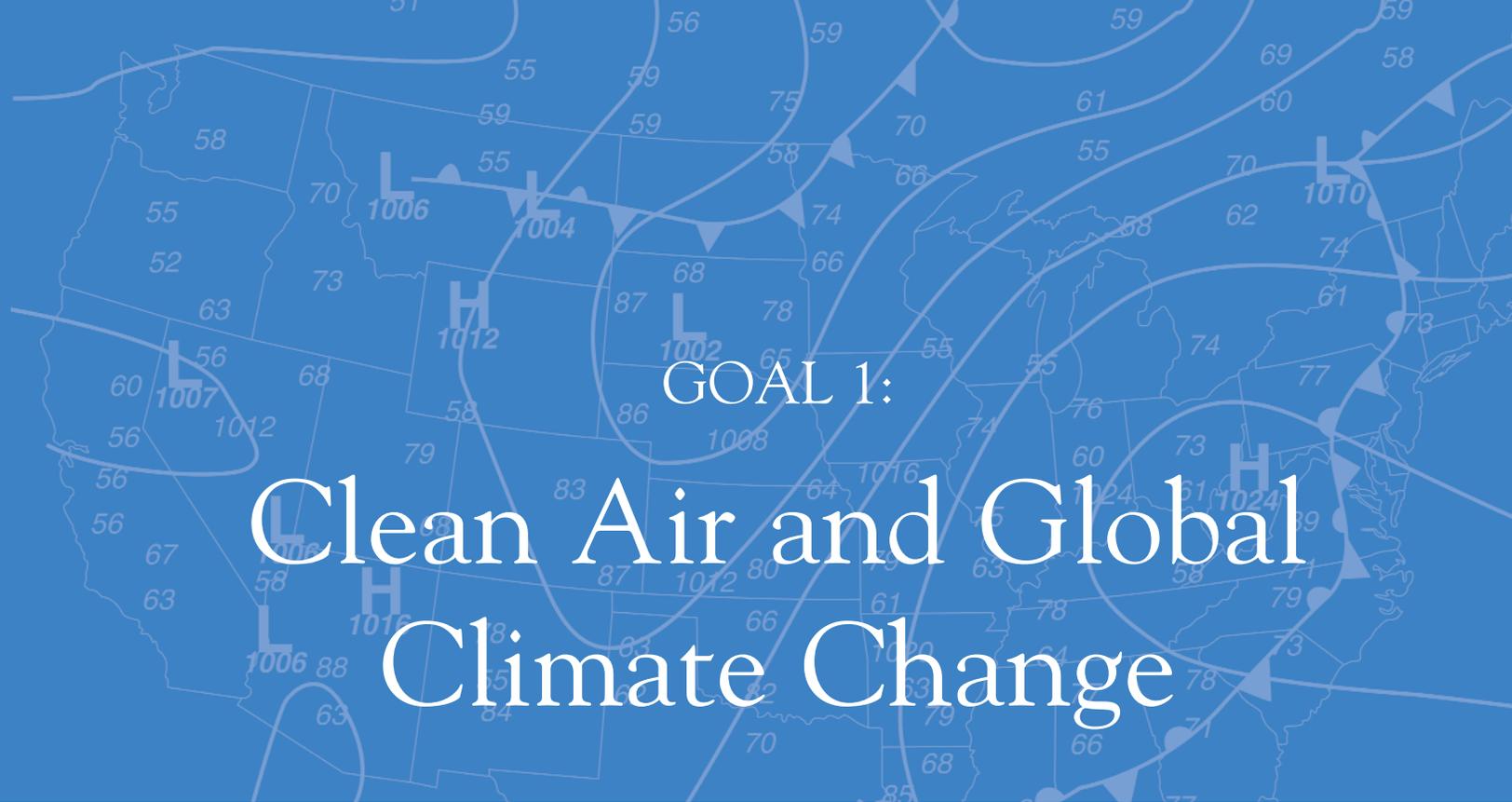




# Clean Air *and* Global Climate Change

*Protect and improve the air so it is healthy to breathe and risks to human health and the environment are reduced. Reduce greenhouse gas intensity by enhancing partnerships with businesses and other sectors.*





# GOAL 1: Clean Air and Global Climate Change

Air pollution comes from many sources: factories and power plants; drycleaners; cars, buses, and trucks; even windblown dust and wildfires. It can threaten human health, causing breathing difficulties, long-term damage to respiratory and reproductive systems, cancer, and premature death. Certain chemicals emitted into the air diminish the protective ozone layer in the upper atmosphere, resulting in overexposure to ultraviolet radiation and increased rates of skin cancer, cataracts, and other health and ecological effects. Air pollution can also affect the environment by reducing visibility; damaging crops, forests, and buildings; acidifying lakes and streams; and stimulating the growth of algae in estuaries and the build-up of toxins in fish. These effects pose a particular risk to Native Americans and others who subsist on plants, fish, and game. Rapid development and urbanization in other countries are creating air pollution that threatens not only those countries but also the United States, since air pollution can travel great distances and across national boundaries.

EPA works to protect human health and the environment by developing regulations and establishing partnerships with other federal agencies, states, tribes, local governments, business and industry, environmental groups, and other stakeholders in programs to reduce air pollution. And according to our annual summary of air quality trends since the 1970s,<sup>1</sup> air quality in the United States has steadily improved. Even as our economy has grown, miles traveled by cars and trucks increased, and energy consumption risen, the trend toward cleaner air has continued.

EPA is dedicated to improving the quality of the air Americans breathe, and we will continue to look for innovative, effective solutions to the nation's remaining air pollution problems. We use a variety of approaches and tools to accomplish this. For example, we are addressing problems with broad national or global impact—emissions from power plants and other large sources, pollution from motor vehicles and fuels, and stratospheric ozone depletion—at the federal level, using our traditional regulatory tools as well as innovative, market-based techniques such as

OBJECTIVES	
Objective 1.1: Healthier Outdoor Air	12
Objective 1.2: Healthier Indoor Air	19
Objective 1.3: Protect the Ozone Layer	20
Objective 1.4: Radiation	21
Objective 1.5: Reduce Greenhouse Gas Emissions	23
Objective 1.6: Enhance Science and Research	25

the earth,<sup>7</sup> increasing the risk of overexposure and consequent health effects, including skin cancer, cataracts, and other illnesses. More than a million new cases of skin cancer are diagnosed each year;<sup>8</sup> 1 in 5 Americans is expected to experience skin cancer; and more than half of all Americans develop cataracts by the time they are 80 years old.<sup>9</sup>

As a signatory to the *Montreal Protocol on Substances that Deplete the Ozone Layer*,<sup>10</sup> the United States regulates and enforces Montreal Protocol provisions domestically. In accordance with this international treaty and related Clean Air Act requirements,<sup>11</sup> EPA will continue implementing domestic programs to reduce and control ozone-depleting substances (ODS) and enforcing rules on their production, import, and emission. Our approach combines market-based efforts with sector-specific technology guidelines to facilitate alternatives to hydrochlorofluorocarbons. We will work in partnership with stakeholders to smooth the transition to ODS substitutes that reduce greenhouse gas emissions and save energy and act on 100 percent of the petitions for substitutes within 90 days of receipt. To help reduce emissions internationally, we will assist in transferring technology to developing countries and work with them to accelerate the phase-out of ODS. We estimate that from 1990 to 2165, worldwide phase-out of ODS will save 6.3 million lives from fatal skin cancer, avoid 299 million cases of nonfatal skin cancers,

and avoid 27.5 million cases of cataracts in the United States alone.<sup>12</sup>

Because the ozone layer is not expected to recover until the middle of this century at the earliest,<sup>13</sup> the public will continue to be exposed to high levels of UV radiation.<sup>14</sup> To address this concern, we will continue education and outreach efforts to encourage school children and their caregivers to change their behavior to reduce UV-related health risks. The SunWise program ([www.epa.gov/sunwise/](http://www.epa.gov/sunwise/)), which we expect to grow from 200 participating kindergarten–grade 8 schools in 2000 to 20,000 by 2011, will teach thousands of school children and adults how to protect themselves from overexposure to the sun.



## OBJECTIVE 1.4: RADIATION

THROUGH 2011, WORKING WITH PARTNERS, MINIMIZE UNNECESSARY RELEASES OF RADIATION AND BE PREPARED TO MINIMIZE IMPACTS TO HUMAN HEALTH AND THE ENVIRONMENT SHOULD UNWANTED RELEASES OCCUR.

### Strategic Targets

- By 2011, 77 percent of the U.S. land area will be covered by the RadNet ambient radiation air monitoring system. (2001 baseline is 35 percent of the U.S. land area.)
- By 2011, the radiation program will maintain a 90 percent level of readiness of radiation program personnel and assets to support federal radiological emergency response and recovery operations. (2005 baseline is a 50 percent level of readiness.)

## MEANS AND STRATEGIES FOR MINIMIZING RELEASES OF RADIATION AND RELATED IMPACTS

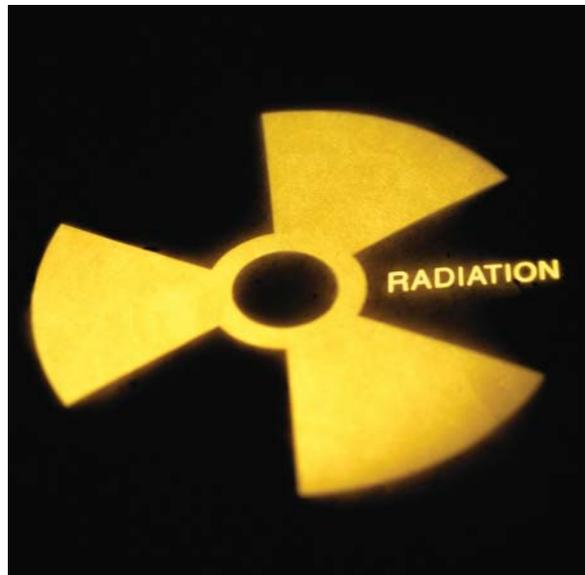
EPA continues to meet statutory mandates for managing radiation waste and controlling radioactive emissions and to fulfill its responsibilities under presidential decision directives for radiological emergency preparedness and response. These responsibilities form the core of our strategy to protect the public and the environment from unnecessary exposure to radiation. We will work with states, tribes, and industry to develop innovative training, public information, and partnership programs to minimize these exposures. We will also conduct radiation-risk assessments to evaluate health risks from radiation exposure; determine appropriate levels for cleaning up contaminated sites; and develop radiation protection and risk management policy, guidance, and rules.

Mining and processing naturally radioactive materials for use in medicine, power generation, consumer products, and industry inevitably generate emissions and waste. EPA will provide guidance and training to help federal and state agencies prepare for emergencies at U.S. nuclear plants, transportation accidents involving shipments of radioactive materials, and acts of nuclear terrorism. EPA will also develop guidance for cleaning up radioactively-contaminated Superfund sites. To manage radioactive releases and exposures, we will conduct health-risk site assessments; risk modeling, cleanup, and waste management activities;

voluntary programs to minimize exposure to radiation in commercial products and industrial applications; national radiation monitoring; and radiological emergency response.

In response to state and local organizations, EPA will continue to provide advice and guidance to help locate, identify, and dispose of radioactive sources that find their way into non-nuclear facilities, particularly scrap yards, steel mills, and municipal waste disposal facilities. We will work with the International Atomic Energy Agency and other federal agencies to prevent metals and finished products suspected of having radioactive contamination from entering the country. Through partnerships with states, local agencies, and tribes we will locate and secure lost, stolen, or abandoned radioactive sources within the United States and investigate and promote practices to reduce industrial radioactive releases. We will expand our ongoing efforts to ensure that tribes receive assistance in dealing with radon exposures in their homes and schools.

One of EPA's major responsibilities related to radiation is certifying that all radioactive waste shipped by the U.S. Department of Energy (DOE) to the Waste Isolation Pilot Plant is disposed of safely and according to EPA's standards. We inspect waste generator facilities and biennially evaluate DOE's compliance with applicable environmental laws and regulations.



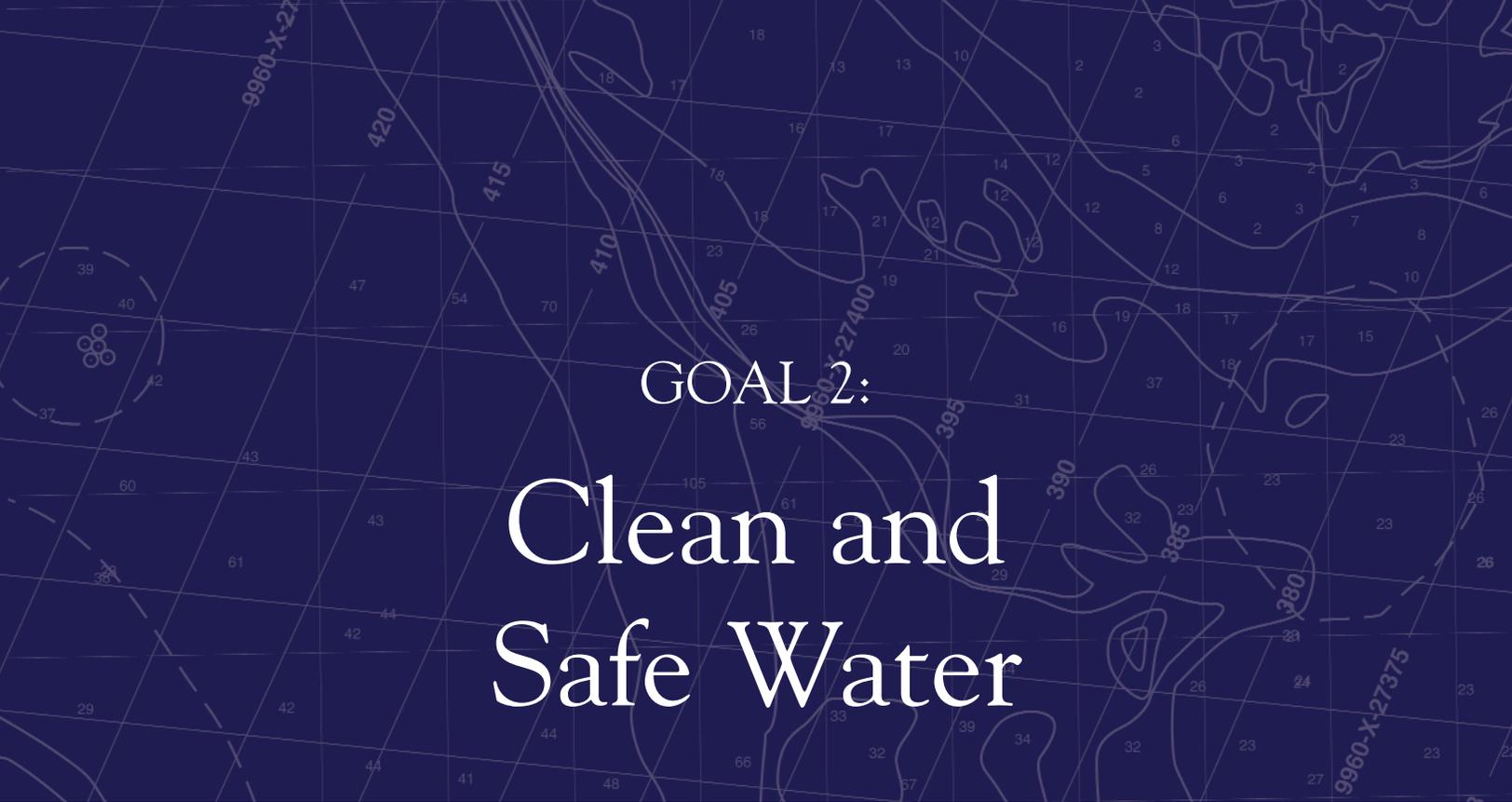




# Clean *and* Safe Water

*Ensure drinking water is safe.  
Restore and maintain oceans, water-  
sheds, and their aquatic ecosystems  
to protect human health, support  
economic and recreational activities,  
and provide healthy habitat for fish,  
plants, and wildlife.*





## GOAL 2: Clean and Safe Water

Since the Clean Water and Safe Drinking Water Acts were enacted over 3 decades ago, government, citizens, and the private sector have worked together to make dramatic progress in improving the quality of surface water and drinking water.

Thirty years ago, many of the nation's drinking water systems provided water to the tap with very limited treatment. Drinking water was too often the cause of illnesses linked to microbiological and other contaminants. Today, drinking water systems monitor the quality of the water they provide and treat water to ensure compliance with standards covering a wide range of contaminants. In addition, efforts to protect waters that are sources of drinking water are helping to keep drinking water safe.

Thirty years ago, about two-thirds of the surface waters assessed by states were not attaining basic water quality goals and were considered polluted.<sup>1</sup> Some of the nation's rivers were open sewers posing health risks, and many water bodies were so polluted that swimming, fishing, and recreation were impossible. Today, the number of polluted waters has been dramatically reduced, and many clean waters are getting even healthier. A massive investment of federal, state, and local funds has resulted in a new generation of sewage treatment. More than 50

industrial sectors now comply with nationally consistent discharge regulations. In addition, sustained efforts to implement best management practices have helped reduce runoff of pollutants from diffuse, or "nonpoint," sources.

### OBJECTIVES

Objective 2.1: Protect Human Health . . . . . 36

Objective 2.2: Protect Water Quality . . . . . 43

Objective 2.3: Enhance Science and Research . . . 50

Cleaner, safer water has renewed recreational, ecological, and economic interests in communities across the nation. The recreation, tourism, and travel industry is one of the largest employers in the country, and a significant portion of recreational spending comes from swimming, boating, sport fishing, and hunting.<sup>2</sup> In addition, each year, more than 180 million people visit beaches for recreation.<sup>3</sup>

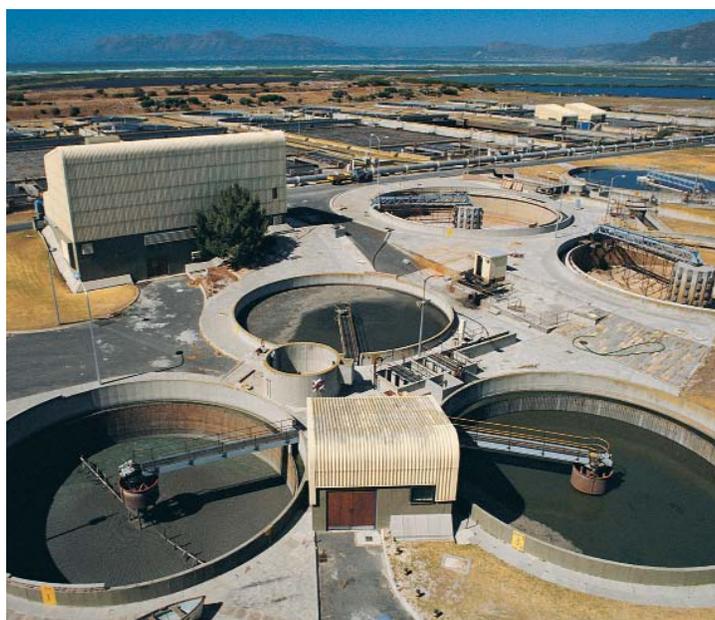
The dramatic restoration of some of the nation's most polluted waters has paid large dividends in enhanced recreation, healthier fisheries, and stronger local economies. Many of the nation's best-known water pollution problem areas are showing the results of years of restoration efforts. The Cuyahoga River, once so polluted that it caught fire, is now busy with boats and harbor businesses. Oregon's Willamette River has been restored to provide swimming, fishing, and water sports. In Boston, the Charles River, once badly polluted, increasingly supports boating and related recreation.



### Water Infrastructure Security

The President has given EPA primary responsibility for coordinating federal, state, and local authorities in the protection of drinking water systems. The Bioterrorism Act of 2002 requires community water systems serving more than 3,300 people to develop vulnerability assessments and to certify emergency response plans. With most of this work now completed, EPA has shifted its focus to reducing risks associated with these vulnerabilities. Our water security program will provide tools and assistance to prevent, detect, respond to, and recover from intentional acts and natural disasters; encourage mutual aid agreements within states and regions; and provide training and exercises to improve water utilities' preparedness.

We are also undertaking two significant initiatives: (1) EPA's Homeland Security Sentinel Initiative (formerly known as Water Sentinel), which will deploy and test a contamination warning system; and (2) the Water Alliance for Threat Reduction, which will provide direct water security training to drinking water utilities serving more than 100,000 people. Collectively, these efforts will represent a robust approach for addressing the threats, vulnerabilities, and consequences facing the water sector.



### Tribal Access to Safe Drinking Water

The 2002 World Summit on Sustainable Development in Johannesburg adopted the goal of reducing the number of people lacking access to safe drinking water and basic sanitation by 50 percent by 2015.<sup>8</sup> In the United States, EPA will focus on providing infrastructure to increase the number of tribal homes with access to safe drinking water and basic sanitation. We will support develop-

ment of drinking water and wastewater facilities in Indian country and Alaska Native villages using set-aside funds from the Drinking Water and Clean Water State Revolving Funds as well as targeted grants.

We will also work with other federal agencies that play key roles in addressing this problem, such as the U.S. Departments of Health and Human Services, Interior, and Agriculture, to coordinate a strategy for improving tribes' access to water and sanitation. (Note that projects to improve infrastructure along the U.S.-Mexico Border and in the Pacific Islands will also increase peoples' access to safe drinking water and basic sanitation. They are described under Goal 4: Healthy Communities and Ecosystems.)

To learn more go to: [www.epa.gov/safewater/](http://www.epa.gov/safewater/).





# Land Preservation *and* Restoration

*Preserve and restore the land by using innovative waste management practices and cleaning up contaminated properties to reduce risks posed by releases of harmful substances.*



## GOAL 3:

# Land Preservation and Restoration

Uncontrolled, wastes released on the land can migrate—contaminating drinking water, causing illness or disease, and threatening healthy ecosystems. EPA is working to minimize risks and to preserve and restore land using the most effective waste management and cleanup methods available. We rely on a variety of strategies: reducing waste at its source, recycling, managing waste to prevent spills and releases, and cleaning up contaminated property. We are especially concerned about threats to our most sensitive populations: children, the elderly, and people with chronic diseases.

The Resource Conservation and Recovery Act (RCRA)<sup>1</sup> and the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA, or Superfund)<sup>2</sup> provide the legal authority for most of EPA's work to preserve and restore the land. We use Superfund authority to clean up uncontrolled or abandoned hazardous waste sites and return land to productive use. Under RCRA, we work in partnership with states and tribes to address risks associated with leaking underground storage tanks and generation and management of hazardous and non-hazardous wastes. Tribal governments are the

primary parties for setting standards, making environmental policy decisions, and managing programs consistent with federal standards and regulations for reservations, and our regional offices work directly with them as the recognized independent authorities for reservation affairs.

We also use authorities provided under the Clean Air Act,<sup>3</sup> Clean Water Act,<sup>4</sup> and Oil Pollution Act of 1990<sup>5</sup> to protect against spills and releases of hazardous materials. Controlling the many risks posed by accidental and intentional releases of harmful substances presents a significant challenge. To minimize these risks, EPA integrates prevention, preparedness, and response efforts. We conduct spill-prevention activities to keep harmful substances from being

released to the environment. And we continue to improve our readiness to respond and minimize contamination and harm to the environment when spills do occur by coordinating with our partners at all levels of government, developing clear authorities, training personnel, and providing proper equipment.

EPA is committed to ensuring environmental justice for all people, regardless of race, color, national origin, or income. Recognizing that minority and/or low-income communities frequently may be exposed disproportionately

### OBJECTIVES

<b>Objective 3.1:</b> Preserve Land .....	62
<b>Objective 3.2:</b> Restore Land .....	67
<b>Objective 3.3:</b> Enhance Science and Research .....	72

## OBJECTIVE 3.2: RESTORE LAND

By 2011, CONTROL THE RISKS TO HUMAN HEALTH AND THE ENVIRONMENT BY MITIGATING THE IMPACT OF ACCIDENTAL OR INTENTIONAL RELEASES AND BY CLEANING UP AND RESTORING CONTAMINATED SITES OR PROPERTIES TO APPROPRIATE LEVELS.

**Sub-objective 3.2.1: Prepare for and Respond to Accidental and Intentional Releases.** By 2011, reduce and control the risks posed by accidental and intentional releases of harmful substances by improving our nation's capability to prevent, prepare for, and respond more effectively to these emergencies.

### Strategic Targets

- By 2011, achieve and maintain at least 95 percent of the maximum score on readiness evaluation criteria in each region.
- By 2011, complete an additional 975 Superfund-lead hazardous substance removal actions. (In FY 2005, 175 of these actions were completed.)
- By 2011, oversee and complete an additional 650 voluntary removal actions. (In FY 2005, 137 of these actions were completed.)
- By 2011, reduce by 25 percent the gallons of oil spilled by facilities subject to Facility Response Plan regulations relative to the 601,000 gallons of oil spilled in 2003.
- By 2011, inspect (and ensure compliance at) 90 percent of the estimated 4,200 facilities subject to Facility Response Plan regulations, up from 50 percent in 2004.

**Sub-objective 3.2.2: Clean Up and Revitalize Contaminated Land.** By 2011, control the risks to human health and the environment at contaminated properties or sites through cleanup, stabilization, or other action and make land available for reuse.

### Strategic Targets

- By 2011, make final assessment decisions at 40,491 of 44,700 potentially hazardous waste sites evaluated by EPA to help resolve community concerns on whether these sites require long-term cleanup to protect public health and the environment and to help determine if they can be cleared for possible redevelopment. (By the end of FY 2005, a total of 38,770 final site assessment decisions had been made.)



- By 2011, control all identified unacceptable human exposures from site contamination for current land and/or groundwater use conditions at approximately 85 percent (1,316) of 1,543 Superfund human exposure sites. (The universe of 1,543 is the number of National Priorities List [NPL] sites with potential human exposure pathways as of FY 2005 and includes 172 Superfund federal facility sites. Baseline: By the end of FY 2006, approximately 82 percent [1,266] of sites had human exposures under control.) By 2011, increase to 95 percent the high National

### Strategic Targets

- Each year through 2011, reach a settlement or take an enforcement action before the start of a remedial action at 95 percent of Superfund sites having viable, liable responsible parties other than the federal government.
- Each year through 2011, address all unaddressed costs in statute of limitations cases for sites with unaddressed total past Superfund costs equal to or greater than \$200,000.

### MEANS AND STRATEGIES FOR RESTORING LAND

EPA leads the federal effort to reduce risks posed by contaminated land by responding to releases and potential releases of harmful substances and undertaking cleanups and other activities to return land to beneficial use. We develop and implement prevention measures, improve response capabilities, ensure that response and cleanup actions are effective, and promote protective, sustainable, and productive uses of formerly contaminated properties. We collaborate with private organizations, communities, businesses, and government agencies at every level to accomplish these ends. We also work to increase public understanding of environmental issues and develop a sense of environmental stewardship for land that has been returned to beneficial use.

### PREPAREDNESS AND RESPONSE

National preparedness is essential to ensure that emergency responders are able to deal with multiple, large-scale emergencies, including those that may involve chemicals, oil, biological agents, radiation, or weapons of mass destruction. EPA will continue to enhance its core emergency response program

by providing specialized training on the Incident Command System; developing additional health and safety materials; participating in exercises with federal, state, and local government agencies, including Regional Response Teams; and strengthening response readiness across multiple regions.

We also are working to improve coordination and communication. For example, as part of the National Incident Coordination Team, we will continue to improve mechanisms for coordinating responses to national emergencies. Under the Continuity of Operations/Continuity of Government program, we will upgrade and test plans, facilities, training, and equipment to ensure that essential government business can continue during a catastrophic emergency. And we will expand our National Response Team capabilities for coordinating large-scale responses with the Department of Homeland Security; Federal Emergency Management Agency; Federal Bureau of Investigation; and other federal, state, and local government agencies.

We also are improving our capability for responding to incidents involving harmful chemical, oil, biological, and radiological substances. Each year, EPA personnel assess, respond to, mitigate, and clean up thousands of releases—whether accidental, deliberate, or naturally occurring. These range from small spills at chemical or oil facilities to larger accidental releases in train and highway accidents, and from



natural disasters, such as hurricanes Katrina and Rita, to national emergencies, such as terrorist events. Over the next 2 years, we will expand our current core emergency response program to address prevention and preparedness and cover all aspects of emergency environmental management.

An important component of our land strategy is preventing oil spills and being prepared for spills that do occur so that oil does not reach our nation's waters. Under the Oil Pollution Act,<sup>19</sup> we require certain facilities to develop Facility Response Plans (FRPs) for use in the event of a spill and to practice implementing them. At the end of FY 2004, EPA had inspected (and found in compliance) 50 percent of the estimated 4,200 FRP facilities; over the next 5 years we will work to ensure at least 90 percent compliance.

### CLEANING UP AND REVITALIZING CONTAMINATED SITES

EPA's cleanup programs strive to protect Americans from risks posed by contaminated land; restore the nation's contaminated land; and enable communities safely to return these properties to beneficial economic, ecological, and social use. We work with our federal, state, tribal, and local government partners to identify sites and facilities that need attention and collaborate to clean them up.



EPA's One Cleanup Program is a long-term initiative that encourages our cleanup programs to work together and with all levels of government to ensure that appropriate cleanup tools are used; resources and activities are coordinated; results are effectively communicated to the public; and cleanups are protective and contribute to revitalizing communities, including those with environmental justice concerns. We will strive to treat people fairly, to provide equal opportunity for participating in cleanup decisions, and to ensure that no population bears a disproportionate burden or risk. The One Cleanup Program reflects our effort to coordinate all of EPA cleanup programs, yet provides the flexibility to accommodate different statutory authorities and approaches.

All of our cleanup programs include common elements: initial assessment, stabilization (when needed to control actual or potential exposure and protect local populations), site investigation, selection of appropriate site remedies, implementation and completion of remedies, and promotion of protective uses/reuses.

*Investigating and Assessing Sites.* With our partners, we identify the type and extent of contamination and the actual or potential exposure to people and environmental receptors. We use the data we collect to determine risks and to select remedies. To better address environmental justice concerns and identify areas that may suffer disproportionate impacts, we will encourage broader use of improved sample collection techniques, analytical tools, and indicators.

*Selecting and Implementing Remedies.* We select remedies based on such criteria as affected media (soil, air, groundwater, etc.), cleanup objectives, compliance with applicable laws, implementation issues, and acceptability to state and tribal governments and the affected communities. Cost and efficiency of the overall cleanup process are also important. When remedies involve leaving contamination in place, EPA will continue



GOAL 4:





# Healthy Communities *and* Ecosystems

*Protect, sustain, or restore the health of people, communities, and ecosystems using integrated and comprehensive approaches and partnerships.*



# GOAL 4: Healthy Communities and Ecosystems

Communities and ecosystems are extremely complex systems of enormous variety. To protect and sustain them, EPA is working to manage environmental risks—from risks presented by the pesticides and chemicals on which we depend, to threats to our watersheds, to hazards posed by pollutants entering our homes, schools, workplaces, and neighborhoods. We work to protect critical ecosystems, such as wetlands and estuaries, and collaborate with states and others on “place-based” efforts to protect resources such as the Great Lakes, Chesapeake Bay, and Gulf of Mexico. We direct our risk-management efforts toward the greatest threats in our communities and the most sensitive populations, including children, the elderly, Native Americans, and residents of areas that may be disproportionately exposed to environmental hazards.

Our strategy for reducing risk calls first for preventing pollution at its source. When programs to prevent pollution are not viable, however, we strive to minimize the waste generated, avoid harming habitat, ensure that wastes are disposed of safely, and remediate contamination that does occur.

Key to protecting the health of people, communities, and ecosystems is identifying, assessing, and reducing the risks presented by the thousands of chemicals on which our society and economy have come to depend. We ensure that chemicals and pesticides entering the market meet health and safety standards and register them for use. And we continue to review chemicals already in commerce to reduce potential risk.

Many of EPA’s programs to achieve and sustain healthy communities and ecosystems are designed to bring tools, resources, and approaches to bear at the local level. We build community capacity by providing information to understand risk and to evaluate the effects of development on health and the environment. We encourage redevelopment by providing funds to inventory, assess, and clean

up the hundreds of thousands of properties that lie abandoned or unused due to previous pollution. Ensuring that homes have access to clean, safe drinking water and basic sanitation is a high priority, and we are assisting communities in addressing local pollution and infrastructure challenges. These local and regional initiatives often rely on collaboration among federal, state, tribal, and

## OBJECTIVES

Objective 4.1: Chemical and Pesticide Risks . . . . .	83
Objective 4.2: Communities . . . . .	91
Objective 4.3: Restore and Protect Critical Ecosystems . . . . .	97
Objective 4.4: Enhance Science and Research . . . . .	109

We are also focusing research on increasing the accuracy, precision, and effectiveness of continuous emission monitors. These results will help us evaluate the effectiveness of the new Clean Air Mercury Rule. We are coordinating this research across several of EPA's programs and internationally, for example, through the United Nations Environment Program Fate and Transport Partnership.

Another high priority for the Mercury Program will be providing information to states and utilities on alternative control technologies. Researchers are also working to identify mercury deposition "hot spots" that already exist or may occur as a result of market trading of mercury emissions.



### HOMELAND SECURITY RESEARCH

Threat and consequence assessment research focuses on rapid evaluation of chemical, biological, and radiological risks associated with a terrorist threat or attack. This research will enable better emergency and fol-

low-up responses by developing products for locating, collecting, and analyzing samples; protecting emergency responders, the public, and the environment; decontaminating buildings; and disposing of contaminated materials. EPA researchers will be developing and refining advisory levels for various contaminants of concern, improving risk assessment methods and communication tools, and supporting emergency and follow-up responders.

Our water infrastructure protection research will continue to focus on treatment operations; drinking water distribution systems; and, to a lesser degree, wastewater collection, treatment operations, and treated

water discharge. This work involves laboratory and field testing and evaluating technologies to detect, contain, treat, and recover from intentional attacks on drinking water and wastewater facilities.

Decontamination and consequence management research will support rapid and cost-effective remediation and restoration of buildings and broad outdoor areas. This research involves laboratory and field testing and evaluation of technologies to decontaminate and dispose of materials and areas affected by intentional attacks.

We will provide the results of our homeland security research to the emergency and remedial response community, elected and appointed officials, and the general public.

### SAFE PESTICIDES AND PRODUCTS RESEARCH

By developing and applying the latest molecular and computational approaches, EPA's Safe Pesticides/Safe Products (SP2) Research Program will provide new tools for interpreting exposure, hazard identification, and dose-response information, strengthening our ability to develop risk assessment methods to protect birds, fish, and other wildlife. This research has become increasingly linked to advances in computational toxicology. Scientific progress in sequencing the human genome has rapidly led to laboratory methods for assessing gene expression on a genome-wide basis, which will contribute to the tools available for SP2 research.

EPA researchers will be developing methods for extrapolation among wildlife species and exposure scenarios of concern (e.g., exposure of endangered species) to advance the scientific foundation for conducting probabilistic risk assessments for wildlife populations. SP2 research will also contribute to evaluating potential ecological effects of biotechnology products, developing risk management approaches, and developing methods for assessing the potential allergenicity of genetically engineered plants.





# U.S. Environmental Protection Agency **Homeland Security Strategy**



October 2004





UNITED STATES ENVIRONMENTAL PROTECTION AGENCY  
WASHINGTON, D.C. 20460

OCT 5 2004

THE ADMINISTRATOR

The U.S. Environmental Protection Agency's 2004 *Homeland Security Strategy* will guide the Agency's homeland security efforts over the next two years. It describes our goals, initiatives, and key activities for protecting our country from the consequences of terrorist attacks.

Many of the homeland security challenges that we face transcend political boundaries. The *Strategy* explains how we will transcend these boundaries to network and collaborate with our federal, state, local, and tribal government partners and the private sector to achieve our goals.

The Agency's initial *Strategy*, which was undertaken immediately following the September 11, 2001, disasters, represented EPA's vision for, prevention of, preparation for, and response to another catastrophic terrorist attack. The 2004 *Strategy* takes this initial effort one step further by addressing the Agency's available resources, recent Presidential Directives and expectations, and the evolving role of the Department of Homeland Security.

EPA continues to evaluate its roles and responsibilities and to apply lessons learned. The challenges ahead are far different from those that existed prior to September 11, 2001, and they continue to evolve. We will update the *Strategy* in the future to redirect our activities as needed.

The 2004 *Strategy* is the result of successful team work and collaboration by all EPA program and regional offices. I extend my thanks for everyone's efforts and look forward to continuing to work closely with our partners and stakeholders as we implement our enhanced homeland security initiatives.

A handwritten signature in black ink, appearing to read "Michael O. Leavitt".

Michael O. Leavitt



## Table of Contents

How to Use This Document .....	i
Acknowledgments .....	iii
List of Acronyms .....	v
Executive Summary .....	ix
EPA’s Strategic Objectives in Homeland Security .....	1
I. Critical Infrastructure Protection .....	1
<i>Objective 1</i> .....	1
<i>Objective 2</i> .....	7
<i>Objective 3</i> .....	8
<i>Objective 4</i> .....	10
<i>Objective 5</i> .....	11
<i>Objective 6</i> .....	14
<i>Objective 7</i> .....	19
II. Preparedness, Response, and Recovery .....	21
<i>Objective 1</i> .....	21
<i>Objective 2</i> .....	27
<i>Objective 3</i> .....	28
<i>Objective 4</i> .....	29
III. Communication and Information .....	33
<i>Objective 1</i> .....	33
<i>Objective 2</i> .....	34
<i>Objective 3</i> .....	36
<i>Objective 4</i> .....	37
IV. Protection of EPA Personnel and Infrastructure .....	39
<i>Objective 1</i> .....	39
<i>Objective 2</i> .....	40
<i>Objective 3</i> .....	41
<i>Objective 4</i> .....	42
V. Evaluation .....	45
<i>Objective 1</i> .....	45



## How to Use This Document

This document is a strategy that identifies EPA's intended objectives, tactics, and planned activities to support the nation's homeland security objectives and EPA's homeland security responsibilities through FY2005. While the document uses terms such as "will," the document is not binding on EPA and is not intended to direct or bind other parties. This document is not intended to, and does not create any right, benefit, or trust responsibility, substantive or procedural, enforceable at law or equity by any person or party against EPA or any other person.



## Acknowledgments

This update of the EPA Homeland Security Strategy was accomplished through the successful teamwork and collaboration by the Agency's program and regional offices and the Administrator's Office. Each program and regional office assessed its homeland security responsibilities, activities, and resources; summarized their status; and provided the updated information to the Administrator's Office of Homeland Security (OHS). OHS synthesized the information into this updated strategy. The following individuals were instrumental to the successful completion of this update:

### Office of Homeland Security

Mary Kruger  
Jonathan Edwards  
Rosemary Workman  
Cayce Parrish  
Laura Flynn  
Valarie Bynum  
Constance Gillam  
Caroline Perez

### Office of Solid Waste and Emergency Response

Kathy Jones

### Office of Water

David Travers  
Joan Harrigan-Farrelly

### Office of Research and Development

Christopher Zarba

### Office of Prevention, Pesticides, and Toxic Substances

Linda Strauss

### Office of Enforcement and Compliance Assurance

Brian Maas  
Dan Drazan  
Ted Stanich  
Stacey Noem

### Office of Air and Radiation

Colby Stanton  
Barnes Johnson

### Office of Environmental Information

Don Flattery  
Charles Cavanaugh

### Office of the Inspector General

Michael Speedling

### Office of Administration and Resource Management

Wesley Carpenter  
Dennis Bushta  
Richard Bashar

Region 1

Matthew Schweisberg

Region 2

Kathy Callahan

Eric Mosher

Region 3

Martin Powel

Region 4

Stan Meiburg

Linda Barrett

Region 5

Richard Karl

Thomas Geishecker

Region 6

Mary Kemp

Ragan Broyles

Region 7

Robert Jackson

Janice Kroone

Region 8

Max Dodson

Jim Knoy

Region 9

Daniel Meer

Region 10

Peter Rubenstein

## List of Acronyms

ACC	American Chemistry Council
AMWA	Association of Metropolitan Water Agencies
API	American Petroleum Institute
ATSDR	Agency for Toxic Substances and Disease Registry
ATTF	Anti-Terrorism Task Force
CAA	Clean Air Act
CBI	Confidential Business Information
CBP	U.S. Customs and Border Protection (DHS)
CBR	Chemical, Biological, and Radiological
CCPS	Center for Chemical Process Safety
CCT	Command Center Team
CCU	Computer Crimes Unit
CDC	Centers for Disease Control and Prevention
CDRG	Catastrophic Disaster Response Group
CDX	Central Data Exchange
CID	Criminal Investigation Division (EPA)
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
COOP	Continuity of Operations
CSEE	Center for Strategic Environmental Enforcement
CSIRT	Computer Security Incident Response Team
CTRRT	Counter-Terrorism Response Team
CWA	Clean Water Act
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
DTRA	DOD Threat Reduction Agency
ECOT	Emergency Communication Outreach Team
ECT	Electronic Crimes Team
EOC	Emergency Operations Center
EPA	Environmental Protection Agency
ERAMS	Environmental Radiation Ambient Monitoring System
ERG	Emergency Response Guidebook
ERT	Emergency Response Team
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FedCIRC	Federal Computer Incident Response Center
FEMA	Federal Emergency Management Agency

FERN	Food Emergency Response Network
FIFRA	Federal Insecticide, Fungicide, and Rodenticide Act
FRERP	Federal Radiological Emergency Response Plan
FRPCC	Federal Radiological Preparedness Coordinating Committee
GSA	General Services Administration
HHS	Department of Health and Human Services
HSC	Homeland Security Council
HSOC	Homeland Security Operations Center
HSPD	Homeland Security Presidential Directive
HQ	Headquarters
ICE	U.S. Immigration and Customs Enforcement (DHS)
IIMG	Interagency Incident Management Group
IMAT	Incident Management Assistance Team
IMT	Incident Management Team
INTERPOL	International Criminal Police Organization
IRIS	Integrated Risk Information System
IRT	Incident Response Team
ISAC	Information Sharing Analysis Center
ISC	Interagency Security Committee
JTTF	Joint Terrorism Task Force
LEPC	Local Emergency Planning Committee
LFA	Lead Federal Agency
LRN	Laboratory Response Network
MCA	Mission Critical Area
MOU	Memorandum of Understanding
NAREL	National Air and Radiation Environmental Laboratory
NCC	National Computing Center
NCERT	National Counter-Terrorism Evidence Response Team
NCFL	National Computer Forensics Laboratory
NCP	National Contingency Plan
NEIC	National Enforcement Investigations Center
NFPA	National Fire Protection Association
NHSRC	National Homeland Security Research Center
NICT	National Incident Coordination Team
NIH	National Institutes of Health
NIOSH	National Institute for Occupational Safety and Health
NIPC	National Infrastructure Protection Center
NRT	National Response Team
NSC	National Security Council
NSI	Nationally Significant Incident
NSPD	National Security Presidential Directive
NSSE	National Special Security Event

OAR	Office of Air and Radiation
OARM	Office of Administration and Resources Management
OCA	Off-Site Consequence Analysis
OCEFT	Office of Criminal Enforcement, Forensics and Training
OCEMR	Office of Communications, Education, and Media Relations
OECA	Office of Enforcement and Compliance Assistance
OEI	Office of Environmental Information
OEP	Occupant Emergency Plans
OHS	Office of Homeland Security
OIG	Office of the Inspector General
OIRA	Office of Information and Regulatory Affairs
OPA	Oil Pollution Act
ORIA	Office of Radiation and Indoor Air
OSC	On-Scene Coordinator
OSHA	Occupational Safety and Health Administration
OSWER	Office of Solid Waste and Emergency Response
PAG	Protective Action Guide
PDA	Personal Digital Assistant
PDD	Presidential Decision Directive
PFO	Principal Federal Official
PREP	Preparedness for Emergency Response Exercise Program
PSD	Personal Security Detachment
RCRA	Resource Conservation and Recovery Act
RERT	Radiological Emergency Response Team
RMP	Risk Management Plan
RRLs	Rapid Response Laboratories
SARA	Superfund Amendments and Reauthorization Act
SBA	Small Business Administration
SCADA	Supervisory Control and Data Acquisition
SCIF	Sensitive, Compartmented, Information Facility
SDWA	Safe Drinking Water Act
SERC	State Emergency Response Commission
SIOC	Strategic Information and Operations Center
SIRT	Security Incident Response Team
STE	Secure Terminal Equipment
STU	Secure Telephone Unit
SWGFACT	Scientific Working Group on Forensic Analysis of Chemical Terrorism
TSCA	Toxic Substances Control Act
USAMIRIID	U.S. Army Medical Research Institute for Infectious Diseases
USAO	U.S. Attorneys' Office
USCG	U.S. Coast Guard

USDA	U.S. Department of Agriculture
USMS	U.S. Marshals Service
USNCB	U.S. National Central Bureaus
USPHS	U.S. Public Health Service
USSS	U.S. Secret Service
VAM	Vulnerability Assessment Methodology
VPN	Virtual Private Network
WaterISAC	Water Information Sharing Analysis Center
WITS	Web Interface for Telescience

## **Executive Summary**

### **Introduction**

For over 30 years the U.S. Environmental Protection Agency (EPA) and its partners have made great progress toward a cleaner, healthier environment for the American people. Following the terrorist events of September 11, 2001, and thereafter, EPA's mission expanded beyond safeguarding the natural environment – the air, water, and land – from traditional sources of pollution. With the Nation under a continuing threat from those who seek to harm it, EPA also has the important responsibility of protecting the environment from terrorist acts.

In September 2002, EPA published a *Strategic Plan for Homeland Security (2002 Plan)*. The 2002 *Plan* reflected the deliberations of the Agency's senior leadership regarding the scope of activities that would appropriately support enhanced and challenging homeland security responsibilities. The 2004 *Homeland Security Strategy (2004 Strategy)* furthers the Agency's strategic planning process and updates the earlier plan. Specifically, the 2004 *Strategy* updates the Agency's objectives and planned activities by taking into consideration available resources through Fiscal Year (FY) 2005. It also preliminarily addresses recently issued Presidential Directives and other stakeholder expectations, as well as the evolving role of the Department of Homeland Security (DHS) in homeland security policies and activities that relate to EPA's mission and expertise. Finally, the 2004 *Strategy* catalogues those activities that have been completed since 2002.

### **Resources**

The 2002 *Plan* was purposely written with the assumption of no budgetary constraints. In developing the 2004 *Strategy*, the Agency balanced EPA's known and projected funding and resources through FY2005 against the desired homeland security objectives and key activities. The 2004 *Strategy* reflects the resource levels presented in the FY2004 and FY2005 President's budget and will help to prioritize objectives, activities and resource usage.

### **Presidential Directives and Expectations**

Shortly following the terrorist attacks of September 11, 2001, the White House began issuing Homeland Security Presidential Directives (HSPDs), which task federal departments and agencies with specific responsibilities and communicate presidential decisions concerning national homeland security policy. The White House also issued the *National Strategy for Homeland Security* in July 2002, the purpose of which was to organize the federal, state, and local governments, as well as the private sector and the American people to secure and protect the country from terrorist attacks. The HSPDs, along with National Security Presidential Directives (NSPDs), the *National Strategy for Homeland Security*, and specific homeland security related statutes, provide the foundation for the homeland security activities undertaken

by the federal government. The White House also provides direction and guidance to federal agencies through the Homeland Security Council (HSC) and specific Policy Coordinating Committees.

Where possible, the 2004 *Strategy* addresses EPA's responsibilities as described in the HSPDs, NSPDs, the *National Strategy for Homeland Security*, and related homeland security statutes. However, since several of the HSPDs were issued after the Agency developed its FY2004 and 2005 budget, the *Strategy* does not yet specifically address all taskings included in those HSPDs. Taskings that are not fully addressed in the 2004 *Strategy* will be prioritized and addressed in subsequent iterations. Relevant HSPDs include:

- HSPD 5 *Management of Domestic Incidents*
- HSPD 7 *Critical Infrastructure Identification, Prioritization and Protection*
- HSPD 8 *National Preparedness*
- HSPD 9 *Defense of United States Agriculture and Food*
- HSPD 10 *National Policy for Biodefense*

### **Evolving Roles and Responsibilities**

The Department of Homeland Security was established in early 2003 to lead a unified national effort to secure America. The 2004 *Strategy* reflects DHS's new leadership role in coordinating homeland security activities across the government. As the new Department's roles and responsibilities continue to evolve, it will likely further influence EPA's homeland security strategic planning process.

### **Unforeseen Threats**

As new threats to the Nation continue to evolve, so must the required preparedness and response by the United States. It is critical to note that although EPA has strived to anticipate the activities that the Agency must carry out in order to safeguard human health and the environment from terrorist attacks, new and unforeseen threats may arise that are not specifically addressed by the 2004 *Strategy*.

### **Relationship to EPA's 2003-2008 Strategic Plan**

The 2003- 2008 *EPA Strategic Plan* establishes five long-term Goals and seven Cross-Goal Strategies for the Agency. The Cross-Goal Strategies encompass all Agency programs and environmental media and contribute toward the achievement of all five *Strategic Plan* Goals. Homeland Security is included as a Cross-Goal Strategy. The 2004 *Homeland Security Strategy* identifies the Agency's homeland security objectives and planned activities, each of which supports one or more of the five Goals identified in the *EPA Strategic Plan*.

## Organization

The 2004 *Strategy* is organized and formatted in the same manner as the 2002 *Plan*. Each of the four Mission Critical Areas (MCAs) has been retained, as well as the goals (now termed objectives), results, tactical action initiatives (tactics) and key activities (subtactics) structure. The MCAs build upon the Critical Mission Areas identified in the *National Strategy for Homeland Security*, but are focused on activities and strategic challenges specific to EPA. The 2004 *Strategy* includes one new Mission Critical Area, Evaluation, through which EPA will assess the Agency's homeland security progress to ensure an effective and efficient use of resources. Projected completion dates are included for most tactics and subtactics. Items that have been completed since the release of the 2002 *Plan* are labeled accordingly.

Below is a brief description of each of the five Mission Critical Areas.

### Critical Infrastructure Protection

EPA has unique programmatic responsibilities and expertise related to the water and wastewater industries and has been designated as the lead federal agency for coordinating the protection of critical infrastructure for the water sector. EPA is committed to assessing and reducing vulnerabilities and strengthening detection and response capabilities in this area. In addition, EPA will contribute to similar efforts led by other federal agencies addressing sectors such as the chemical, food, transportation, and energy sectors. EPA also will provide environmental expertise to support federal law enforcement activities. Further, EPA is working to improve compliance monitoring and surveillance of imports of dangerous chemicals, waste and materials at more than 300 ports of entry across the country.

### Preparedness, Response, and Recovery

Under the *National Strategy for Homeland Security* and various federal response plans, EPA has specific response and recovery responsibilities. EPA emergency responders play a vital role in the federal response to any chemical, biological, radiological, or nuclear terrorist events. EPA will continue to focus on strengthening its response capabilities, clarifying roles and responsibilities to ensure an effective response, and promoting improved response capabilities across government and industry in the areas in which the Agency has unique knowledge and expertise.

### Communication and Information

Comprehensive, accurate, well-organized, and timely information is critical to sound decision-making. EPA possesses unique capabilities to collect, synthesize, interpret, manage, and disseminate complex information related to human health and the environment. Effectively

managing and sharing this information within the Agency and with EPA's partners at all levels of government and industry will contribute to the Nation's homeland security capabilities.

### Protection of EPA Personnel and Infrastructure

The security and protection of personnel and infrastructure are critical to ensuring EPA's ability to respond to terrorist incidents as well as continue to fulfill the Agency's mission. In recognition of this, EPA has undertaken steps to safeguard and protect employees, ensure the continuity of operations, and protect Agency facilities nationwide.

### Evaluation

Internal evaluations of Agency activities are important for identifying areas needing improvement to promote efficient use of EPA's resources. EPA will conduct internal studies and evaluations of its homeland security activities and determine if the Agency is achieving the desired objectives described in the 2004 *Strategy*.

### **Accomplishments**

The Agency has accomplished a great deal in the area of homeland security as is reflected by the completions noted in the 2004 *Strategy*. Below is a brief listing by Mission Critical Area of some of the key accomplishments.

### Critical Infrastructure Protection

- Developed and implemented a water sector vulnerability assessment process and issued \$140 million in water security grants
- Developed water sector Response Protocol Toolbox and initiated security training
- In collaboration with DHS and HHS, deployed and activated BioWatch
- Established National Counter-Terrorism Evidence Response Teams
- Established a National Homeland Security Research Center
- Signed a Memorandum of Understanding with the U.S. Customs and Border Protection to ensure seamless information sharing of environmental compliance and enforcement data

### Preparedness, Response, and Recovery

- Developed an EPA National Approach to Response, which directs EPA coordination in the event of multiple terrorist incidents occurring, and assisted in the development of the National Incident Management System
- Initiated environmental laboratory response capacities and capabilities assessment
- Continued to broaden expertise on pesticide and industrial chemicals

- Continued to develop new technologies for sampling and analysis, decontamination, and risk assessment

#### Communication and Information

- Developed draft criteria and guidance for sensitive information
- Developed both internal and external incident communications protocols
- Established a Center for Strategic Environmental Enforcement
- Instituted new technologies for enhancing communications during incidents

#### Protection of EPA Personnel and Infrastructure

- Updated Occupational Emergency Plans
- Established minimum regional COOP requirements
- Upgraded EPA's Emergency Operations Center
- Completed physical security vulnerability assessments for EPA Security Level 4 and 3 facilities

#### **Next Steps**

#### Future Updates

Future updates of EPA's *Homeland Security Strategy* are likely as the nation's security needs continue to evolve in a dynamic threat environment, as changes occur in Administration priorities, and as EPA conducts the budgetary planning process for FY2006 and beyond.

#### Implementation Tracking System

In addition to listing the homeland security activities planned for 2004 and 2005, the *Strategy* also accounts for the activities that have been completed since 2002. The presentation of completed items, however, is limited in scope and function. For example, it does not have the functional capability to allow users to sort the information electronically and generate desired reports. As a result, the Administrator's Office of Homeland Security is exploring the development of an implementation tracking database of the objectives, tactics, and key activities presented in the 2004 *Strategy*.

## Exhibit 1: EPA's Homeland Security Objectives

### ***Critical Infrastructure Protection Objectives***

1. EPA will work with the states, tribes, drinking water and wastewater utilities (water utilities), and other partners to enhance the security of water and wastewater utilities and the ability to respond effectively to security threats and breaches.
2. As requested, EPA will support the Department of Homeland Security (DHS) and other federal agencies in implementing the responsibilities and functions assigned by Homeland Security Presidential Directives (HSPDs) and National Security Presidential Directives (NSPDs) on matters related to EPA's mission and critical infrastructure.
3. EPA will work with other federal agencies, the building industry, and other partners to help reduce the vulnerability of indoor environments in buildings to chemical, biological, and radiological (CBR) incidents.
4. EPA will help to ensure that critical environmental threat monitoring information and technologies are available to the private sector, federal counterparts, and state and local government to assist in threat detection.
5. EPA will be an active participant in national security and homeland security efforts pertaining to food, transportation, and energy.
6. EPA will manage its federal, civil, and criminal enforcement programs to meet its homeland security, counter-terrorism, and anti-terrorism responsibilities under the *National Strategy for Homeland Security*, *Homeland Security Act of 2002*, Presidential Executive Orders, Homeland Security Presidential Decision Directives (HSPDs), and environmental civil and criminal statutes in accordance with the National Response Plan and the EPA National Approach to Response.
7. EPA will identify the Agency's critical infrastructures, assess their vulnerabilities, and take appropriate mitigation under PDD 63, HSPD 7, and the Project Matrix methodology.

### ***Preparedness, Response, and Recovery Objectives***

1. Consistent with HSPD 8, EPA will be prepared to respond to and recover from a major terrorist incident anywhere in the country. To do this, the Agency will maintain trained personnel and effective communications, ensure practiced coordination and decision-making, and provide the best technical tools and technologies to address threats.
2. EPA will assist in the development of a comprehensive National Response Plan for management of all domestic incidents.
3. In accordance with HSPDs 5 and 8, EPA will support and develop the preparedness of state, local, and tribal governments and private industry to respond to, recover from, and continue operations after a terrorist attack.
4. EPA will contribute its unique perspective to advance the state of the knowledge in the areas relevant to homeland security to provide responders and decision-makers with tools and the scientific and technical understanding they need to manage existing or potential threats to homeland security.

### ***Communication and Information Objectives***

1. EPA will use best available environmental information from internal and external sources to ensure informed decision-making and appropriate response.
2. EPA will effectively disseminate timely, quality environmental information to all levels of government, industry, and the public, allowing them to make informed decisions about human health and the environment.
3. EPA will classify, declassify, safeguard, manage, and destroy all national security information in accordance with Executive Order 12958, as amended by Executive Order 13292; and exchange information with other federal, state, and local assets to prevent, deter, and respond to terrorist threats or attacks; and improve and streamline personnel security services to ensure employees are granted and maintain active security clearances in a timely manner.
4. EPA will continuously and reliably communicate with employees and managers.

***Protection of EPA Personnel and Infrastructure Objectives***

1. EPA will safeguard its employees.
2. EPA will ensure the continuation of the Agency's essential functions and operations.
3. EPA will maintain a secure technology infrastructure capable of supporting lab data transport and analysis functions, 24x7 telecommunications to all EPA locations, and management of critical data and information.
4. EPA will ensure that the Agency's physical structures and assets are secure and operational.

***Evaluation Objective***

1. EPA will add to knowledge, verification, or action contributing to reduction or elimination of infrastructure and other security risks or challenges.



## EPA's Strategic Objectives in Homeland Security

### I. Critical Infrastructure Protection

#### *Strategic Objectives, Tactical Action Initiatives, and Benchmarks*

Defending the nation's critical infrastructure is essential to protecting the public in the event of a terrorist attack on the United States. The *National Strategy for Homeland Security* and the Homeland Security Presidential Directive (HSPD) 7, *Critical Infrastructure Identification, Prioritization and Protection*, designate EPA as the lead federal agency for protecting the nation's water sector critical infrastructure. Also, HSPD 9, *Defense of United States Agriculture and Food*, directs EPA to develop a comprehensive, nationwide biosurveillance program for water and a laboratory network to support such a program.

EPA's strategic objectives for critical infrastructure protection reflect the Agency's role in safeguarding public health and safety by supporting improved security measures for the water sector. Specifically, EPA will provide support to drinking water and wastewater utilities by placing an emphasis on preparedness and prevention, and by assisting those responsible for assessing and reducing vulnerabilities and maximizing response capabilities. In addition, EPA will continue to develop guidance, training, tools, and technologies to improve key responders' abilities to support the nation's water sector critical infrastructure.

EPA also provides support in other areas of the nation's critical infrastructure for which the Agency has experience and capabilities. As requested, EPA will provide technical expertise to other governmental agencies and the private sector to prevent, reduce, mitigate, and recover from terrorist attacks on sectors such as the chemical, food, transportation, and energy resource sectors. In addition, EPA will manage its federal, civil, and criminal enforcement capabilities to respond to any terrorist threats and actions that violate the nation's environmental laws. EPA will also protect its own critical infrastructures in accordance with PDD 63, HSPD 7, and the Project Matrix Methodology.

**OBJECTIVE 1 ⇒ EPA will work with the states, tribes, drinking water and wastewater utilities (water utilities), and other partners to enhance the security of water and wastewater utilities and the ability to respond effectively to security threats and breaches.**

Under both the Safe Drinking Water Act (SDWA) and the Clean Water Act (CWA), EPA works closely with other government agencies, and water utilities to ensure clean and safe water. Under the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002*, community

water systems that serve more than 3,300 people are required to undertake vulnerability assessments by June 30, 2004 and revise or develop emergency response plans six months later.<sup>1</sup>

As the federal lead for the water sector, EPA will build on its long established relationships with drinking water and wastewater utilities, water-related government entities, and associations to ensure that the water sector has the technical tools and support necessary to address security needs. EPA, in coordination with key partners and through lessons learned from security efforts already underway, will continue to identify security concerns that present the greatest risks to the water sector and to ensure that the water sector and others that support or rely on the sector understand security threats and vulnerabilities as well as the measures that can be adopted to reduce risk.

### **TACTICS**

**1.1 EPA, working with the water sector, will develop measurable goals for critical water infrastructure protection efforts, will utilize available sources of information to analyze water sector security activities against appropriate measures, and will revise approaches and actions, as necessary.**

### **RESULTS**

By the end of FY2005, the water sector will have in place key indicators to clearly measure water security results and achievements.

#### **1.1.1 Indicator Development and Implementation**

- Work with the water sector to develop measures that are consistent with the Agency's overall Strategic Plan as well as its specific Homeland Security Strategy.
- Work with the water sector to enlist the participation and involvement of principals (e.g., states, localities, water utilities) and ensure their commitment to the indicators that measure the water sector's security results and achievements.
- Work with water sector partners to develop standards for incorporating security measures in drinking water and wastewater facility design and construction. (FY2005)

**1.2 EPA will continue to provide assistance on security-related issues to the water sector and others who support or rely on the sector, and ensure that such assistance reflects the most up-to-date information.**

### **RESULTS**

*By the end of FY2005, drinking water and wastewater utilities across the country will have the tools and training to improve preparedness and emergency response plans, and access timely threat analysis information (e.g., WaterISAC). Related sectors, such as law enforcement, emergency response, public health officials, medical practitioners,*

---

<sup>1</sup>The respective statutory deadlines for the submission of vulnerability assessments are as follows: (1) systems serving more than 100,000 people, March 31, 2003; (2) systems serving between 50,000 and 100,000 people, December 31, 2003; (3) systems serving between 3,300 and 50,000 people, June 30, 2004.

*environmental laboratories, and other governmental entities, will have improved tools and associated training to better support the water sector.*

### 1.2.1 Tools and Guidance

- Develop guidance and tools on how to conduct vulnerability assessments, prepare emergency response plans, and address threats from terrorist attacks or other intentional actions. In FY2002, work with partners to develop and distribute initial outreach materials, guidance, and tools for all drinking water systems and all wastewater utilities. Completed.
- Complete and disseminate guidance for drinking water systems serving less than 3,300 persons. (FY2004)
- Enhance existing security enhancement guidance by adding information on security enhancement product categories. (FY2004)
- Initiate deployment of the Water Contaminant Information Tool to provide easy access to key information on priority contaminants, and develop components of the Tool including data on treatability and toxicity levels. Revise periodically as new information becomes available. (FY2004)
- Develop and disseminate a compendium of environmental laboratory capability to analyze water samples, and identify mechanisms for enhancing laboratories' emergency response capacity. Revise periodically as new information becomes available. (FY2005)
- Consult with appropriate departments and agencies of the federal government and provide baseline information on the kinds and potential impacts of terrorist attacks or other intentional actions that are probable threats to community water systems and wastewater utilities. Completed.
- In FY2003, provide information to states, tribes, utilities, and associations on effectiveness of security improvements to reduce risk and address threats. Completed.

### 1.2.2 Training

- Provide training and technical assistance to water utilities on threats, initial security measures, vulnerability assessments, emergency response plans, and other related security issues. Include training to build expertise in states and other appropriate organizations sufficient to provide technical assistance to utilities. Begin in FY2002, and continue training in subsequent fiscal years. Provide financial assistance to states to support training and technical assistance for small and medium drinking water systems. Otherwise, support training directly. Completed.
- Provide training and technical assistance to drinking water and wastewater utilities on preparing and updating vulnerability assessments, adopting security measures, and preparing/revising emergency response plans. Focus training on technical, financial, and managerial capacity building. Include training to build expertise in states and other appropriate organizations sufficient to provide technical assistance to utilities.

- Working with the appropriate agencies, EPA programs, and stakeholders, support simulations and emergency response exercises in FY2004 and subsequent years.
- Provide training on the Response Protocol Toolbox (see Tactic 1.3, Protocols) for water utilities and other emergency responders. (FY2005)
- Establish official relationship with national level law enforcement organizations to provide cross training with water sector. (FY2005)
- Support the Physician On-Line Reference Guide to Recognizing Waterborne Diseases and the Health Effects of Water Pollution. (FY2004)
- Do performance evaluations with environmental laboratories. Develop and provide training on analytical methods as new information becomes available. (FY2005)
- Conduct a risk communication workshop for water utilities, public health officials, laboratories, and other relevant stakeholders to share experiences on crisis management and develop educational materials. (FY2004)

#### **1.2.3 Financial Assistance to Systems, States, and Tribes**

- In FY2002, provide \$53 million in financial assistance to support approximately 400 large drinking water system vulnerability assessments, and/or designs for security upgrades and/or emergency response plans. Completed.
- Provide guidance on ways to finance security enhancements through training on financing options. (FY2005)
- Develop public/private partnership with business community to provide low-cost security enhancements to drinking water systems. (FY2004)
- Provide financial support to states and tribes to coordinate with other homeland security activities. (FY2004)

#### **1.2.4 Information Analysis, Sharing and Protection**

- Assist the water sector in maintaining a secure Water Information Sharing and Analysis Center (WaterISAC) to exchange and analyze threat and incident information and to serve as a clearinghouse for sensitive information.
- Ensure coordination with the Department of Homeland Security and other appropriate departments and agencies of the federal government in reviewing and updating threat, response preparedness, and vulnerability information. Use such information to develop bulletins, advisories, and fact sheets to be provided, as appropriate, to water utilities and response agencies using secure technologies, e.g., the WaterISAC.
- Build partnerships with appropriate organizations (including states, local law enforcement, and water utilities) to encourage appropriate citizen action to alert authorities of suspicious activities around water and wastewater infrastructure. (FY2005)
- Disseminate research results and other security related information through conferences and postings on the WaterISAC, as appropriate.
- In accordance with protocol established in 2002, maintain security of vulnerability assessments sent to EPA.

- Implement a vulnerability assessment compliance review process. (FY2004)
- Review available vulnerability assessments to develop aggregate data to guide EPA's assistance, research, and technical support to water systems. (FY2004)
- In FY2003, develop and implement a vulnerability assessment review process and enforcement policy. Completed.
- In FY2003, in consultation with appropriate federal law enforcement and intelligence agencies, develop protocols to store and protect copies of vulnerability assessments submitted by community water systems. Completed.

#### 1.2.5 Embedding Security into "Business as Usual"

- Identify how to integrate water utility security activities into traditional water and wastewater program activities (e.g., operator certification, inspections, treatment optimization, and asset management) and provide appropriate guidance and training. (FY2005)
- Identify the multiple benefits of security enhancements and technologies for water quality improvements. (FY2005)

### 1.3 **EPA will develop tools to better prevent, detect, mitigate, and/or recover from potential physical, cyber, chemical, biological, and radiological attacks to water utilities. EPA will prioritize the development of technical support based on the water sector's top vulnerabilities.**

#### **RESULTS**

*By the end of FY2005, water utilities, key response agencies, and policymakers will have an array of tools to help make timely and effective analytical and technological decisions to enhance security, detect attacks, and respond to/recover from incidents.*

#### 1.3.1 Research/Technology Development Planning and Implementation

- Develop a water utility security research plan in the first quarter of FY2003. The research plan will build on information gathered in the FY2002 interagency assessment of the state of knowledge on drinking water contaminants, the ability to detect them, and the effectiveness of various treatment methods to counteract them. Completed.
- Begin implementation of interim priority research projects in FY2002, review and update the plan on an annual basis, and continue implementation through FY2005.

#### 1.3.2 Technology Development and Testing

- Expand the availability and the use of models to predict/track the fate and transport of contaminants in surface waters and water distribution systems. Improve capability to use models to enhance decision-making on security improvements (e.g., placement of contaminant detection and prevention devices). (FY2005)
- Coordinate with other agencies to develop innovative mobile treatment and pumping units for use during emergency situations. (FY2005)

- Work with water utilities to develop and implement at least three and up to five pilot testing programs in FY2003 to evaluate promising technologies. Completed.

### 1.3.3 Monitoring, Analysis and Surveillance Technologies

- Develop the conceptual framework for creating a nationwide monitoring and surveillance program for water utilities that would provide early warning in the event of a terrorist attack, and implement as resources become available.
- Develop the conceptual framework for a water laboratory alliance that would enhance the nation's ability to monitor and respond to a terrorist attack, and implement as funds become available.
- Update and maintain the on-line National Environmental Methods Index and its associated expert system to include laboratory methods that can be used in analyzing priority contaminants. (FY2004)
- Support the development of methods and sampling kits for the detection and analysis of biological and chemical contaminants in water.
- In collaboration with other agencies, build on the existing disease surveillance network to detect and control disease outbreaks by more effectively linking public health and water system data.
- Develop guidelines for wastewater utilities on the safe and effective analysis, treatment, and disposal of decontaminated waste. (FY2004)
- Disseminate surveillance technologies, analytical methods, and other critical information through mechanisms identified under 1.2.1 (e.g., Security Product Guide) and 1.2.4 (e.g., Water ISAC or the Homeland Security Information Network). (FY2004 and 2005)

### 1.3.4 Protocols

- Finalize the Response Protocol Toolbox, a modular guidance document for drinking water and wastewater utilities, laboratories, and first responders, on how to prepare for, respond to, and recover from water contamination threats. (FY2004)
- Finalize guidance on developing/revising emergency response plans. (FY2004)
- Evaluate cyber security issues as they relate to Supervisory Control and Data Acquisition (SCADA) and other computer-assisted systems for water utilities. (FY2004)
- Assess approaches that can be used to assure continuity of supply. (FY2004)

### 1.3.5 Threat Identification

- Develop, in consultation with appropriate federal agencies and organizations, a baseline threat document for wastewater utilities and revise, as appropriate, the existing drinking water threat document. (FY2004)
- Analyze implications of sector interdependencies and meet with relevant sectors (e.g., the transportation, energy, and telecommunications sectors) and related federal, state, and local agencies to identify collaborative opportunities to reduce risk. (FY2004)

**1.4 EPA will work with stakeholders to identify the research and development needs in the areas of water security and rapid risk assessments to enhance the security of water and wastewater utilities.**

See MCA 2, Objective 4, Tactics 4.3 and 4.4 for tactics and results.

**OBJECTIVE 2 ⇒ As requested, EPA will support the Department of Homeland Security (DHS) and other federal agencies in implementing the responsibilities and functions assigned by Homeland Security Presidential Directives (HSPDs) and National Security Presidential Directives (NSPDs) on matters related to EPA’s mission and critical infrastructure.**

HSPDs and NSPDs task federal departments and agencies, including EPA, with specific homeland security responsibilities either directly, or in support of another department or agency (e.g., DHS).

**TACTICS**

**2.1 As requested and within resource constraints, EPA will support and provide assistance to DHS and other federal departments and agencies in carrying out their critical infrastructure protection activities for recently issued and future HSPDs and NSPDs related to EPA’s mission (e.g., the chemical sector and the food and agriculture sector).**

**RESULTS**

*EPA provides the requested support and assistance to DHS and other federal departments and agencies.*

HSPD 5, *Management of Domestic Incidents*, is intended to enhance the ability of the U.S. to manage domestic incidents by establishing a National Incident Management System (NIMS) and designating the Secretary of the Department of Homeland Security as the Principal Federal Official (PFO) to coordinate federal resources used in response to or recovery from terrorist attacks, major disasters, or other emergencies in specific cases. This directive also assigns specific responsibilities to the Attorney General, Secretary of Defense, Secretary of State, the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs, and directs the heads of all federal departments and agencies to provide their full and prompt cooperation, resources, and support as consistent with their own responsibilities for protecting national security. EPA will be called upon to provide agency-specific expertise and support whether it is a terrorist attack, other intentional criminal act or a natural disaster.

HSPD 7, *Critical Infrastructure Identification, Prioritization, and Protection*, establishes a national policy for federal departments and agencies to identify and prioritize the nation’s critical infrastructure and key resources and protect them against terrorist attacks. DHS is

responsible for coordinating the overall national effort. DHS is also responsible for coordinating protection activities for specific critical infrastructure sectors, such as the chemical sector. Given EPA's expertise and statutory responsibilities related to the chemical sector, DHS may request assistance from EPA as it implements the tasks specified in HSPD 7.

HSPD 9, *Defense of United States Agriculture and Food*, establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies. HSPD 9 includes responsibilities for which EPA is directed to work in cooperation with other federal departments and agencies, such as the Department of Agriculture and Health and Human Services.

HSPD 10 (also NSPD 33), *National Policy for BioDefense*, establishes a national policy to prevent, protect against, and mitigate biological weapons attacks. HSPD 10 directs EPA to work in coordination with the Attorney General and the Departments of Defense, Agriculture, Labor, Health and Human Services, and Homeland Security to develop specific standards, protocols, and capabilities to address the risks of contamination following a biological weapons attack and to develop strategies, guidelines, and plans for decontamination of persons, equipment, and facilities. (Unclassified Text)

**2.1.1** Under HSPD 5, provide staffing to the Department of Homeland Security (DHS) national Homeland Security Operations Center (HSOC) and the Interagency Incident Management Group (IIMG) as called for in the Initial National Response Plan, dated September 30, 2003, to serve as agency subject matter experts with reach-back capability during heightened alert levels and during surge periods. Completed.

**OBJECTIVE 3 ⇒ EPA will work with other federal agencies, the building industry, and other partners to help reduce the vulnerability of indoor environments in buildings to chemical, biological, and radiological (CBR) incidents.**

EPA will utilize existing statutory responsibilities under the Clean Air Act (CAA) and the Comprehensive Environmental Response, Compensation, and Liability Act, as amended (CERCLA) to support and develop the preparedness of state and local governments and private business and industry to respond to, recover from, and continue operations following a terrorist attack. As outlined in this strategy, EPA will work with other agencies to ensure that building air protection guidance is produced and widely disseminated and that training on such guidance is available. In support of efforts expected to be undertaken by the Department of Homeland Security, EPA will also work with its partners in other federal agencies, academia, industry organizations, and public health organizations to identify and conduct research on needed technologies, as appropriate.

**TACTICS**

- 3.1 EPA will work with other federal agencies to ensure that building protection guidance is produced.** Completed.

**RESULTS**

*Building managers will have the basic tools they need to adequately protect their buildings from the threats of CBR terrorism by FY2003. Target audiences in the building community will have access to more in-depth guidance on topics of concern for protecting their buildings by FY2004.*

- 3.1.1** Work with federal partners on the Office of Homeland Security Building Air Protection Work Group (“the Work Group”) to produce guidance for protecting building environments from airborne chemical, biological, or radiological attacks. Completed.
- 3.1.2** Work with federal partners on the Work Group to produce additional in-depth guidance on specific topics related to protecting building environments from airborne chemical, biological, or radiological attacks. Completed.
- 3.2 EPA will work with federal partners and non-governmental organizations to review utility of any guidance developed and solicit input, through an invitational workshop, to learn of additional areas where federal guidance would be valuable.** Completed.

**RESULTS**

*A workshop of invited private sector participants will be convened in FY2003 to solicit their views on additional areas of in-depth guidance needed to provide adequate building protection.* Completed.

- 3.3 EPA will work with other federal and non-federal agencies to compile a list of existing information resources on building air protection.** Completed.

**RESULTS**

*An inventory of existing federal guidance will be developed by the end of FY2002.* Completed.

- 3.3.1** Work with other federal agencies to prepare an inventory of existing federal guidance on this topic. Completed.
- 3.3.2** Explore the feasibility of inventorying non-federal resources on this topic. Completed.
- 3.4 EPA will work with other federal agencies to determine whether means currently exist to evaluate the efficacy and feasibility of new technologies proposed for use in buildings to protect occupants from possible terrorist threats.**

**RESULTS**

*By the end of FY2003, the Office of Homeland Security Building Protection Work Group will develop a process for assessing new building protection technologies.*

**3.4.1** Through the Work Group and OHS infrastructure, develop a process to identify candidate technologies for review by knowledgeable federal authorities and give feedback to inquiring members of the buildings community.

**3.5 EPA will work with other federal agencies to ascertain whether guidance should be developed for the public on how to protect themselves while in their residences from possible biological, chemical, or radiological attacks. Completed.**

**RESULTS**

*An OHS Building Air Protection Work Group document will be developed in FY2003 that gives guidance on how the public can protect themselves while in their residences. Completed.*

**3.5.1** Through the OHS interagency Work Group, develop residential guidance for the public. Completed.

**3.6 In cooperation with other federal agencies, support the DHS Building Protection Work Group to coordinate research strategies on building air protection.**

**RESULTS**

*Work Group participants will brief the research strategy of their agency to the entire Work Group. Steps leading to a comprehensive federal inventory of research planned or underway will be developed to aid in directing resources to filling critical information gaps.*

**3.7 EPA will work with stakeholders to identify the necessary research and development in the areas of building security and rapid risk assessments to reduce the vulnerability of indoor air environments to chemical, biological and radiological incidents.**

See MCA II, Objective 4, Tactics 4.1 and 4.4 for tactics and results.

**OBJECTIVE 4 ⇒ EPA will help to ensure that critical environmental threat monitoring information and technologies are available to the private sector, federal counterparts, and state and local government to assist in threat detection.**

EPA will work closely with other federal and state agencies with threat detection responsibilities to ensure that EPA's existing monitoring expertise, standards, capabilities, and data are appropriately integrated into their efforts to detect terrorist threats. In addition, air monitoring may provide valuable and timely data to detect anomalies in the ambient air that may indicate if further, more detailed, analysis is warranted.

### **TACTICS**

**4.1 In support of the Department of Homeland Security, EPA will work with the states, tribes, and other federal agencies to develop and implement BioWatch, a system utilizing EPA's air monitoring infrastructure to detect potential biological threats in the ambient air.**

#### **RESULTS**

*By FY2003, EPA's ambient air monitoring data will be fully available to DHS as part of the BioWatch air monitoring system. Assuming funding availability, EPA will begin enhancing its ability to collect ambient air monitoring data on a near real-time basis. The enhancement process may be implemented by the end of FY2008.*

- 4.1.1 Provide support to other federal agencies on their biological detection monitoring.
- 4.1.2 Along with DHS and HHS, deploy BioWatch system in 31 U.S. cities. Completed.
- 4.1.3 Enhance real-time monitoring capabilities, if needed, at selected sites within current monitoring network for reporting indicators threats to the ambient air.
- 4.1.4 EPA will work with its partners regarding the implementation of the system, including the procedures for responding to anomalies when they are detected. (FY2004)

**4.2 EPA will utilize the current monitoring infrastructure to provide filters or historical data to other federal agencies, upon request. Completed.**

#### **RESULTS**

*Beginning in FY2002, EPA will provide particulate filters and historical data to other federal agencies, as requested. Completed.*

- 4.2.1 Provide particulate filters to Sandia National Laboratory for analysis of biological agents. Completed.

**OBJECTIVE 5 ⇒ EPA will be an active participant in national security and homeland security efforts pertaining to food, transportation, and energy.**

While other federal departments and agencies have primary responsibility for these sectors, EPA has relevant authorities and expertise to complement their efforts. The Agency will use the knowledge and experience it has gained in implementing and enforcing the nation's environmental laws (which address pesticides and toxic substances, air and water pollution, drinking water, hazardous waste, and emergency preparedness and response, among other issues) to contribute to the federal government's efforts to secure the nation's food, transportation, and energy infrastructure.

## **TACTICS**

**5.1 EPA is working with the U.S. Immigration and Customs Enforcement (ICE), the U.S. Coast Guard, and state agencies such as the Council of Radiation Control Program Directors (CRCPD) to prevent the importation of unwanted radioactive materials into the United States.**

### **RESULTS**

*Provide assistance to its partners to monitor and prevent entry into U.S. seaports of radioactively contaminated scrap metal. EPA will also collect data on the frequency with which this scrap metal is imported into the U.S., the types of metals and the quantity, source, and intended destination.*

**5.1.1** Work with ICE to develop and refine radiation detection methods in international scrap metal shipments coming into the U.S. as well as developing protocols with other federal agencies, states, private sector concerns, and the public. (FY2004)

**5.1.2** Collect data on the frequency with which radioactively contaminated scrap metal is imported into the United States and the costs associated with management of this problem. (FY2004)

**5.2 EPA will work with U.S. Customs and Border Protection (CBP) to ensure compliance with entry and import permits and to create a seamless information-sharing system that allows for coordinated communication among themselves, and also the broader law enforcement and intelligence gathering community.**

### **RESULTS**

*In FY2003, EPA and CBP will sign a Memorandum of Understanding (MOU) to create a seamless information-sharing system between the two agencies designed to provide real-time access to data necessary for compliance and enforcement decision-making. In FY2003, EPA will also develop an integrated enforcement strategy for imports/exports of toxic and hazardous materials, pesticides, and waste, including a process for referring cases from CBP and ICE to EPA for enforcement. (MOU signed on January 15, 2003.)*

**5.2.1** Improve EPA data infrastructure and intelligence gathering capabilities and links to ICE and other law enforcement databases.

- 5.2.2 EPA will work with CBP to increase compliance monitoring and civil/criminal enforcement of environmental laws at the border.
- 5.2.3 Improve EPA information sharing with the FBI, DHS, and other law enforcement agencies, as well as the intelligence community, in cases involving threats or suspected acts of terrorism or other intentional criminal acts under the environmental statutes or threats/acts against critical infrastructure protected by EPA. Completed.

**5.3 EPA will work with the other federal departments/agencies, state and local governments, and the private sector to help protect the nation's food supply from biological and chemical contamination due to acts of terrorism.**

**RESULTS**

*In FY2004 and FY2005, EPA will continue to participate in interagency workgroups established to protect the nation's food supply from biological, chemical, and radiological contamination. EPA has the statutory authorities to license pesticides in/on food and products used to inactivate biowarfare agents or novel pathogens on inanimate surfaces and EPA has the responsibility to ensure safe drinking water. Under HSPD 9 (Defense of United States Agriculture and Food), DHS, USDA, and HHS must coordinate with EPA to develop strategies for mitigating and responding to major crop/livestock diseases and pests, for decontaminating premises, and for ensuring safe drinking water (for drinking water activities, see Mission Critical Area I, Objective 1, Tactic 1.3 and Mission Critical Area II, Objective 4, Tactic 4.3).*

- 5.3.1 Participate in interagency activities designed to deter/prevent contamination and disruption of crop and livestock production and the food supply.
- 5.3.2 Assist the U.S. Department of Agriculture (USDA), the Food and Drug Administration (FDA), and the Centers for Disease Control and Prevention (CDC) in development of a secure, electronic communication system for federal, state, and local governments that deal with food, using EPA's water utility system as a model. Completed.
- 5.3.3 Share EPA's plans for protection and preparedness with the federal food agencies. Completed.
- 5.3.4 Provide other food agencies with a list of contacts. Completed.
- 5.3.5 Participate in preparedness exercises conducted by other federal agencies related to food and water incidents. Completed.

**5.4 EPA will work with other federal, state, and local food agencies to share and strengthen current laboratory methodologies and capacities to respond to food-contamination emergencies.**

**RESULTS**

*In FY2003 and FY2005, EPA will coordinate with other agencies and increase lab capabilities to deal with these emergencies.*

- 5.4.1 Upgrade existing EPA laboratory capabilities to deal with food and environmental contaminants. (FY2004-FY2005)
- 5.4.2 Participate in the USDA/FDA chaired Food Emergency Response Network (FERN). Serve as members of the National Food Laboratory Steering Committee, the FERN Governance Committee, and the FERN Methods Development and Validation Work Group.
- 5.4.3 Work with other federal food agencies in the FERN to: 1) identify laboratories, 2) assess capabilities, and 3) develop methods to evaluate chemical contamination of food.

**OBJECTIVE 6 ⇒ EPA will manage its federal, civil, and criminal enforcement programs to meet its homeland security, counter-terrorism, and anti-terrorism responsibilities under the *National Strategy for Homeland Security, Homeland Security Act of 2002, Presidential Executive Orders, Homeland Security Presidential Decision Directives (HSPDs), and environmental civil and criminal statutes in accordance with the National Response Plan and the EPA National Approach to Response.***

EPA enforcement programs monitor compliance with and enforce a number of environmental statutes and associated regulations that can be important in homeland security efforts. Compliance and enforcement efforts in the accident and spill prevention regulatory programs can help assure that facilities take steps that are important in preventing unanticipated releases of materials harmful to public health or the environment and that such facilities are prepared to address the results of such an event. Enforcement of regulatory requirements related to manufacturing, distribution, and sales of pesticides and toxic substances can help assure that these materials stay out of the hands of criminals. Enforcement of regulatory requirements related to the generation, transportation, treatment, storage, and disposal of hazardous waste and substances can help assure that these materials stay out of the hands of criminals and protect the public health and the environment. Enforcement of emergency planning requirements can assure that facilities and first responders have the information necessary to respond to emergencies safely and efficiently. Enforcement of import/export laws can help assure that hazardous materials are not imported for illegal purposes.

The Agency's criminal enforcement program has the lead responsibility within EPA for crimes related to environment statutes. Terrorist threats or attacks are criminal acts. The intentional, unauthorized, release of a chemical or hazardous material, whether chemical, biological, or radiological is a crime. The motive determines whether the crime is an environmental crime or a terrorist act. Many times the motive for an intentional release is not immediately clear. As such, they are investigated by the federal government as a violation of any number of different federal

laws, including the criminal provisions of the nation's environmental laws, which are investigated by EPA Special Agents pursuant to title 18, United States Code, section 3063.

In general, under the provisions of HSPD 5, HSPD 7, HSPD 9, PDD 39, PDD 62 and the NRP, the Secretary of the Department of Homeland Security, the Attorney General, and other officials can call upon EPA law enforcement and technical resources, as well as response assets to be used for detection, preparation for, prevention, protection, as well as response to and recovery from a terrorist threat or attack.

## **TACTICS**

**6.1 EPA will fulfill its homeland security roles and responsibilities under the *National Strategy for Homeland Security, Homeland Security Act of 2002, Presidential Executive Orders, Homeland Security Presidential Directives (HSPDs), and environmental civil and criminal statutes in accordance with the National Response Plan and the EPA National Approach to Response to respond to requests for law enforcement support by the FBI or DHS to detect, prepare for, prevent, protect, and respond to terrorist attacks.***

## **RESULTS**

*By end of FY2003, EPA will have a counter-terrorism team trained to collect forensic evidence and respond in a hazardous environment. This team will be capable of being deployed to an incident within 12 hours after notification by the FBI or DHS. This capability is also incorporated into the EPA National Approach to Response Policy that provides a more integrated Agency-wide response to requests for support.*

- 6.1.1** Develop four, five-member EPA Office of Criminal Enforcement, Forensics, and Training (OCEFT) National Counter-Terrorism Evidence Response Teams (NCERT) to provide criminal, investigative, and technical environmental crime scene support to the FBI, DHS, or EPA emergency responders. Completed.
- 6.1.2** Develop a three-member Training/National Enforcement Investigations Center Counter-Terrorism Response Team (CTRTR) to provide NCERT personnel and other law enforcement agencies with civilian technical/scientific threat assessment/response support.
- 6.1.3** Train OCEFT/NCERT and CTRTR personnel to deliver law enforcement support to the DHS and/or USSS in the direct protection of critical infrastructure during National Special Security Events (NSSEs). Completed.
- 6.1.4** OECA will provide criminal investigative technical support to the FBI Joint Terrorism Task Forces (JTTFs) throughout the United States, which support local, county, state, and federal efforts to identify or detect, protect, prepare, prevent, and respond to threats/attacks on or to water systems as needed. Completed.

- 6.2 EPA will maintain an active presence at the FBI Strategic Information and Operations Center (SIOC), which houses the National Joint Terrorism Task Force (NJTTF) and the DHS national Homeland Security Operations Center (HSOC) with personnel familiar with and knowledgeable about EPA's programs and capabilities in order to provide critical environmental threat monitoring information to law enforcement and other agencies to ensure that EPA's existing monitoring expertise, standards, capabilities, and data are appropriately integrated into their efforts to detect terrorist attacks.**

**RESULTS**

*Beginning in FY2002, EPA will provide personnel to the FBI's NJTTF and the DHS HSOC.*

- 6.2.1** In FY2002, assign one EPA CID Special Agent to the NJTTF to act as a bridge between EPA programs and the FBI Counter Terrorism Division, including the Weapons of Mass Destruction Operations Unit, Countermeasures Unit and the Hazardous Materials Response Unit. Completed.
- 6.2.2** In FY2004, assign EPA OCEFT personnel to the DHS national HSOC. Completed.

- 6.3 The Agency will provide incident response and counter-terrorism training through the National Enforcement Training and the Federal Law Enforcement Training Center to federal, state, and local law enforcement personnel on environmental investigative techniques and related environmental criminal and civil investigations supporting homeland security and counter/anti-terrorism activities.**

**RESULTS**

*Beginning in FY2002, EPA will develop and begin conducting training of federal, state, and local law enforcement officials in homeland security issues. By the end of FY2003, the Office of Enforcement and Compliance Assistance (OECA) will train all necessary Headquarters (HQ) and regional compliance and enforcement staff. By the end of FY2002, EPA will begin the training programs at the Federal Law Enforcement Training Center.*

- 6.3.1** Provide environmental domestic terrorism training to the FBI, CBP, ICE and USSS law enforcement and technical support personnel.
- 6.3.2** Provide environmental international terrorism training to the State Department as well as through the State Department and the International Criminal Police Organization's (INTERPOL) U.S. National Central Bureaus (USNCB).
- 6.3.3** Provide environmental counter-terrorism training to State Associations of Chiefs of Police.
- 6.3.4** Provide environmental counter-terrorism training to County Sheriffs' offices through the Environmental Crime Committee of the National Sheriffs' Association and the Major County Sheriffs' Association.

**6.3.5** Provide environmental domestic and international training to the Environmental Crimes and Terrorism Committees of the International Association of Chiefs of Police and the Major City Chiefs of Police.

**6.4 EPA will implement and manage current criminal and civil regulatory programs that address areas related to homeland security.**

**RESULTS**

*EPA will expand compliance assistance and enforcement efforts for facilities subject to accident and spill prevention to include new guidance, public outreach, and increased inspections and enforcement actions.*

- 6.4.1** Provide analysis of environmental information and data [e.g., Clean Air Act (CAA), Risk Management Plan (RMP), Off-Site Consequence Analysis (OCA)] to deliver threat assessment products and related law enforcement support, through the OCEFT Center for Strategic Environmental Enforcement (CSEE), to local communities. This is provided through the DOJ U.S. Attorneys' Office (USAO), Anti-Terrorism Advisory Councils (ATACs), and DOJ FBI Joint Terrorism Task Forces (JTTF) to assist with the assessment of national, transborder, transnational, and international threats to domestic security.
- 6.4.2** Support a DOJ initiative to reduce security vulnerabilities of pipeline, fuel storage, chemical plant, and drinking water facilities through the increased enforcement of environmental laws, such as CAA 112(r) and CWA 311 - SPCC. DOJ maintains that the risk of a catastrophic terrorist incident can be reduced by increased inspections, bolstering enforcement and compelling compliance.
- 6.4.3** Increase efforts to deter the illegal import and export of hazardous waste and toxic and hazardous chemicals and materials regulated by EPA.
- 6.4.4** Improve data collection concerning hazardous waste import shipments through regulatory amendments and increased cooperation with the CBP at 301 ports of entry.
- 6.4.5** Develop a comprehensive tracking system for imports, including the electronic transmission of documents from sending governments to EPA, the Central Data Exchange (CDX)/Web Interface for Telescience (WITS) interface, and EPA regional linkage.
- 6.4.6** Improve border screening and movement monitoring of imported and exported hazardous waste, particularly waste chemicals of concern, in partnership with BCBP and industry at 301 ports of entry.
- 6.4.7** Increase efforts under the Federal Insecticide, Fungicide, and Rodenticide Act/Toxic Substances Control Act (FIFRA/TSCA) for manufacturing, distribution, sales, and licensing.

**6.5 EPA will meet direct protection responsibilities. Completed.**

**RESULTS**

*By the end of FY2002, EPA will develop and implement a plan for protective services. Completed.*

- 6.5.1** Maintain Special Agent Personal Security Detachment (PSD) Teams for the protection of Cabinet-level Presidential Appointees from terrorist threats as directed by the White House. Completed.
- 6.5.2** Assist USSS and the FBI with NSSE support of the President, Vice President, and other Designated Domestic and Foreign Dignitaries. Completed.

**6.6 EPA will meet the environmental, law enforcement, and cyber critical infrastructure protection responsibilities under HSPD 7.**

**RESULTS**

*EPA's CIO will lead an Intra-Agency Computer Security Incident Response Team (CSIRT) and work with EPA's Office of the Inspector General (OIG) and EPA's Criminal Investigation Division (CID), to plan responses to and counter cyber-attacks and promote critical infrastructure protection (CIP) within EPA and among approved, authorized, and delegated state programs interfacing with and reporting environmental data or information to the Agency.*

- 6.6.1** The OIG will establish a Computer Crimes Unit (CCU), which includes a computer forensic lab and intrusion unit. The CCU facilitates interagency and intra-Agency cooperative efforts to combat intrusions and other illegal activities involving the EPA's computer infrastructure.
- 6.6.2** The OIG will provide OIG/CCU support to Agency information security personnel by providing incident detection, response training, and incident response procedures.
- 6.6.3** The OIG will provide OIG/CCU support to OIG Office of Audits role in penetration testing of the EPA's computer network, and to the Office of Environmental Information (OEI) in the development of a penetration laboratory to identify vulnerabilities and correct them.
- 6.6.4** OIG and OECA will develop a team approach, consistent with their respective jurisdictions, under which EPA-OIG and EPA-CID will work with OEI to respond to cyber-attacks from both a program integrity, and a criminal environmental enforcement perspective, as appropriate, and will agree on procedures to share information relating to cyber-attacks in a manner that enables each to respond quickly and effectively.
- 6.6.5** In FY2002, OECA/OCEFT commenced operation of the National Computer Forensics Laboratory (NCFL) and a CID Electronic Crimes Team (ECT) to work jointly with the EPA OEI Security Staff, EPA OIG CCU, FBI, USSS, and other law

enforcement agencies in preventing and responding to criminal and terrorist cyber-attacks (e.g., denial of service attacks, illegal access, alteration or deletion of compliance data or confidential water infrastructure data, threats on EPA employees or facilities). Completed.

- 6.6.6 OECA will provide criminal investigator/technical support to the Agency's Water Security Division. Completed.
- 6.6.7 In FY2003, CID will assign one NCFL ECT member to the EPA OEI National Computer Center (NCC) to provide support to the on-site OIG CCU staff and the NCC's Information Security Staff. Completed.
- 6.6.8 In FY2003, NCFL ECT members will make twelve homeland security related presentations at water and wastewater trade association vulnerability assessment training sessions. Completed.

**6.7 EPA will use its Compliance Assistance Centers, compliance inspectors, and other field personnel to distribute information on compliance with programs related to homeland security and general information on security.**

**RESULTS**

*All compliance inspectors and enforcement personnel will receive homeland security training. Materials related to homeland security requirements as they relate to EPA's statutory and regulatory authorities will be disseminated to the regulated community.*

- 6.7.1 Develop and collect materials from various EPA programs and provide to the Compliance Assistance Centers and inspectors. (FY2004)
- 6.7.2 Provide training in issues related to homeland security to compliance inspectors and enforcement personnel. (FY2004)
- 6.7.3 Develop an implementation plan for outreach to the regulated community. (FY2004)
- 6.7.4 Train inspectors at border crossings in the United States, Mexico and Canada to detect illegal imports of chemicals, waste and materials, and expand existing hazardous waste border compliance center to include imports of toxic and chemical substances and include Canadian border. (FY2005)

**OBJECTIVE 7 ⇒ EPA will identify the Agency's critical infrastructures, assess their vulnerabilities, and take appropriate mitigation under PDD 63, HSPD 7, and the Project Matrix methodology.**

PDD 63 and HSPD 7 require every department and agency to develop a plan for protecting its own critical infrastructures. Federal department heads are responsible for the identification, assessment, remediation, and protection of their respective internal critical infrastructure and key resources.

**TACTICS**

- 7.1 EPA will work with DHS on implementing HSPD 7 and the Project Matrix methodology, including identify its critical infrastructures, and determine its inter-connectivity and interdependencies with other governmental and private sector critical infrastructures**

**RESULTS**

*By FY2004, inter-connectivity and interdependencies will be determined for each critical asset.*

- 7.1.1** EPA will work with DHS in Phase 2 of Project Matrix to complete an assessment of each critical EPA asset regarding its inter-connectivity and interdependencies with other government and private critical assets beyond EPA. (FY2004)

- 7.2 EPA will incorporate the results of Project Matrix into its internal protective measures.**

**RESULTS**

*By FY2005, EPA will have in place a comprehensive plan for protecting its physical and cyber critical infrastructure and key resources.*

- 7.2.1** EPA will incorporate the results of the Phase 1 and 2 Project Matrix determinations into the mitigation efforts described in Section II, III, and IV of this Strategy. (FY2005)
- 7.2.2** Update Continuity of Operation (COOP) Plans to ensure the recovery and reconstitution of these essential capabilities. (FY2005)

## II. Preparedness, Response, and Recovery

### *Strategic Objectives, Tactical Action Initiatives, and Benchmarks*

The terrorist attacks of September 11, 2001, and the subsequent anthrax releases have shown that EPA must continue to enhance its capabilities in preparedness, response, and recovery capabilities to adequately protect human health and safeguard the environment. The Agency must work more closely with government and industry partners, and ensure that all federal partners know where EPA fits into the federal response system. EPA currently maintains a cadre of personnel trained to respond to intentional or accidental chemical, biological, and radiological (CBR) releases, to protect the public health, and clean up contamination. The Agency continues to work closely with state and local agencies to enhance their own CBR preparedness and response programs, and provides the same type of response support in the event of national disasters under the Federal Response Plan (FRP) and, for radiological or nuclear incidents, under the Federal Radiological Emergency Response Plan (FRERP). EPA also provides support to the FBI during the initial or law enforcement phases of a terrorist threat or act, and plays a major role during the response, recovery, and mitigation phases of an attack.

In addition, the National Strategy for Homeland Security specifically designates EPA, in the event of a national incident, with the lead responsibility for decontamination of affected buildings and neighborhoods and providing advice and assistance to public health authorities in determining when it is safe to return to these areas and on safest disposal options for residues.

EPA also plays a critical role in regulating or recommending safe and effective chemicals to be used in the decontamination of buildings and other facilities contaminated with anthrax, other biowarfare agents, and new and emerging pathogens (e.g., SARS, Norwalk virus, Monkeypox, etc.).

**OBJECTIVE 1 ⇒ Consistent with HSPD 8, EPA will be prepared to respond to and recover from a major terrorist incident anywhere in the country. To do this, the Agency will maintain trained personnel and effective communications, ensure practiced coordination and decision-making, and provide the best technical tools and technologies to address threats.**

EPA will continue to maintain a sufficient body of trained personnel to respond quickly to multiple terrorist threats involving hazardous substances. In order to be effective, these personnel must have the best tools and technologies available to deal with the effects of weapons of mass destruction. In particular, the Agency will enhance its capability to respond to incidents involving biological, chemical, and radiological contaminants.

EPA is implementing a multifaceted mechanism - the National Approach to Response - to manage its emergency response assets during a Nationally Significant Incident in a coordinated manner. This approach will bring together existing criminal investigation, forensic evidence collection, and emergency response assets, along with a new management approach, to ensure the efficient and effective utilization of EPA assets. This approach will provide consistency in addressing key aspects of a response such as organizational elements (e.g., Incident Command System/Unified Command (ICS/UC), support personnel, and national teams), exercises and training, equipment, laboratory capability/capacity, and contracting. In addition, this approach will ensure that roles and responsibilities are clearly articulated.

## **TACTICS**

- 1.1 EPA will implement a new national approach to response that defines its internal emergency response decision-making and communications structures to be prepared for potential terrorist attacks of national significance. Completed.**

### **RESULTS**

*In exercises and nationally significant responses, EPA's decision-making and communication structures will function without major problems.*

- 1.1.1 Review the Agency's emergency response decision-making and communication structures for Nationally Significant Incidents (NSIs) and develop modifications. Completed.
  - 1.1.2 Dialogue with senior management, revise as needed and issue policy memo. Completed.
  - 1.1.3 Communicate the structures Agency-wide and train key personnel. Completed.
- 1.2 EPA will establish measurable improvement goals for the core-emergency response program and develop readiness criteria.**

### **RESULTS**

*In FY2003, EPA will establish readiness criteria for the core-emergency response program. In FY2004, EPA will develop and implement a baseline readiness assessment. After setting a baseline readiness score, EPA will improve by at least 10 percentage points per year until 100% readiness is achieved.*

- 1.2.1 Implement evaluation process and establish a baseline score. Completed.
  - 1.2.2 Continuously evaluate and improve the Agency's capabilities, as measured in the readiness criteria. (Annual)
- 1.3 EPA will increase the number and capability of emergency response personnel in the regional offices, labs, and ERT to enhance all counter-terrorism preparedness, response, and recovery functions.**

## **RESULTS**

*EPA will have enough On-Scene Coordinators (OSC), with in-house technical/scientific expertise and resources, ready to implement a full incident command for responses to major simultaneous terrorist incidents as follows: FY2004, two such incidents, and increasing by one per year, up to five simultaneous incidents. A major incident requires 10 OSCs capable of being incident commander and 20 OSCs in support roles, plus various technical and support personnel, and 100 contractor personnel for 24/7 operations for six months.*

*By the end of FY2004, EPA's Radiological Emergency Response Team (RERT) deployable lab capability will have been expanded through the purchase and implementation of additional equipment. In future years, RERT mobile lab capabilities will be maintained, updated, and exercised regularly.*

- 1.3.1** Create an Environmental Response Team (ERT) West to support the Agency-wide counter-terrorism program. Completed.
- 1.3.2** Enhance, and where appropriate, establish regional Emergency Operations Centers (EOC).
- 1.3.3** Hire additional OSCs. Completed.
- 1.3.4** Enhance the medical surveillance program for all potential responders and issue new guidelines. (FY2004)
- 1.3.5** Secure resources and staff for the National Response Decontamination Team to become fully functional. (FY2005)
- 1.3.6** Coordinate internally on sampling and analysis protocols, and laboratory data.
- 1.3.7** Develop and document procedures for exceeding administrative limits on radiation exposure during emergency response. (FY2004)
- 1.3.8** Replace NAREL's mobile environmental radiation lab and make ready for deployment in FY2005.

- 1.4** **EPA will establish an Incident Management Team (IMT) in each Region, which will be staffed by the Regions' emergency responders and other personnel and will be the Agency's immediate response mechanism for incidents, including terrorist incidents, in the Regions. The trained personnel from these IMTs also will serve as a pool of available emergency responders who will be called on to respond in the event of nationally significant incidents as part of national Incident Management Assistant Teams (IMATs).**

## **RESULTS**

*By early-mid FY2005, all elements of the Regional Incident Management Teams will be trained and capable of responding. By mid-late FY2005, the Regional Incident Management Teams will be deployed to an actual incident or to a major exercise.*

- 1.4.1** Identify constraints such as indemnification and limits of liability. (FY2002) Completed.

- 1.4.2 Identify training needs and train team members within the Incident Management Teams. (FY2004-2005)
- 1.4.3 Develop standard operating procedures for the IMT. (FY2004)
- 1.4.4 Pilot the overall IMT approach through participation in regional and National exercises. (FY2005)
- 1.4.5 Evaluate IMT. (FY2006)

**1.5 EPA will upgrade its existing radiation monitoring system to increase preparedness for terrorist and other incidents.**

**RESULTS**

*In FY2002 and beyond, EPA radiation laboratories will routinely analyze Environmental Radiation Ambient Monitoring System (ERAMS)/ National Monitoring System samples and maintain laboratory capability to perform radiochemical analyses for air, water, and other environmental samples during a contamination event.*

*In FY2005, EPA will be able to provide a radiation monitoring system that will have the capability of being deployed to the vicinity of an incident and provide near real-time radiological information downwind from the incident.*

- 1.5.1 Initiate purchase of upgraded equipment. (FY2004)
- 1.5.2 Research and identify new real-time gamma spectroscopy capabilities. (FY2005)
- 1.5.3 Acquire monitors for the deployable component to the National Monitoring System. (FY2004)
- 1.5.4 Develop a database for the maintenance of data from the National Radiation Monitoring System. (FY2005)

**1.6 EPA will examine its existing regulatory framework with respect to preparedness, response, and recovery from terrorist incidents. Completed.**

**RESULTS**

*EPA will be able to affirmatively state that no gaps exist in its response authorities.*

- 1.6.1 Perform analysis between existing authorities and all response plans to identify any gaps. (FY2002) Completed.
- 1.6.2 Develop white papers for senior management review to identify potential changes to current plans, regulations, or agreements. (FY2003) Completed.

**1.7 EPA will ensure its readiness to utilize the Agency's monitoring expertise during preparedness and recovery to monitor air quality for biologicals, chemicals, and radiologicals.**

**RESULTS**

*EPA will annually demonstrate its ability to deploy to an incident with emergency air monitoring capability necessary to ensure the safety of responders and the public. In exercises, federal, state, and local responders will demonstrate the ability to implement the Protective Action Guides (PAG) for response to a terrorist radiation incident.*

- 1.7.1 Develop a comprehensive mobile air Rapid Response Laboratory (RRL) to support the Office of Air and Radiation's (OAR) air monitoring for general population exposures and coordination with local and state monitoring agencies on public health protection. In addition to air monitors, the RRL will have advanced meteorological capabilities to support localized mixing, dispersion, and transport forecasting. (FY2004)
- 1.7.2 Identify regional points of contact and inventory monitoring equipment and skill within the regions that could be redeployed during an incident. (FY2004)  
Completed.
- 1.7.3 Exercise the deployment and use of EPA's air monitoring equipment. (FY2004)
- 1.7.4 Maintain and enhance EPA's air monitoring expertise and capabilities in ERT and via project ASPECT (airplane mounted sensors).
- 1.7.5 Coordinate with the Federal Radiological Preparedness Coordinating Committee (FRPCC) to revise the PAGs as necessary to incorporate counter/anti-terrorism and new guidance. (FY2004)
- 1.7.6 Augment EPA's capabilities to support the Advisory Team for Environment, Food, and Health under the FRERP. (FY2005)

**1.8 EPA will develop and implement a comprehensive training and exercise program for EPA's national emergency response program.**

**RESULTS**

*In FY2004 and beyond, EPA will implement a training and exercise program to test EPA personnel familiarity with and ability to implement EPA's National Approach to Response, incorporating lessons learned from each exercise.*

- 1.8.1 Establish a mechanism to identify specific objectives to be tested in exercises so that the successes and shortfalls can be incorporated into plans, procedures, acquisitions, and future exercises. (FY2004)
- 1.8.2 Develop five exercise scenarios for use nationally as a tabletop exercise. The five suggested scenarios include: Radiological (dirty bomb); Biological (persistent, contagious agent); Chemical Agent (in major public facility; various agents - sarin, VX, Br3, mustard, other); Large Scale Explosion/Building (collapse); Large Scale Fire (either chemical or oil). (FY2004)
- 1.8.3 Conduct five inter-regional/Headquarters tabletop exercises. (Annually)
- 1.8.4 Continue EPA's Radiological Emergency Response Team (RERT) training and incorporate RERT readiness into annual radiological exercises.

- 1.9 EPA will create a Response Support Corps of EPA employees within each region and at EPA Headquarters to stand ready to provide critical support to onsite EPA personnel during a nationally significant incident.**

**RESULTS**

*In FY2004 and beyond, the EPA Response Support Corps will stand ready to provide assistance in the field and in office settings during incidents that exceed existing response capabilities.*

- 1.9.1** Establish procedures for activating the RSC and determining the personnel and skills needed for a specific incident. (FY2004)
  - 1.9.2** Provide all RSC staff basic training on the Superfund Emergency Response Program and incident management. (FY2004)
  - 1.9.3** Provide RSC members the opportunity to participate in on-going removal actions and table top exercises.
- 1.10 EPA will ensure that the National Counter-terrorism Evidence Response Team (NCERT) maintains readiness to provide law enforcement, investigative, and technical forensic support to intentional threats or releases of hazardous materials and terrorist threats or attacks involving biological, chemical, or radiological agents in accordance with the National Approach to Response.**

**RESULTS**

*In FY2003, EPA's NCERT will establish readiness criteria for NCERT deployment throughout the United States in an incident of national significance. NCERT personnel and response equipment will be capable of supporting law enforcement investigation of an incident of national significance.*

- 1.10.1** Identify the NCERT Core Team made up of Special Agents and science support personnel that will present the "rapid deployment" team during the initial stages of an incident of national significance. Completed.
- 1.10.2** Create two mobile NCERT Response Vehicles to be staged in Washington D.C. and Denver, CO. Completed.
- 1.10.3** Initiate purchase of upgraded equipment.
- 1.10.4** Develop procedures for collection and handling forensic evidence in hazardous environments involving biological, chemical, radiological, and nuclear material in accordance with FBI and DHS guidance.
- 1.10.5** Provide OCEFT CID Special Agent to participate in National Joint Terrorism Task Force (NJTTF) at FBI Strategic Information Operations Center (SIOC). Completed.
- 1.10.6** Provide OCEFT CID Special Agent to participate in National Homeland Security Operations Center (HSOC) at the Department of Homeland Security. Completed.

- 1.10.7** Scientific and Technical Support - Provide support to Agency/national programs for the prevention, preparedness, response, and recovery from a terrorist threat or attack.

**OBJECTIVE 2 ⇒ EPA will assist in the development of a comprehensive National Response Plan for management of all domestic incidents.**

Under the leadership of the Department of Homeland Security and the White House Homeland Security Council, EPA and other members of the federal response community – with input from states, tribes and local government - will put into place a comprehensive, all-incident National Response Plan (NRP). This plan will integrate the current family of federal domestic prevention, preparedness, response, and recovery plans into a single, all-discipline, all hazards plan. The plan and related operational document, the National Incident Management System (NIMS), are required by Homeland Security Presidential Directive 5 (HSPD 5) issued on February 28, 2003. The Initial NRP (issued on September 30, 2003), the NIMS (planned for issuance by December 31, 2003) and the final or “full” NRP (planned for issuance by June 2004) will define and clarify both federal oversight requirements as they relate to aspects of incident management, as well as information flow during all phases, and from all participants in response to a terrorist attack or other disaster.

#### **TACTICS**

- 2.1 Pending the development and publication of the full NRP, EPA will contribute to the development of the Initial National Response Plan (INRP) which implements, on an interim basis, the domestic incident management authorities, role, and responsibilities of the Secretary of Homeland Security as defined by HSPD 5. It is applicable to domestic incident management in the context of terrorist attacks, major disasters, and other emergencies.**

#### **RESULTS**

*In FY2003 and FY2004, EPA will contribute to the development and issuance of the Initial National Response Plan (INRP).*

- 2.1.1** Evaluate existing interagency plans and if necessary, issue a policy to clarify EPA’s capabilities and authorities. Completed.
- 2.1.2** Reassess various plans (National Contingency Plan (NCP)), Federal Response Plan (FRP), Federal Radiological Emergency Response Plan (FRERP), and PDDs) to take into account lessons learned from September 11 and the anthrax incidents, and if necessary, initiate changes in the plans. Completed.
- 2.1.3** Coordinate with DOD Defense Threat Reduction Agency (DTRA) and other federal agencies on the collection and communication of air monitoring and assessment data. Completed.
- 2.1.4** Compare existing plans, interagency agreements, and applicable law, and identify direct and derivative authority for response to terrorist attacks or their intentional

criminal acts involving the release of hazardous materials to the environment or threats and/or attacks on critical infrastructure.

- 2.2 EPA will work with the Department of Homeland Security to develop the National Incident Management System (NIMS), which will provide a consistent national approach for federal, state, tribal, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. (FY2004) Completed.**

**RESULTS**

*EPA will contribute to the development and issuance of the National Incident Management System (NIMS) to be published by the Department of Homeland Security in FY2004. Completed.*

- 2.3 EPA will work with the Department of Homeland Security to develop the full National Response Plan, which will incorporate and all-hazards, multi-domain approach in the context of an incident “life-cycle.”(FY2004)**

**RESULTS**

*EPA will contribute to the development and issuance of the full National Response Plan (NRP) to be published by the Department of Homeland Security by FY2004.*

**OBJECTIVE 3 ⇒ In accordance with HSPDs 5 and 8, EPA will support and develop the preparedness of state, local, and tribal governments and private industry to respond to, recover from, and continue operations after a terrorist attack.**

The first response to an incident of terrorism usually takes place at the local level. It is therefore important to increase the capability of industry and state and local governments to respond to weapons of mass destruction and other terrorist attacks. EPA has existing relationships with these private and public partners through its preparedness and response programs; increasing the involvement in planning and information exchange between these varied organizations ultimately will improve response and recovery efforts. Key players in the implementation of this objective will be LEPCs, SERCs, and state Radiation Control Programs. As part of this effort, EPA will strive to improve upon the partnerships needed to support environmental preparedness nationwide and evaluate the state of readiness.

**TACTICS**

- 3.1 EPA will foster coordination among federal, state, tribal, and local emergency responders for response to homeland security incidents, including suspected criminally caused chemical releases.**

**RESULTS**

*State, tribal, and local emergency responders will increase their capability/ preparedness for response to homeland security incidents.*

- 3.1.1** Support training and exercises to promote coordination among federal, state, tribal, and local emergency responders.

**OBJECTIVE 4 ⇒ EPA will contribute its unique perspective to advance the state of the knowledge in the areas relevant to homeland security to provide responders and decision makers with tools and the scientific and technical understanding they need to manage existing or potential threats to homeland security.**

The unanticipated nature of the terrorist attacks on the United States have illustrated the need for EPA to expand its capabilities for responding to future, unknown threats to domestic security. The Agency intends to expand the state of the knowledge of potential threats, as well as its response capabilities, by assembling and evaluating private sector tools and capabilities so that preferred approaches can be identified, promoted, and evaluated for future use in responding to an attack. Where gaps exist, EPA will work with federal institutions and other organizations to fill those gaps through collaborative research.

**TACTICS**

- 4.1 EPA will undertake research, development, testing, and communication/ implementation of enhanced methods for detection and containment of biological and chemical warfare agents and bulk industrial chemicals intentionally introduced into large buildings/structures and for decontamination of building surfaces, furnishings, and equipment, with safe disposal of residual materials.**

**RESULTS**

*During FY2003 - FY2005, EPA will implement a plan for research, development, testing, and communication of enhanced methods for detection and containment of biological and chemical warfare agents and bulk industrial chemicals intentionally introduced into large buildings, as well as for decontamination of building surfaces, furnishings, and equipment, with safe disposal of residual materials. Detection activities include those related to defining the extent of contamination and verifying successful decontamination.*

- 4.1.1** Detection of Contaminants—Testing/verification of existing detection devices; development of new devices or methods for rapid response. (Conduct five evaluations by FY2004)
- 4.1.2** Containment of Contaminants—Development, evaluation, and testing of methods, and procedures for preventing the introduction and spread of contaminants, protecting building occupants, emergency responders, and decontamination crews. (Issue technical guidance by FY2004)

- 
- 4.1.3 Decontamination of Indoor Materials—Develop and evaluate the safety, efficacy, cost and materials compatibility of a range of technologies for decontaminating chemical and biological agents on indoor surfaces. (Complete study by FY2004)
  - 4.1.4 Development of Efficacy Test Methods—Collaboratively develop and evaluate sporicidal test methods for measuring the effectiveness of liquid and gaseous/vaporized chemicals in inactivating anthrax spores or surrogate Bacillus spores. To accomplish this objective, establish and lead an Interagency Expert Panel on Anthrax Efficacy Test Methods and Surrogates that will oversee the collaborative testing. (Phase I - FY2003; Phase II and III - FY2005)
  - 4.1.5 Disposal of Contaminated Clean-up Equipment and Supplies—Testing of disposal options methods; assessment of residual risk of disposal options; regulatory support to Agency programs for decontamination, disposal, and disposal permitting. (FY2005)
  - 4.1.6 Technology Transfer -Transfer of Improved Methods to Users—Provision of guidance and technical support on improved detection, containment, and decontamination methods for facility managers, building occupants, emergency responders, those sampling and analyzing materials in the environment, and decontamination crews. (FY2004)
- 4.2 **EPA will collaborate with other federal and state agencies, universities, industry, and others to identify efficacious pesticides to control potentially introduced high risk pathogens for crops, livestock, and human health.**

### **RESULTS**

*In FY2004 and FY2005, EPA will coordinate with these entities to begin to identify antimicrobials and pesticides that may be needed in the event of an attack involving a crop/pest disease or pathogen. EPA will work with these agencies under HSPD 9 (Defense of United States Agriculture and Food).*

- 4.2.1 Coordinate with CDC and others on evaluating and recommending antimicrobial chemicals that would be effective for inactivating emerging human pathogens and biological warfare agents in/on buildings, their contents, and indoor surfaces.
- 4.2.2 Issue crisis exemptions to permit the use of antimicrobial chemicals in a safe and efficacious manner in/on buildings, their contents, and indoor surfaces in order to inactivate Bacillus anthracis (anthrax) spores resulting from attacks in late 2001 through the United States mail system. (FY2004)
- 4.2.3 Provide guidance on EPA's registration requirements to companies seeking approval of antimicrobial chemicals intended to decontaminate biowarfare agents or emerging human pathogens. EPA will then review applications and make registration decisions for individual products. (FY2005)
- 4.2.4 Coordinate with USDA, state agencies and others on identifying, evaluating and approving pesticides that are suitable for addressing crop and livestock disease.

**4.3 EPA will undertake research, development, testing, and communication/implementation of enhanced methods for detection, treatment, and containment of biological and chemical warfare agents and bulk industrial chemicals intentionally introduced into drinking water systems.**

**RESULTS**

*To be determined*

- 4.3.1 Detection of Contaminants—Testing/verification of existing detection devices; development of new devices or methods for rapid response; and design of a detection network. (Complete six verifications by FY2004)
- 4.3.2 Containment of Contaminants—Development, evaluation, and testing of methods, and procedures for preventing the spread of contaminants in drinking water sources and distribution systems. (FY2005)
- 4.3.3 Decontamination of Contaminated Drinking Water—Development, evaluation, and testing of methods, technologies, and procedures for decontaminating drinking water, with consideration of efficacy, utility, safety, and cost. (FY2005)
- 4.3.4 Scientific and Technical Support—Provide support to Agency/national programs for understanding and managing events.
- 4.3.5 Technology Transfer -Transfer of Improved Methods to Users—Provision of guidance and technical support on improved detection, containment, and decontamination methods for utility managers, and emergency responders. (FY2005)

**4.4 EPA will develop technical information, including practices and procedures for developing rapid assessments to aid decision-makers and response personnel in emergency situations.**

**RESULTS**

- 4.4.1 Framework for conducting Rapid Risk Assessments—EPA will develop practices and procedures for developing rapid assessments to aid decision-makers and response personnel in emergency situations. (FY2005)
- 4.4.2 National Expertise Inventory—EPA will inventory internal, government, and private sector national expertise to provide quick access to nationally recognized experts in areas relevant to homeland security (e.g., biology, chemistry, exposure assessments, and detection/treatment technologies). Inventory will be used to provide highly specialized expertise to emergency response efforts. Completed.
- 4.4.3 Determine and prioritize biological contaminants, chemicals of concern, and radionuclides for which response protocols are needed. (Complete evaluation by FY2004)

- 
- 4.4.4 Develop Acute Exposure Guideline Limits (AEGLs), which are short term exposure limits for hazardous substances for purposes of chemical emergency response, planning, and prevention.
  - 4.4.5 Using tools and procedures developed under Tactics 4.1 and 4.3, simulate field tests (and get feedback from emergency responders) and report on the safety and efficacy of new methods for detection, containment, decontamination and disposal.
  - 4.4.6 Provide support to determine “How Clean is Safe” (e.g., provisional guidance values) to assist Agency officials in decision-making for the various stages of response to a terrorist incident (i.e., emergency/rescue response, containment, decontamination). (FY2005)
  - 4.4.7 Expand the National Expertise Inventory to include a directory of sampling and analysis technologies, methods, and subject experts for use by emergency responders. (Subject matter experts listing completed. Methods directory to be completed FY2004)
  - 4.4.8 Develop and compile information for use by emergency responders and decision-makers when communicating risks associated with terrorist incidents.
- 4.5 **EPA will address Homeland Security laboratory issues with other federal agencies, such as the White House Homeland Security Council, Department of Homeland Security, and/or CDC, and will assist in developing intergovernmental response networks of environmental and health and food laboratories’ capabilities and capacities for the analyses of chemical, biological and radiochemical compounds of concern in support of emergency response/WMD events.**

### **RESULTS**

*In FY2004, EPA will continue to work with other federal, state, and private sector entities to share information. EPA will support establishing regional intergovernmental response networks of laboratories with capabilities and capacities for analyses of environmental chemical, biological and radiological contaminants associated with WMD.*

- 4.5.1 Participate in federal interagency workgroups (e.g., USDA/FDA’s FERN, CDC’s Laboratory Response Network (LRN), FBI’s Scientific Working Group on Forensic Analysis of Chemical Terrorism (SWGFACT) to address laboratory issues, including assessment of capability and capacity for analyses of biological, chemical and radiological warfare agents/contaminants of concern.
  - 4.5.2 Coordinate with a response network of federal, state, and local government and private laboratories capable of environmental sample analyses for chemical, biological, and radiological contaminants associated with WMD. Completed.
  - 4.5.3 Develop and maintain one common Interagency electronic data reporting format (e.g., Staged Electronic Data Deliverable) for use during emergencies, incorporating electronic submission from qualified laboratories. (FY2005)
  - 4.5.4 Create a compendium of EPA, state and select private sector laboratories that are currently capable of analyzing environmental samples for chemical, biological, and radiological agents associated with WMD. (FY2004)
-

### III. Communication and Information

#### *Strategic Objectives, Tactical Action Initiatives, and Benchmarks*

To be most effective when making decisions related to homeland security, the Agency must have clearly defined and understood approaches to sharing and communicating necessary information, including classified material, with internal and external users. EPA will work to improve communications with Agency employees and managers; ensure that information is effectively shared within the Agency; and work with the Department of Homeland Security to improve and extend data-sharing partnerships with federal, state, and local governments. EPA will also work to ensure that clear structures are in place to exchange relevant information with the national security, law enforcement, and intelligence communities. EPA realizes that there may be times during emergencies when decisions must be made quickly and decisively without having knowledge of the full breadth and depth of the situation. At these times, the Agency will leverage and optimize its resources to make an informed decision.

**OBJECTIVE 1 ⇒ EPA will use best available environmental information from internal and external sources to ensure informed decision-making and appropriate response.**

EPA plays an important part in the collaborative effort to prevent, detect, and respond to environmental security threats by ensuring that decision-makers have access to the data they need. EPA will continue to broaden its efforts in this area to include enhancing the consistency of monitoring data collection and facilitating data sharing among federal agencies and state and local governments.

Over time, EPA will work to ensure resource, public health, and environmental protection data will be linked together to monitor the state of the nation's environment and to perform environmental risk management and resolution. Data on pollutant releases/emissions, ambient conditions, and environmental effects will be more complete, of higher quality, and displayed in an easy to understand format.

#### **TACTICS**

##### **1.1 EPA will enhance consistency in the collection of environmental data.**

#### **RESULTS**

*EPA will have the ability to collect and analyze environmental information from all necessary sources to respond to incidents and threats.*

##### **1.1.1 Develop an emergency response database and presentation tools. Completed.**

1.1.2 Develop Staged Electronic Data Deliverables (i.e., SEDD) for chemical and radiological agents in a standard format. (Initial work for Rad is complete as of FY2003, working on further modifications).

1.1.3 Develop an analytical data management tool for emergency response data. (FY2005)

**1.2 EPA will build partnerships with key health and environmental organizations to facilitate the sharing of homeland security related information.**

**RESULTS**

*Linkages between health and environmental data sources and EPA access portals will support flows, analysis, and tools necessary to monitor and respond to incidents and threats.*

1.2.1 Sign MOU with HHS and CDC/Agency for Toxic Substances and Disease Registry (ATSDR) to support data sharing. (FY2002)

1.2.2 Develop EPA-wide geospatial data sharing program with partners. (FY2003)

1.2.3 Develop capacity for federal, state, and local health agencies to use standard reporting formats. (FY2003)

**1.3 EPA will develop a situation management capability to inform appropriate action by federal, state, local, and private entities. Completed.**

**RESULTS**

*The situation capability will support confident decision-making by linking science and policy through data and technology.*

1.3.1 Review records management procedure and information holdings to ensure conformance to the March 19, 2002, memorandum from White House Chief of Staff Card entitled “Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security,” and the October 12, 2001, memorandum from Attorney General Ashcroft regarding disclosure decisions under the Freedom of Information Act. Completed.

1.3.2 Develop draft EPA criteria and guidance on protection of sensitive information. Completed.

**OBJECTIVE 2 ⇒ EPA will effectively disseminate timely, quality environmental information to all levels of government, industry, and the public, allowing them to make informed decisions about human health and the environment.**

EPA will improve its ability to communicate effectively with the public regarding terrorist incidents and environmental threats. The Agency will challenge environmental and public health agencies to develop better approaches to sharing information about environmental consequences in ways that the public can easily understand. EPA will also work with the new Department of Homeland Security and other federal agencies to develop a process that will allow timely release of environmental data that are critical to effective decision-making at all levels. In addition, EPA will create appropriate tools and environmental outreach materials that address health impacts and exposure guidelines for relevant contaminants, and will develop understandable materials describing common emergency response activities (sampling and monitoring, debris hauling, washing activities, etc.).

Finally, the Agency will establish a clearly defined approach to policymaking, on-scene coordination, and external communications in a critical response context to ensure clarity and consistency of messages and enhanced coordination within government.

### **TACTICS**

- 2.1 EPA will use a structured approach within the Agency for information releases that clearly defines roles for public communication during incidents and emergencies.**  
Completed.

#### **RESULTS**

*Lines of authority and roles/responsibilities for communication will be understood and relied upon by staff and management during and after an incident.*

- 2.1.1** Create a cross-Agency workgroup to address internal threat, incident, or emergency communication barriers and make recommendations for change—coordinate with the National Incident Coordination Team (NICT). Completed.
  - 2.1.2** Integrate information dissemination processes into emergency response planning. Completed.
  - 2.1.3** Develop a protocol for internal communications in support of incident/emergency response. Completed.
  - 2.1.4** Develop training and educational material to inform managers and staff of communication processes and structure used during incidents/emergencies. Completed.
- 2.2 EPA will improve the ability to communicate effectively with the public regarding incidents and threats.**

#### **RESULTS**

*EPA will be able to effectively and reliably communicate information about incidents and environmental risks in ways the public can understand.*

- 2.2.1** Develop a network of tools to facilitate public communication.

- 2.2.2 Work with public health agencies to create specific environmental outreach materials that address health impacts and exposure risks.
- 2.2.3 Enhance the Integrated Risk Information System (IRIS) to include repository of exposure data used to communicate with the public.
- 2.2.4 Define approach to ensure access to Agency Web-based information 24x7. Completed.
- 2.2.5 Define critical data applications and categories with time sensitive parameters.
- 2.2.6 Identify hot site(s) for critical data hosting and build out, test and operate. Completed.
- 2.2.7 Ensure backup power and telecommunications redundancy to the National Computing Center (NCC) and hot sites(s). Completed.
- 2.2.8 Create a mirror site for the Agency's public access Web site. Completed.

**OBJECTIVE 3 ⇒ EPA will classify, declassify, safeguard, manage, and destroy all national security information in accordance with Executive Order 12958, as amended by Executive Order 13292; and exchange information with other federal, state, and local assets to prevent, deter, and respond to terrorist threats or attacks; and improve and streamline personnel security services to ensure employees are granted and maintain active security clearances in a timely manner.**

EPA will work with the Department of Homeland Security to create a clearly defined structure for coordination with the national security, law enforcement, response, and intelligence communities. As outlined in Section II, the Agency will develop appropriate response coordination plans to ensure an EPA and government-wide understanding of roles, responsibilities and capabilities.

### TACTICS

- 3.1 **EPA will create clearly defined mechanisms for appropriate communication and coordination with national security and law enforcement communities.**

### RESULTS

*EPA will demonstrate effective management and use of sensitive and classified information through the use of the appropriate facilities and protocols.*

- 3.1.1 Design a Sensitive, Compartmented, Information Facility (SCIF) or redesign EPA's existing SCIF. Completed.
- 3.1.2 Certify the SCIF meets appropriate standards. Completed.
- 3.1.3 Issue design criteria for the construction of a Sensitive, Compartmented, Information Facility (SCIF). (FY2005)
- 3.1.4 Develop policies and procedures for managing and operating a SCIF. (FY2005)

**3.2 EPA will improve its National Security Information program through establishing comprehensive policies and procedures for classifying, declassifying, safeguarding, and managing classified information.**

**RESULTS**

*EPA will have a model National Security Information program that will allow the Agency to participate as a full partner in sharing of appropriate classified material with the law enforcement and national security communities.*

- 3.2.1 Develop policies and procedures to classify, declassify, and safeguard national security information. (FY2004)
- 3.2.2 Develop and implement an education and training program on National Security Information. (FY2004)
- 3.2.3 Develop and implement a self-audit and inspection program. (FY2004)
- 3.2.4 Issue an EPA Order on National Security Information. Completed.
- 3.2.5 Perform computer intrusion investigations relating to Homeland Security matters effecting EPA computer networks, programs, and operations.

**3.3 EPA will continue to improve its Personnel Security Program through providing timely processing of investigation applications, reviewing and adjudicating investigations, and granting security clearances.**

**RESULTS**

*EPA will have the security clearances necessary for full participation and support of Agency and inter-Agency activities and emergency response functions.*

- 3.3.1 Work with OPM to ensure security clearances are being processed in a timely manner.
- 3.3.2 Maintain an up-to-date list of employees with security clearances.
- 3.3.3 Track and monitor the status of all security clearances and investigations.
- 3.3.4 Pass security clearances to other federal agencies in a timely manner on an as-needed basis.
- 3.3.5 Initiate periodic re-investigations in a timely manner to maintain active clearances on personnel.

**OBJECTIVE 4 ⇒ EPA will continuously and reliably communicate with employees and managers.**

EPA is committed to supporting its employees and staff, whether they are directly responsible for homeland security activities or engaged in day-to-day environmental protection responsibilities. A critical step in fulfilling this commitment is ensuring that the capacity exists for continuous

communication (including voice and data connectivity) with employees, responders, and decision-makers throughout the life of an incident.

#### **TACTICS**

#### **4.1 EPA will deploy new technology applications for communication during national emergency situations.**

##### **RESULTS**

*Continuous communication with employees, responders, and decision-makers will occur throughout the life of an incident through the use of current technology.*

**4.1.1** Deploy a Virtual Private Network (VPN) in full production for EPA. Completed.

**4.1.2** Coordinate with other agencies on development and deployment of a federal extranet.

**4.1.3** Develop specifications for mobile command posts. (FY2004)

#### **4.2 EPA employees will be provided with appropriate information, training, and support to respond to emergencies and incidents.**

##### **RESULTS**

*EPA employees will be prepared, informed, and trained to effectively manage and respond to terrorist threats and incidents.*

**4.2.1** Develop health and safety training/guidance for emergency responders. (FY2005)

**4.2.2** Develop and communicate employee safety and health information in conjunction with Occupant Emergency Plan communication training.

**4.2.3** Offer stress management training and individualized counseling for employees.

**4.2.4** Provide Continuity of Operations Plan (COOP) education and training Agency-wide.

**4.2.5** Refine message process for reaching employees at work, home, and at emergency sites.

## IV. Protection of EPA Personnel and Infrastructure

### *Strategic Objectives, Tactical Action Initiatives, and Benchmarks*

In order for EPA to meet all of the objectives established in this Strategy, the Agency must ensure the security of its own personnel and infrastructure and be able to provide continuity of operations in an emergency. The Agency's strategic objectives for protecting EPA personnel and infrastructure cover the protection of EPA's personnel, continuity of operations, and the protection of EPA's information infrastructure and other physical assets.

#### **OBJECTIVE 1 ⇒ EPA will safeguard its personnel.**

EPA is committed to safeguarding its personnel by providing a safe workplace that is as secure from physical or cyber attacks as possible.

The Agency will maintain up-to-date Occupant Emergency Plans (OEP) for EPA facilities to respond to terrorist attacks and other emergencies. In addition, all Agency personnel will be trained on the OEPs, and the OEP exercise program will be continued and revitalized to ensure that Agency personnel are able to effectively implement the plans when needed.

The Agency will also help develop and effectively utilize a unified federal response group of safety and health experts and capabilities, including representatives from HHS and FEMA. EPA will also work with local emergency planners to ensure that EPA facilities are included in local contingency planning activities.

#### **TACTICS**

##### **1.1 EPA will actively manage and maintain a robust and vibrant Occupant Emergency Plan (OEP) Program to safeguard personnel.**

#### **RESULTS**

*EPA personnel will be familiar with evacuation and shelter-in-place procedures at EPA's facilities nationwide in the event of an emergency or national incident.*

- 1.1.1 Maintain up-to-date OEPs for EPA facilities.
- 1.1.2 Conduct frequent evacuation and shelter-in-place drills.
- 1.1.3 Fully implement the revised HQ OEP program to include AA-ship management responsibilities and accountability. (FY2004)
- 1.1.4 Provide continuing education and training to personnel, managers and supervisors, security guards, and OEP Team representatives. (As needed basis)

## 1.2 EPA will utilize a unified federal response group of safety and health experts.

### **RESULTS**

*EPA safety and health professionals will be properly equipped, properly trained, and an integral part of a unified network of federal partners ready to respond in the event of an emergency.*

- 1.2.1 EPA will pursue a strengthening of field proficiencies of safety and health professionals, as well as establish an internal capability for unified support.
- 1.2.2 EPA will strengthen and maintain a network with other federal partners such as: CDC, National Institute for Occupational Safety and Health (NIOSH), ATSDR, National Institutes of Health (NIH), U.S. Public Health Service (USPHS), HHS, and U.S. Army Medical Research Institute for Infectious Diseases (USAMRIID) to stay current and involved in the cutting edge of medical and protective applications relative to biological, chemical radiation exposures, and/or other terrorist related risks.
- 1.2.3 EPA will integrate a core training program to include emergency response and safety and health personnel to improve consistency, communication and support capabilities.

**OBJECTIVE 2 ⇒ EPA will ensure the continuation of the Agency's essential functions and operations.**

EPA is committed to ensuring that it is prepared to continue essential functions during an emergency. The primary vehicles to accomplish this task are the Continuity of Operations (COOP) Plans. The Agency will continue to enhance these plans at the Headquarters and regional levels to ensure that it can quickly deploy key personnel to alternative locations and expeditiously resume essential functions. EPA is working to enhance access to critical records and databases and improve communications with field offices in order to support this effort. A prescribed exercise program will also assist in the improvement of implementation of the plans. Finally, EPA will develop memoranda of understanding and interagency agreements as needed to ensure that EPA can secure goods and services to support continued EPA operations.

### **TACTICS**

- 2.1 **EPA will maintain current COOP Plans and ensure organizations are prepared to implement them.**

### **RESULTS**

*EPA will have the capability to ensure the continuation of essential functions in the event of an emergency or threat of emergency as demonstrated through exercises.*

- 2.1.1 Update planning documents. Completed.
- 2.1.2 Prepare an alternate facility. Completed.
- 2.1.3 Establish capability to communicate, coordinate operations, and access requisite records and databases from that alternate facility. (FY2004)
- 2.1.4 Conduct regular training activities and exercises.
- 2.1.5 Participate in interagency COOP exercise (Forward Challenge). (FY2004)

**2.2 EPA will ensure the quick identification of technical and scientific expertise.**

**RESULTS**

*EPA will have the technical and scientific expertise it needs, where and when it is needed, to respond to and recover from a national emergency. To ensure the quick identification of technical and scientific expertise, EPA will implement a Workforce Planning methodology in a phased-in approach.*

- 2.2.1 Pilot the Workforce Planning methodology and information management tools to identify competencies in at least six program offices and three regions. Begin to address the mission critical skill and competency gaps/surpluses in those offices. (FY2004)
- 2.2.2 Complete an Agency-wide implementation of the Workforce Planning methodology for all areas of the pilot offices (approximately 9,000 personnel). (FY2004)
- 2.2.3 Complete an Agency-wide Workforce Planning System competency inventory. (FY2005)

**OBJECTIVE 3 ⇒ EPA will maintain a secure technology infrastructure capable of supporting lab data transport and analysis functions, 24x7 telecommunications to all EPA locations, and management of critical Agency data and information.**

EPA is committed to analyzing and aligning the Agency's technical (IT and labs) capabilities to meet expectations and strategic objectives. EPA will provide a "hot" site for critical Agency data with redundant telecommunications capability and will support an emergency response center with the necessary information technology infrastructure to ensure data and voice communication throughout at all times. EPA will also provide wireless and hardwired technologies to all emergency response personnel for voice, email, and internet access.

**TACTICS**

- 3.1 **EPA will analyze and align technical capabilities to meet expectations and strategic objectives.**

**RESULTS**

*EPA's technical infrastructure will continuously and reliably support decision-makers and staff in carrying out the Agency's responsibilities during and after incidents and threats.*

**3.1.1** Conduct analysis of OEI technical capabilities.

**3.2 EPA will provide a "hot" site for critical data with redundant telecommunications capability.** Completed.

**RESULTS**

*EPA operates a "hot" site with redundant telecommunications for critical data.*

**3.2.1** Develop specifications and create a "hot" site for critical operations. Completed.

**3.3 EPA will support an emergency response center with needed IT infrastructure.** Completed.

**RESULTS**

*The emergency response center has the necessary IT infrastructure.*

**3.3.1** Coordinate with the Office of Solid Waste and Emergency Response (OSWER) to ensure continuous service. Completed.

**3.4 EPA will provide wireless and hardwired technologies to all emergency response personnel for voice, email, and internet access.**

**RESULTS**

*All emergency response personnel have wireless and hardwired technologies for voice, email and internet access.*

**3.4.1** Develop specifications and provide wireless and hardwired technologies to emergency response personnel. (FY2004)

**OBJECTIVE 4 ⇒ EPA will ensure that the Agency's physical structures and assets are secure and operational.**

EPA is committed to an on-going program of assessing, mitigating, and auditing and upgrading EPA's physical infrastructures and assets to ensure they meet minimum physical security requirements as outlined in DOJ's USMS Vulnerability Assessment of Federal Facilities, June 28, 1995. Additionally, the Agency will design, construct, and lease new buildings and major additions that reflect contemporary security features in accordance with the Interagency Security

Committee's (ISC) Security Design Criteria, dated May 28, 2001; and GSA's new Security Leasing Standards (Draft Dated February 3, 2003).

EPA will also protect technical assets, both fixed and mobile, such as monitors, scanner vans, mobile sample prep trucks, trailers, etc., so that equipment will be accessible and functioning in the event of an emergency.

## **TACTICS**

### **4.1 EPA will safeguard and protect its EPA personnel and buildings/facilities by continually assessing and improving physical security.**

#### **RESULTS**

*EPA personnel will be able to work in safe and secure facilities, which are continually being assessed and upgraded, as appropriate, to meet contemporary security standards, including leveraging and optimizing new technology.*

- 4.1.1** EPA will complete physical security vulnerability risk assessments for all of EPA's Security Level 4 and 3 facilities. (FY2003) Completed.
- 4.1.2** In accordance with Federal Protective Service guidance, EPA will conduct physical security vulnerability risk assessments of its Security Level 4 facilities every two years, Security Level 3 facilities every three years, and Security Level 2 facilities every four years.
- 4.1.3** EPA will mitigate critical and high physical security vulnerabilities and risks at EPA's Security Level 4, 3, and 2 facilities, where appropriate. These mitigation efforts will be ongoing for multiple years.
- 4.1.4** EPA will conduct reviews/audits at Security Level 3 and 4 facilities to ensure that funded mitigation efforts were completed properly and identify new findings. (FY2004)
- 4.1.5** EPA will complete window vulnerability assessments at its Security Level 3 and 4 facilities. (FY2004)
- 4.1.6** EPA will initiate window mitigation efforts at three of its Security Level 3 and 4 facilities. (FY2004)
- 4.1.7** EPA will develop and implement new physical security standards through assistance from the Interagency Security Committee, the U.S. DOJ's USMS Vulnerability Assessment of Federal Facilities (June 28, 1995), and other relevant guidance. (FY2005)
- 4.1.8** EPA will determine, select and provide the appropriate protective equipment and level of protection, as well as appropriate training, for safety, health, and security personnel involved in response and remediation. (FY2003)
- 4.1.9** EPA will coordinate and provide medical consultation, monitoring, and treatment for personnel who may experience hazardous exposures to threatening agents while engaged in terrorist act response and remediation activities and/or support.

**4.1.10** Design, construct, and lease buildings that reflect contemporary security features in accordance with applicable criteria. EPA will incorporate Interagency Security Committee's Design Criteria and GSA's Public Building Services' Facilities Standard into design and construction. Additionally, EPA will implement GSA's new Security Leasing Standards (Draft dated February 3, 2003) on all leases from this point forward.

**4.2 EPA will protect technical assets, both fixed and mobile (e.g., monitoring and testing equipment), so equipment will be accessible and functioning in the event of an emergency.**

**RESULTS**

*EPA will have the equipment it needs, where and when it needs it, and technical assets will be adequately protected, accessible, and functioning.*

**4.2.1** Standardize methods for conducting technical procedures so staff from various labs and HQ offices are interchangeable in deploying to the field and operating equipment. EPA will develop two standardized methods in FY2003 and three methods in FY2004 for conducting technical procedures for deploying field and operating equipment. (FY2003 and FY2004)

**4.2.2** Security services will be acquired from commercial providers or local law enforcement entities, as needed, to protect fixed and mobile assets.

## V. Evaluation

### *Strategic Objectives, Tactical Action Initiatives, and Benchmarks*

OIG will conduct audits and evaluations to help ensure that EPA achieves its Homeland Security objectives and its appropriations supporting homeland security are spent efficiently and effectively. Also, OIG is responsible for assessing cyber threat information that affects EPA's computer infrastructure, and will initiate needed investigative responses.

**OBJECTIVE 1 ⇒ EPA will add to knowledge, verification, or action contributing to reduction or elimination of infrastructure and other security risks or challenges.**

OIG will organize its assessment of EPA homeland security along topical responsibilities: water and wastewater security, food safety, and air. Many of the concerns that apply to water security will be applicable to the other Agency priorities as well. Therefore, OIG will construct an assessment template that can be applied to water, food, and air. The template will consider: threats, capabilities, and deficiencies, readiness, management, and effectiveness. The mix of questions can include – but is not limited to – the following:

- Threats, Risks, and Vulnerabilities: How are threats and risks identified and validated? How are threat assessments to be conducted? How are assessments disseminated, accessed, and stored?
- Preparedness: Do emergency response plans reflect the findings of the vulnerability assessments? What is the emergency response concept of operations and how are the roles, responsibilities, and activities of the respective stakeholders identified, coordinated, and exercised?
- Capabilities: What capabilities are required by each stakeholder to implement the emergency response plans? What is EPA's role in identifying and addressing challenges that may impede implementation of emergency response plans? How will stakeholders compensate for challenges (in the short term) and resolve them (in the long term)?
- Research and Technology Assessment: How will EPA identify and prioritize objectives in its Homeland Security research plan? How will the Agency's research and development complement work in other agencies and the private sector? How will the Agency select the technologies to initiate its technology verification program?
- Financial Assistance: Are current and planned security grants sufficient to achieve the Agency's security objectives? Are the grants effective in achieving the Agency's objectives? Are grants awarded directly to utilities more or less efficient than those administered through the states?

- Oversight and Effectiveness: Are management and financial controls in place to prevent waste, fraud, and abuse by contractors? Are agreements and understandings in place to ensure coordination of functional activities contracted by operators and government agencies? Are objectives established?

## **TACTICS**

### **1.1   OIG evaluation work will help determine: How can EPA better execute its Strategy to prevent, prepare, and respond to a terrorist attack to minimize adverse impacts on human health and the environment?**

#### **RESULTS**

*By FY2005, the OIG will answer the following questions and provide specific recommendations to improve the economy, efficiency and effectiveness EPA strategic Homeland Security initiatives.*

- 1.1.1   Water Security: How well is EPA carrying out its responsibilities to coordinate the protection of drinking water and wastewater infrastructures?
- 1.1.2   Water Security Grants: Is EPA adequately monitoring grantee performance? Are the grants resulting in improvements in security of large drinking water systems?
- 1.1.3   Air Protection - How well is EPA carrying out its responsibilities to protect ambient and indoor air from chemical and biological threats?
- 1.1.4   Food Supply Safety: How well is EPA carrying out its responsibilities assisting other federal agencies in protecting the nation's food supply?
- 1.1.5   Equipment Purchases for Counter Terrorism Preparedness: Should EPA stockpile normal response equipment and supplies? How did EPA determine needed quantities? Does EPA know that contractors do not have or cannot get needed quantities quickly? Have other ways to address the quantity concerns, such as setting up purchase agreements, been pursued? Will contractors receive government-furnished equipment instead of buying equipment themselves? How will EPA track this equipment?