



OFFICE OF THE UNDER SECRETARY OF DEFENSE

DCN 2623

3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION
TECHNOLOGY
AND LOGISTICS

JUN 21 2005

Mr. Frank Cirillo
Director, Review & Analysis
The Defense Base and Realignment Commission
2521 South Clark Street, Suite 600
Arlington, VA 22202

Dear Mr. Cirillo:

In our continued efforts to ensure you have the material used in the Department's BRAC 2005 process, enclosed are drafts of the DoD Strategy for Homeland Defense and Civil Support dated September 13, 2004, January 4, 2005, and March 28, 2005, respectively. These are the coordination drafts available during the development of the 2005 BRAC recommendations and referred to in BRAC Policy Memorandum, "Transformation Through Base Realignment and Closure (BRAC 2005) Policy Memorandum Five – Homeland Defense".

This same material is being provided to Congress.

Sincerely,

Philip W. Grone
Deputy Undersecretary of Defense
Installations and Environment

Enclosure:

A compact disc containing the following information:

1. Strategy for Homeland Defense and Civil Support dated September 13, 2004
2. Strategy for Homeland Defense and Civil Support dated January 4, 2005
3. Strategy for Homeland Defense and Civil Support dated March 28, 2005

 **RECEIVED**
06212005



FIRST COORDINATION DRAFT

Strategy for Homeland Defense and Civil Support



**Department of Defense
Washington, D.C.**

Current as of: September 13, 2004

FIRST COORDINATION DRAFT



Table of Contents

Executive Summary1

I. Context7

 Relationship to Standing National and Defense Strategies7

 Organizing for Homeland Defense and Civil Support8

 Key Definitions.....10

 Legal Authorities.....10

 Security Environment.....11

 Assumptions12

II. Active, Layered Defense.....13

III. Strategic Goal and Key Objectives.....17

 Lead.....19

 Support22

 Enable22

IV. Core Capabilities.....25

 Capabilities for Achieving Maximum Awareness of Threats25

 Capabilities for Interdicting and Defeating Threats at a Safe Distance29

 Capabilities for Providing Mission Assurance35

 Capabilities for CBRNE Consequence Management.....40

 Capabilities for Enhancing US and International Capabilities for Homeland Defense and Homeland Security41

V. Implications of the Strategy.....45

 Force Structure45

 Technology.....48

 Funding50

VI. Implementing the Strategy53

 Managing Homeland Defense and Civil Support Risk.....53

 Actions for Immediate Implementation54

VII. Conclusion.....59

Appendix A. Legal Authorities.....61

Appendix B. New Roles for the Guard and Reserve63

Appendix C. Strategic Planning Guidance Tasking69



Executive Summary

"The world changed on September 11, 2001. We learned that a threat that gathers on the other side of the earth can strike our own cities and kill our own citizens. It's an important lesson; one we can never forget. Oceans no longer protect America from the dangers of this world. We're protected by daily vigilance at home. And we will be protected by resolute and decisive action against threats abroad."

President George W. Bush

September 17, 2002

Protecting the United States homeland from attack is the highest priority of the Department of Defense (DoD). On September 11, 2001, the world changed dramatically. For the first time since Pearl Harbor, we experienced catastrophic, direct attacks against our territory. This time, however, the foe was not another nation but terrorists seeking to undermine America's political will and destroy our way of life. As a result, the United States has become a nation at war, a war whose length and scope may be unprecedented.

We now confront an enemy who will attempt to engage us not only far from US shores, but also at home. Terrorists will seek to employ asymmetric means to penetrate our defenses and exploit the openness of our society to their advantage. By attacking our citizens, our economic institutions, our physical infrastructure, and our social fabric, they seek to destroy American democracy. We dare not underestimate the devastation that terrorists seek to bring to Americans at home.

To defeat 21st century threats, we must think and act innovatively. Our adversaries consider US territory an integral part of a global theater of combat. We must therefore have a strategy that applies to the domestic context the key principles that have shaped

the successful transformation of US power projection and joint expeditionary warfare.

Protect the United States from Attack through an Active, Layered Defense

This Strategy for Homeland Defense and Civil Support focuses on achieving the Defense Department's paramount goal: securing the United States from attack by external enemies, while recognizing the need for an innovative approach to military operations within the United States. The strategy is rooted in the following:

- Respect for America's constitutional principles;
- Adherence to Presidential and Secretary of Defense guidance;
- Compliance with the Department's statutory authorities to conduct homeland defense and civil support missions;
- Recognition of terrorist and state-based threats to the United States; and
- Commitment to continue transformation of US military capabilities.

Protecting the United States in the ten-year timeframe covered by this Strategy requires a strategic concept for an active, layered defense. **This active, layered defense is global, seamlessly integrating US capabilities in the forward regions of the world, the global commons of space and cyberspace, in the geographic approaches to US territory, and within the United States. It is a defense in depth.** To be effective, it requires superior intelligence collection and analysis, calculated deterrence of enemies, a layered system of mutually supporting defensive measures that are neither passive nor ad hoc, and the capability to mass and focus sufficient warfighting assets to defeat any attack.

This active, layered defense employs tactical defenses in a strategic offense. It maximizes threat awareness and seizes the initiative from those who would harm us. In so doing, it intends to defeat potential challengers before they threaten the United States at home.

Organizing Construct—Lead, Support, and Enable

Although the active, layered defense extends across the globe, this Homeland Defense and Civil Support Strategy focuses primarily on DoD's activities in the homeland and the approaches to US territory. In those geographic layers, the Department undertakes a range of activities to protect the United States from attack. These generally divide into the following categories:

- **Lead:** At the direction of the President or the Secretary of Defense, the Department of Defense executes military missions that prevent, deter, defend, and defeat attacks upon the

United States, our population, and our defense critical infrastructure.

- **Support:** At the direction of the President or the Secretary of Defense, the Department of Defense provides support to civil authorities. This support is part of a comprehensive national response to prevent and protect against terrorist incidents or deal with the consequences of an attack or disaster. DoD provides support in situations where civilian responders are unable, overwhelmed or where DoD's unique capabilities are required.
- **Enable:** The Department of Defense actively seeks to improve the homeland defense and homeland security contributions of our domestic and international partners and, in turn, to improve DoD capabilities by sharing expertise and relevant technology, as appropriate, across traditional military and civilian boundaries.

Key Objectives of the Strategy

Within the lead, support, and enable framework for homeland defense and civil support, the Department is focused on the following paramount objectives, listed in order of priority:

- **Achieve maximum awareness of potential threats.** Together with the Intelligence Community and civil authorities, DoD works to obtain and promptly exploit all actionable information needed to protect the United States. DoD has mechanisms to provide that information to warfighters and policy makers.

- **Interdict and defeat threats at a safe distance.** The Department of Defense will defend the United States in our air and maritime approaches. Consistent with applicable law, we also defeat external threats within US airspace and on US territory.
- **Provide mission assurance.** The Department of Defense performs assigned duties, even under attack or after disruption. We protect our forces, installations, and information; ensure crisis management, continuity of operations (COOP), and continuity of government (COG); and ensure the security of defense critical infrastructure.
- **Support civil authorities to deal with the consequences of domestic chemical, biological, radiological, or nuclear or high explosive (CBRNE) mass casualty attacks.** The Department of Defense will be prepared to provide forces and capabilities in support of domestic CBRNE consequence management, particularly for multiple simultaneous mass casualty incidents. Although organized, trained and equipped primarily for warfighting missions, US military forces must be trained and ready to provide timely assistance to civil authorities in times of domestic catastrophes as well.
- **Improve national and international capabilities for homeland defense and homeland security.** The Department of Defense is learning from the experiences of domestic and international partners and sharing expertise with federal, state, local,

and tribal authorities, the private sector, and US allies and friends abroad. By sharing expertise across traditional boundaries, we improve the ability of the Department of Defense to carry out an active, layered defense.

Capability Themes for Homeland Defense and Civil Support

Several important themes underlie the objectives and capabilities established by this Strategy:

- **Intelligence, Surveillance, and Reconnaissance Capabilities.** The Department of Defense requires current and actionable intelligence defining potential threats to US territory. DoD must also ensure that it can identify and track suspect traffic in the air and maritime approaches and conduct reconnaissance to examine wide areas of the maritime and air domains to discover potential threats before they reach the United States.
- **Information-Sharing.** Together with domestic and international partners, DoD will integrate information collected from a wide range of sources. The events of September 11, 2001 highlighted the need to share information across federal agencies and, wherever possible, with state, local, and tribal authorities, the private sector, and international partners.
- **Joint Operational Capabilities for Homeland Defense.** DoD must continue to transform US military

forces, especially the Reserve Component, to execute homeland defense and civil support missions in the air and sea approaches, within US airspace, and on US territory.

- **Interagency and Intergovernmental Coordination.** The Department of Defense and our domestic and international partners will continue to coordinate closely in the execution of homeland defense and civil support missions.

When fully realized, this Strategy for Homeland Defense and Civil Support will transform and improve DoD capabilities in each of these areas. The Nation will have effective intelligence, surveillance, and reconnaissance capabilities for homeland defense, and information will be widely shared with relevant decision-makers. The Department of Defense will have well-trained and responsive forces for homeland defense. These forces will use a networked information enterprise and innovative operational concepts to eliminate barriers among the land, air, and maritime operating environments. Finally, the Department of Defense, our interagency partners, and our allies and friends abroad will achieve unity of effort in the execution of homeland defense and civil support missions.

Projected Implications of the Strategy

This Strategy was developed with an understanding of its force structure, resource, and technology implications. Such a fiscally informed approach is necessary given the Department's resource constraints and the demands of the National Defense Strategy. As DoD components implement the strategic

tenets outlined in this document, a more precise accounting of the forces, technological advances, and financial resources it requires will be needed. An initial assessment indicates that certain adjustments will be required.

- **Force Structure.** The Department requires timely, trained, and transformed forces for homeland defense and civil support. In particular, maritime defense of the United States will require new force capabilities. Countering low-flying airborne vehicles in US airspace and in the US approaches will likewise require additional capabilities. The Department will improve the planning, training, and equipping of warfighting forces for their potential use in support of domestic CBRNE consequence management. Finally, throughout the range of homeland defense and civil support missions, the Department will need to make better use of Reserve Component forces.
- **Technology.** The Strategy calls for significant investments in advanced technology to enable information sharing. Information sharing in turn requires research related to privacy and collaboration tools. The Strategy also requires advances in imagery collection capabilities; improved sensors for a better picture of air, land, and maritime environments; and improved technologies and equipment for remote detection of CBRNE materials. The Strategy emphasizes the need for basic research into non-lethal capabilities to better support homeland defense missions. It also

emphasizes the need for medical technology investments in such areas as automated triage, telemedicine, and self-care. In these areas and others, the Department of Defense will use programs for rapidly prototyping new capabilities, such as Advanced Concept Technology Demonstrations (ACTD).

- **Funding.** Some of the Strategy's core capabilities could also be among its most costly. Foremost among these is the planned expansion of the Department's information infrastructure, a prerequisite for integrating information and ensuring maximum awareness of threats. Providing the right capabilities and assets for maritime defense of US territory may also require a substantial financial investment. Other elements that will have major fiscal implications are better sensor technology, closing gaps in critical infrastructure protection, improved capabilities for continuity of operations, new non-lethal capabilities, and key improvements in Reserve Component capabilities for homeland defense and civil support.

Implementing the Homeland Defense and Civil Support Strategy

As DoD's forces and resources are limited, the Strategy recognizes the need to manage risk within the homeland defense and civil support mission areas. It does so by allocating DoD forces and resources in accordance with the Strategy's prioritization of objectives. That is, within the homeland defense and civil

support mission space, we will focus our resources on fulfilling the Department's lead responsibilities for homeland defense. As a second priority, we will ensure the Department's ability to support civil authorities in recovering from mass casualty CBRNE incidents within the United States. The Department also will ensure that homeland defense is appropriately resourced relative to other National Defense Strategy priorities within the Department's overall integrated risk management strategy.

This Strategy includes a series of initiatives designed to drive the Department's transformation for homeland defense and support of civil authorities across the five key objectives:

- Conduct a zero-based assessment of the sensors and other capabilities needed to detect, identify, and track objects in the air, land, sea, and space
- Assess the architectural requirements and investment options for ensuring interoperability among DoD and interagency partners in the homeland defense mission space;
- Identify initiatives to improve defense intelligence and IC capabilities for homeland defense;
- Assess the maritime requirements of US Northern Command;
- Develop joint concepts of operations and requirements for a joint, rapidly deployable area air and cruise missile defense architecture;
- Develop a detailed roadmap to expand the use of National Guard and other Reserve Component units for homeland defense and civil support missions;

- Develop a concept of operations and identify requirements for the domestic employment of non-lethal capabilities;
- Ensure that the Department of Defense fully implements the Defense Critical Infrastructure Program Integrated Risk Management Strategy;
- Analyze current DoD capabilities for continuity and crisis management;
- Ensure the protection of high priority DoD installations and personnel from CBRNE attacks; and
- Implement a comprehensive and systematic homeland defense exercise program by FY2006.

The Department will move swiftly on these initiatives in order to protect the United States from attack. This will require the integration of homeland defense and civil support into the Department's capabilities development processes.

The Strategy for Homeland Defense and Civil Support is not a static document. Even as the Department of Defense implements this Strategy, it will continue to adapt to changes in the strategic environment, incorporate lessons learned from operational experience, and capitalize on emerging technology and operational concepts.



I. Context

“For most of the twentieth century, the world was divided by a great struggle over ideas: destructive totalitarian visions or freedom and equality. That great struggle is over. The militant visions of class, nation, and race which promised utopia have been defeated and discredited. America is now threatened less by conquering states than we are by failing ones. We are menaced less by fleets and armies than by catastrophic technologies in the hands of the embittered few. We must defeat these threats to our Nation, allies, and friends.”

*The National Security Strategy of the United States of America
September 2002*

The Strategy for Homeland Defense and Civil Support embodies the core principles articulated in the US Constitution, the Nation’s laws, and in Presidential and Secretary of Defense guidance. It also responds to the challenges posed by the security environment over the next decade.

Relationship to Standing National and Defense Strategies

The Strategy for Homeland Defense and Civil Support integrates the objectives and guidance expressed in the National Security Strategy, the National Strategy for Homeland Security, and the National Defense Strategy to guide Department of Defense operations to protect the US homeland.

- The National Security Strategy (2001) expanded the scope of US foreign and

security policy to encompass forward-reaching preventive activities, including pre-emption, against hostile states and terrorist groups.

- The National Strategy for Homeland Security (2002) guides the national effort to secure the US homeland against terrorist attacks. It provides direction and a framework for action at all levels of government that play a role in homeland security.
- The National Defense Strategy (2001), set forth in the Quadrennial Defense Review, identified the defense of the United States as DoD’s primary mission, to include its land, sea, air, and space approaches. Thus, the first strategic objective of the National Defense Strategy is to protect the United States from attack.

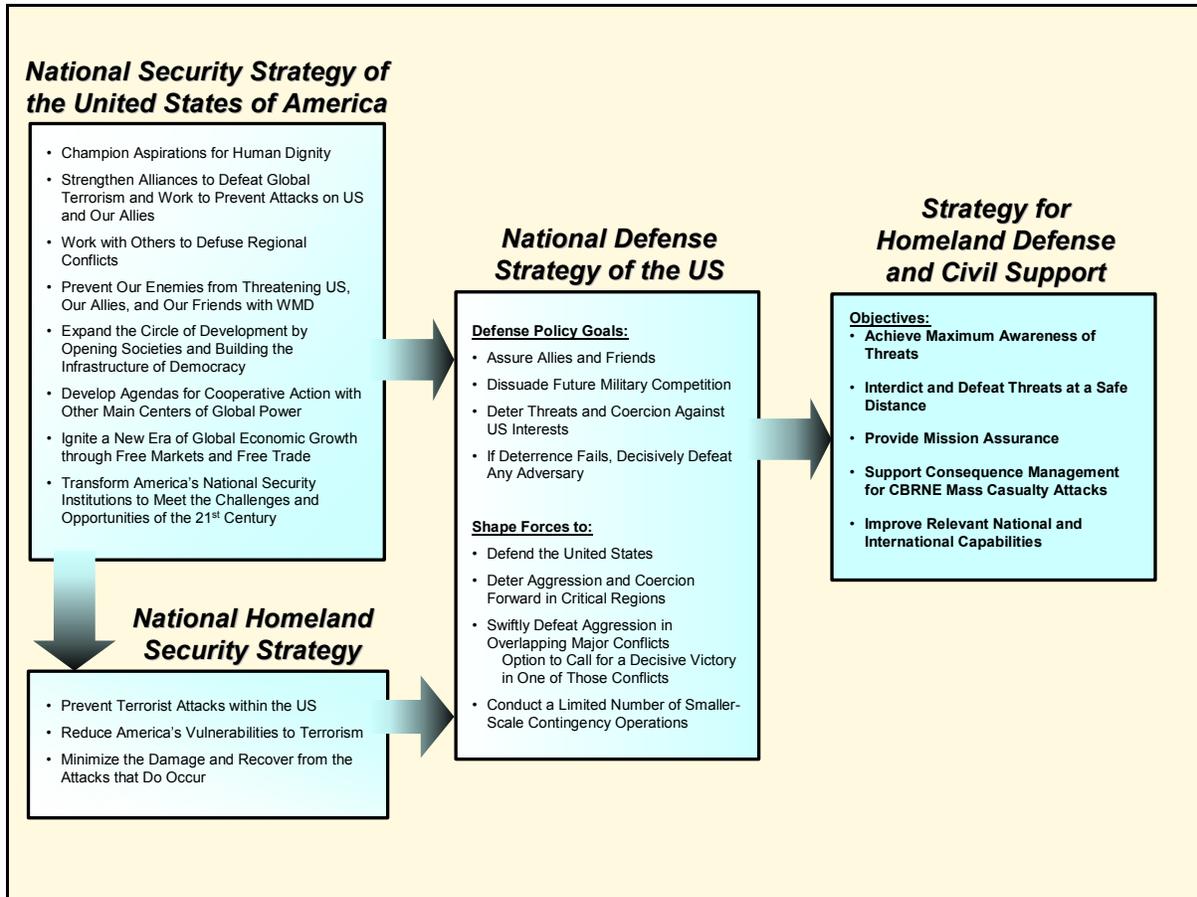


Figure 1: Strategic Underpinnings of the Homeland Defense and Civil Support Strategy

In addition to these overarching strategies, the Strategy for Homeland Defense and Civil Support is also informed by, and complements, the many national and homeland security implementing strategies. These include the National Military Strategy, the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, the National Strategy to Secure Cyberspace, the National Strategy for Combating Terrorism, the National Strategy to Combat Weapons of Mass Destruction, the National Strategy for Biodefense, the National Strategic Plan for Homeland Security Science and Technology, and the DoD Director of Force Transformation's Military Transformation: A Strategic Approach.

Organizing for Homeland Defense and Civil Support

In light of the importance of homeland defense and DoD's contributions to homeland security, the Secretary of Defense, with the support of Congress, has improved the Department's organization and oversight structure for homeland defense and civil support.

- **The Assistant Secretary of Defense for Homeland Defense.** As directed in the 2003 National Defense Authorization Act, the Assistant Secretary of Defense for Homeland Defense provides overall supervision of DoD's homeland defense activities.

I. Context

The establishment of the Assistant Secretary for Homeland Defense responded to the need for improved policy guidance to combatant commanders and other DoD components on homeland defense and civil support issues.

- **US Northern Command**, headquartered in Colorado Springs, Colorado. Established in 2002, US Northern Command is responsible for planning, organizing, and undertaking all aspects of homeland defense and executing civil support missions within the continental United States, Alaska, and territorial waters. It also coordinates security cooperation with Canada and Mexico. In addition to the

land masses of the United States, Canada, and Mexico, the US Northern Command (NORTHCOM) area of responsibility includes the coastal approaches, the Gulf of Mexico, Puerto Rico, and the US Virgin Islands.

- **US Pacific Command**, headquartered in Honolulu, Hawaii. US Pacific Command (PACOM) has homeland defense and civil support responsibilities for Hawaii and US territories, possessions, and freely associated states in the Pacific.

All other regional and functional combatant commands, the Military Departments, and other DoD elements also contribute to the protection of the US homeland from attack.

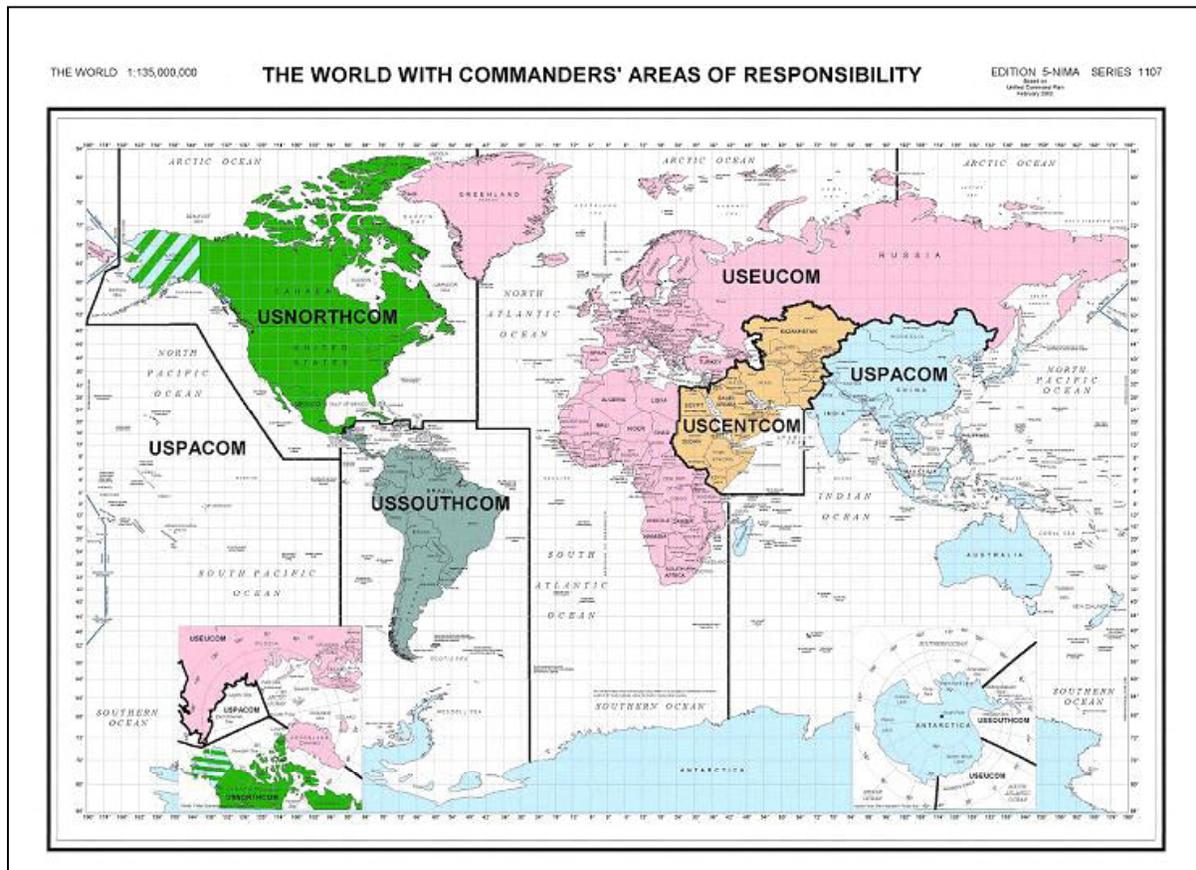


Figure 2: Regional Combatant Commanders' Areas of Responsibility

- Other regional combatant commanders can promote international cooperation on homeland defense through exercises and military-to-military contact programs. Together with the functional combatant commanders, these regional commanders can also provide early interdiction and defeat of adversaries intent on attacking US territory.
- The Military Departments organize, train, and equip US military forces for homeland defense missions—in the land, aerospace, maritime, and cyber domains.
- Other DoD Components contribute to homeland defense through intelligence collection, analysis, and prioritization; capabilities analysis; and oversight of relevant policy, acquisition, logistics, personnel, readiness, and financial matters.

The Homeland Defense and Civil Support Strategy will guide all DoD Components across the full range of homeland defense and civil support activities.

Key Definitions

Homeland security, as defined in the National Strategy for 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 Department of Homeland Security is the lead federal agency for homeland security. In addition, its responsibilities extend beyond terrorism to preventing, preparing for, responding to, and

recovering from a wide range of major domestic disasters and other emergencies.

Homeland defense is the protection of US sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression. The Department of Defense is responsible for homeland defense.

Defense support of civil authorities, or civil support, is DoD support provided during and in the aftermath of domestic emergencies—such as terrorist attacks or major disasters—and for designated law enforcement and other activities. When directed by the President or Secretary of Defense, DoD provides support of civil authorities by employing the Nation’s federal military forces, the Department’s career civilian and contractor personnel, and DoD agency and component assets.

Legal Authorities

The primary legal authority to conduct military missions in defense of US territory and interests is Article II, Section 2 of the US Constitution, which gives the President, as commander in chief, broad authority to conduct homeland defense missions.

In homeland defense missions, DoD discharges the statutory obligation to defend the Nation. Homeland defense missions thus constitute a critical part of DoD’s core war-fighting mission.

In addition, a variety of statutory provisions provide the basis for the Department’s support missions. Among those are the Stafford Act (42 USC 5121 et. seq.), which provides the statutory framework for the Department’s disaster relief efforts in support of civil authorities, and the Defense Against

Weapons of Mass Destruction Act (Public Law 104-201, September 23, 1996), which authorized the Department to support civil authorities in domestic CBRNE consequence management.

Appendix A provides a detailed discussion of relevant legal authorities.

Security Environment

The defining characteristic of the security environment over the next ten years is the certainty of substantial diverse and asymmetric challenges to the United States, our allies, and interests. This Strategy for Homeland Defense and Civil Support addresses the full range of challenges to the US homeland over the next decade.

Nation state military threats to the United States will persist throughout the next decade. Rogue nations, for example, pose immediate and continuing challenges to the United States and our allies, friends, and interests. In addition, we must prepare for the potential emergence of regional peer competitors.

The United States will also face a range of asymmetric, transnational threats. The disintegration of the Soviet Union at the end of the last century fundamentally reconfigured the strategic landscape. Old adversaries became partners, alliances dissolved or adjusted to new challenges, and some states began to disintegrate in the vacuum created by the end of superpower competition. In many former totalitarian states, US ideals of freedom and democracy took firm root. Elsewhere in the world, however, radical ideologies espoused by transnational terrorist groups also took hold. Over time, these terrorists have gained

increasing access to destructive capabilities heretofore the exclusive domain of nation-states. **In the next ten years, these terrorist groups, poised to attack the United States and actively seeking to inflict mass casualties, represent the most immediate challenge to the Nation's security.**

Transnational terrorist groups view the world as an integrated, global battlespace in which to exploit perceived US vulnerabilities, wherever they may be. This battlespace includes the US homeland. Terrorists seek to attack the United States at home and abroad and will use asymmetric means to achieve their ends, such as simultaneous, mass casualty attacks. On September 11, 2001 and, more recently, in the 2004 Madrid train bombings, terrorists demonstrated both the intent and capability to conduct complex, geographically dispersed attacks against the United States and our allies. It is foreseeable that adversaries will also develop or otherwise obtain chemical, biological, radiological, nuclear, or high-yield explosives (CBRNE) capabilities, with the intent of causing mass panic or catastrophic loss of life. Although America's allies and interests abroad will be the most likely targets of terrorism in the coming decade, we should also anticipate enemy attacks aimed at Americans at home.

A number of underlying factors in the security environment support the conclusion that these transnational challenges will persist throughout the timeframe of this Strategy. These factors include the following: the spread of extremist ideologies, the existence of failed or failing states, the spread of information technology and expertise, and the illicit proliferation of CBRN materials and advanced weaponry to rogue states, terrorist groups, and criminal organizations. Further,

we anticipate that adversaries will continue to traffic in narcotics, weaponry, and other illicit material to fund their activities.

Despite the certainty of significant state and transnational threats, we face great uncertainty regarding the specific character, timing, and sources of potential attacks. Our inability to predict the future with precision must not be a rationale for paralysis. Rather, we must pursue an active, layered defense to mitigate that uncertainty—primarily through the deterrent presence and operational employment of agile military forces, reprioritized intelligence collection, improved analysis and broader sharing of information. Prudence dictates that we must also be prepared to respond and recover rapidly from attacks.

Assumptions

This Strategy makes the following key assumptions:

- The United States will continue to face traditional military challenges emanating from hostile nation-states. Nation-state adversaries will incorporate asymmetric threats into their broader strategies of competition and confrontation with the United States.
- Terrorists will seek and likely gain surreptitious entry into the United States to conduct mass casualty attacks against Americans on US soil.
 - Terrorists will leverage vulnerabilities to create new methods of attack.
 - Terrorists and/or rogue states will attempt multiple, simultaneous mass casualty CBRNE attacks against the US homeland.
- Terrorists will try to shape and degrade American political will in order to diminish American resistance to terrorist ideologies and agendas.
- Allies and friends will cooperate with the United States in mutually beneficial security cooperation arrangements.
- US Northern Command and US Pacific Command will continue to develop mature homeland defense capabilities in the air, land, and sea domains, with appropriate support provided by other combatant commands.
- The Department of Homeland Security and other federal, state, and local agencies will continue to improve their prevention, preparedness, response, and recovery capabilities throughout the decade.
- The Department of Defense will promote the integration and sharing of applicable DoD capabilities, equipment, and technologies with federal, state, local, and tribal authorities and the private sector.
- In the event of major catastrophes, the President or Secretary of Defense will direct DoD to provide substantial support of civilian authorities. DoD's responses will be planned, practiced, and carefully integrated into the national response.
- The likelihood of US military operations overseas will be high throughout the next ten years.



II. Active, Layered Defense

“The war on terror will not be won on the defensive. We must take the battle to the enemy, disrupt his plans, and confront the worst threats before they emerge. In the world we have entered, the only path to safety is the path of action. And this nation will act.”

President George W. Bush

June 1, 2002

The Department is transforming its approach to homeland defense, just as it is transforming national defense capabilities overall. **Guiding homeland defense planning is the concept of an active, layered defense, predicated on seizing the initiative from adversaries.**

The case for an active, layered defense is clear. The United States has multiple points of vulnerability that adversaries seek to exploit. Commerce relies on the flow of goods and people across the Nation’s borders, through our seaports and airports, and on our streets and highways. The US free market economy requires trust in the uninterrupted electronic movement of financial data and funds through cyberspace. The symbols of American heritage—monuments and public buildings—are a source of national pride and are open to all. Vast and potentially vulnerable natural resources provide power to our homes and food for our tables.

To safeguard the American way of life and to secure our freedom we cannot depend on passive or reactive defenses. A strictly defensive strategy is easily subject to enemy reconnaissance and inevitable defeat. By contrast, an active, layered defense relies on early warning of an emerging threat in order

to quickly deploy and mass a decisive response.

The United States must keep potential adversaries off balance by both an effective defense of US territory, and when necessary, by projecting power across the globe. **We must seize the initiative from adversaries and leverage DoD advantages in netcentric operations. In short, the United States must act in ways that an enemy cannot predict, circumvent, or overcome. Multiple barriers to attack must be deployed across the globe, creating an unpredictable web of land, sea, and air assets that are arrayed to aggressively detect, deter, and defeat hostile action.**

An active, layered defense stretches across the integrated, global battlespace. This battlespace consists of the forward regions, the approaches to the United States, the American homeland, and the global commons of space and cyberspace. In each of these four areas, DoD must create effective barriers to attacks against the US homeland, whether launched by a hostile nation-state or a transnational terrorist group.

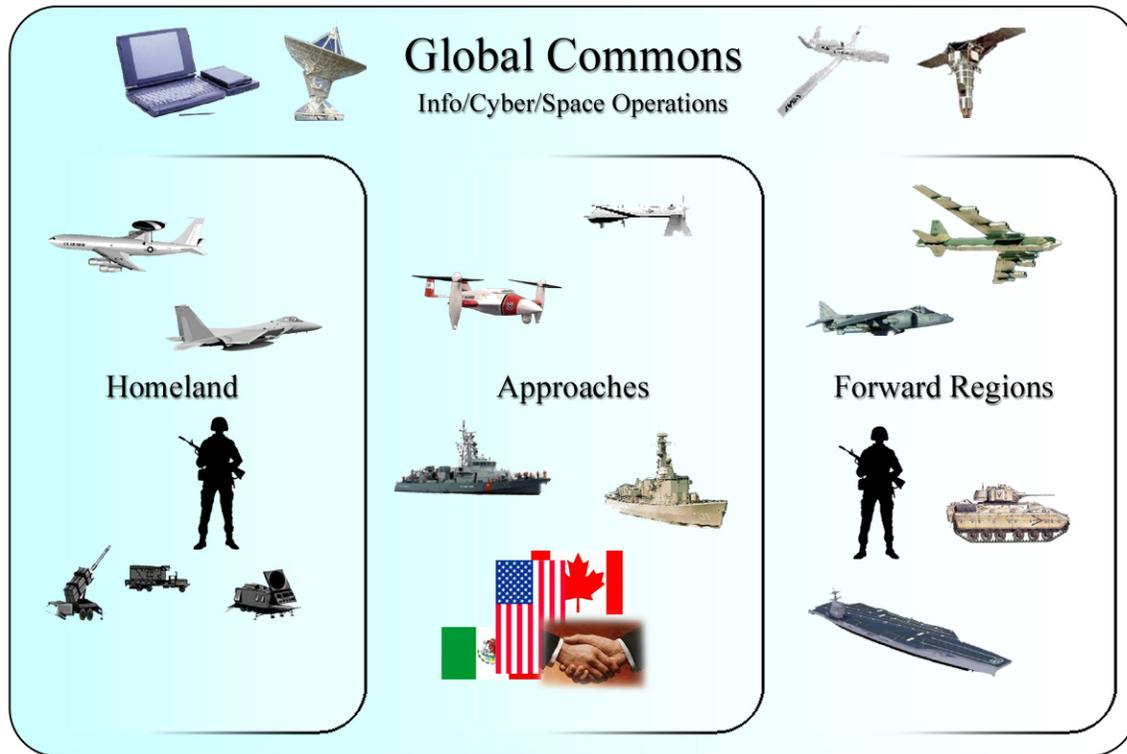


Figure 3: Active, Layered Defense Concept

The Forward Regions. Overseas, US military success depends on the quality of intelligence and the Department’s power projection capabilities. To respond quickly to rising threats, the United States requires accurate, timely, and actionable intelligence. Improved human intelligence (HUMINT) and analysis of possible terrorist threats and measurement and signatures intelligence (MASINT) on potential CBRN weapons are critical in this regard. In addition, US military forces must be trained, ready, and postured to interdict potential enemies, eliminate enemy sanctuaries, and maintain regional stability, in conjunction with allies and friendly states. In addition, the United States must counter and delegitimize the ideological support for terrorist groups, disrupt their flow of funding, and create an environment that curtails recruitment.

The Approaches. The waters and airspace geographically contiguous to the United States are critical homeland defense battle-spaces. In these approaches, US Northern Command and US Pacific Command, supported by other combatant commands, have the greatest opportunity to detect, deter, and, if necessary, defeat threats en route—before they reach the United States. **This requires maximum awareness of threats in the air and maritime avenues of approach as well as the interdiction capabilities necessary to maintain US freedom of action and protect the United States at a safe distance.**

To achieve these objectives, the United States requires advanced sensor capabilities that can detect, identify and track emerging threats in air and maritime environments. These objectives also require improved MASINT— which can provide unambiguous

identification of CBRN materials—and investments in remote CBRN detection.

Critical to our success will be sophisticated and agile maritime interdiction capabilities that can be called upon across the vast reaches of our maritime approaches in order to defeat transnational terrorist threats in international waters. This enhanced maritime interdiction capability in turn requires innovative maritime platforms and forces to conduct consensual and non-consensual searches. Finally, maximum threat awareness and effective interdiction require information sharing and cooperation with America’s closest neighbors and other international partners to protect land, sea, and air approaches.

The American Homeland. The US homeland includes the United States, its territories and possessions, and the Commonwealths and Compact States of the Pacific. Within US territory, the Department of Defense has the following responsibilities:

- DoD is responsible for defeating hostile state and transnational terrorist attacks against the United States, when so directed by the President or Secretary of Defense. The North American Aerospace Defense Command is the cornerstone of our homeland air defense capability. Our air defense success rests on an integrated system for air surveillance and defense against air threats at all altitudes. DoD also maintains land forces capable of responding rapidly, when so directed, to threats against

DoD personnel, defense critical infrastructure, or other domestic targets. Finally, DoD supports the Department of Homeland Security in executing the US Coast Guard’s lead responsibilities for maritime homeland security and law enforcement in US territorial waters.

- DoD supports civilian law enforcement and counterterrorism authorities consistent with US law. This includes providing expertise, equipment, and training facilities to domestic law enforcement when so directed. It can also include the use of US military forces to support civilian law enforcement in responding to civil disturbances, as provided in US law.
- **DoD provides critical CBRNE consequence management capabilities in support of civil authorities.** With few exceptions, DoD’s consequence management capabilities are designed for the wartime protection of the Department’s personnel and facilities. Nevertheless, civil authorities are likely to call upon these capabilities if a domestic CBRNE catastrophe occurs in the ten-year time frame of this strategy. **DoD therefore must prepare and train substantial numbers of personnel for potential employment in a domestic CBRNE consequence management mission.**



Figure 4: The Homeland Defense and Civil Support Mission Space

The Global Commons. The global commons consist of space and cyberspace, to which no nation or actor can lay claim. America's ability to defend the global commons and operate effectively from them is critical to the conduct of all US military missions, from the forward regions to the homeland. This is particularly true given our reliance on netcentric capabilities. **An active, layered**

defense requires a trustworthy information system, impervious to disabling digital attacks. Computer network defense must ensure that networks can self-diagnose problems and build immunity to future attacks. At the same time, networks must remain operational and consistently available for the execution of US military missions.



III. Strategic Goal and Key Objectives

"We must build and maintain our defenses beyond challenge. Our military's highest priority is to defend the United States . . . The threats and enemies we must confront have changed, and so must our forces."

The National Security Strategy of the United States of America

September 2002

Although the employment of an active, layered defense in the forward regions contributes significantly to homeland defense, this Strategy for Homeland Defense and Civil Support focuses particular attention on the establishment of an active, layered defense in the US homeland, its approaches, and the information domain of the global commons. In these geographic layers, the Department's activities to protect the United States generally fall into one of the following categories:

- **Lead:** DoD leads military missions to deter, prevent, and defeat attacks on the United States, its population, and its defense critical infrastructure. This includes defending the maritime and air approaches to the United States and protecting US airspace, territorial seas, and territory from attacks. The Department is also responsible for protecting DoD personnel located in US territory.
- **Support:** At the direction of the President or Secretary of Defense, the Department provides defense support to civil authorities in order to prevent terrorist incidents or manage the consequences of an attack or a disaster. Support may be requested when DoD has unique capabilities to contribute or when civilian responders are overwhelmed. DoD's

contributions to the comprehensive national response effort can be critical, particularly in the near-term, as the Department of Homeland Security and other agencies strengthen their preparedness and response capabilities.

- **Enable:** Efforts to share capabilities and expertise with domestic agencies and international partners reinforce the Department's lead and support activities. At home, the Department works to improve civilian capabilities for homeland security by lending expertise and sharing relevant technology. For example, DoD is sharing training and simulation technologies with the Department of Homeland Security, as well as unmanned aerial vehicle technologies for civilian surveillance along the Nation's borders. Abroad, the Department's security cooperation initiatives improve collective capabilities for homeland defense missions through exercises, information-sharing agreements, and formal defense agreements, such as NORAD.

To protect the United States from attack, the Department of Defense will focus on achieving five key objectives that relate to the lead, support, and enable categories. In order of priority, these objectives are:

1. Achieve maximum awareness of potential threats (Lead);
2. Interdict and defeat threats at a safe distance from the United States, and US territories and possessions (Lead);
3. Provide mission assurance (Lead);
4. Ensure DoD’s ability to support civil authorities in domestic CBRNE consequence management (Support); and

5. Improve domestic and international partner capabilities for homeland defense and homeland security (Enable).

These objectives are described in detail below. The defense capabilities required to fulfill them, summarized in the text box below, are discussed in detail in Section IV of the Strategy.

ACTIVITIES	OBJECTIVES	CORE CAPABILITIES
LEAD	<p>Achieve Maximum Awareness of Threats</p> <p>Interdict and Defeat Threats at a Safe Distance</p> <p>Provide Mission Assurance</p>	<ul style="list-style-type: none"> • Focus and orient intelligence efforts for homeland defense operations • Improve human intelligence collection and ensure comprehensive analysis and understanding of potential threats • Detect, identify, and track emerging threats in the air and maritime approaches and within US airspace • Ensure information sharing within the DoD and with domestic and international partners • Interdict and defeat national security threats in the maritime, air and land approaches and within US territory • Ensure the capability to disarm and neutralize CBRNE devices (and any explosive components) in the approaches and forward regions • Protect DoD domestic personnel and installations from CBRNE attacks • Ensure crisis management and DoD continuity preparedness • Implement a protective risk management strategy for defense critical infrastructure • Ensure preparedness of the Defense Industrial Base • Conduct protection operations for designated national critical infrastructure
SUPPORT	Support Consequence Management for CBRNE Mass Casualty Attacks	<ul style="list-style-type: none"> • When directed by the President or Secretary of Defense, assist in consequence management for CBRNE mass casualty attacks
ENABLE	Improve Relevant National and International Capabilities	<ul style="list-style-type: none"> • Improve interagency planning and interoperability • Leverage DoD expertise to enhance the US civil sector’s prevention, preparedness, response, and recovery capabilities • Enhance international partner capabilities for homeland defense and homeland security

Figure 5: DoD Objectives and Core Capabilities for Protecting the United States from Attack

Lead

Objective 1: Achieve maximum awareness of threats

To defend the Nation in the 21st century, the Department requires forewarning, as well as immediate situational awareness, of potential attacks against the United States. No longer is it sufficient to track the military movements of hostile nation states, their military aircraft and warships. In the 21st century threat environment, transnational terrorists and rogue states may employ a wide range of civilian vessels and aircraft as weapons, engage in cyber attacks, or target civilian infrastructure to achieve devastating effects.

To protect the United States in this environment, the Department of Defense, in cooperation with domestic and international partners, will seek to achieve maximum awareness of threats. By so doing, the United States increases the time available for an effective operational response. Such threat awareness is grounded in DoD's netcentric approach to operations. **Threat awareness includes: the ability to obtain comprehensive, accurate, timely, and actionable intelligence and information; exploiting relevant information and making it available to warfighters, policy makers, and others responsible for identifying and responding to threats.**

An active, layered defense requires information to flow freely regardless of operational boundaries. Relevant information may originate in one or several of the operational domains—land, sea, air, cyberspace, or space. It may originate from an array of domestic and foreign sources. To achieve maximum awareness of threats, information will be posted to DoD's Global

Information Grid, integrating operational domains and facilitating information sharing across traditional military-civilian boundaries. Using fused and shared threat awareness, our domestic and international partners and we can determine the most appropriate means to deter, interdict, or defeat threats and act accordingly.

Objective 2: Interdict and defeat threats at a safe distance

During the Cold War, the United States focused on preventing Soviet submarines, ballistic missiles, and long-range bombers from attacking the American homeland. Although concerns about traditional conventional and nuclear threats to the US homeland remain, we recognize that in the next ten years, adversaries will present a host of new challenges. They may attempt to use commercial vessels to transport terrorists or weapons to the United States. They may attempt to intrude on US airspace with low-altitude aircraft, cruise missiles, and unmanned aerial vehicles. They may attempt to convert maritime vessels, aircraft, and other modes of transportation into weapons. Through these and other means, our enemies will constantly challenge – in asymmetric ways – the security of the United States.

An active, layered defense relies on the US ability to interdict and defeat these threats at a safe distance from US territory. Transnational terrorists and other adversaries are working to exploit US vulnerabilities, conducting reconnaissance within the United States and attempting to identify patterns in our defenses. **To counter such adversary strategies, we must shift from a passive homeland defense of US territory to an active presence of forward deployed**

capabilities, designed to detect, deter, and defeat approaching threats.

In the maritime approaches, DoD is working with the Department of Homeland Security to integrate US maritime defense and to optimize the mutually supporting capabilities of the US Navy and the US Coast Guard. **As the Chief of Naval Operations has stated, “forward deployed naval forces will network with other assets of the Navy and the Coast Guard, as well as the intelligence agencies to identify, track and intercept threats long before they threaten this nation.”** This will require a level of situational awareness in the maritime domain similar to that in the air approaches. The goal of such a “maritime NORAD,” as the CNO explains, is to **“extend the security of the United States far seaward, taking advantage of the time and space purchased by forward deployed assets to protect the U.S. from impending threats.”**

In the air domain, DoD has primary responsibility for defending US airspace and protecting the United States from ballistic missiles, cruise missiles, and other aerospace attacks. For North America, this defense is carried out in partnership with Canada, through NORAD. In addition, the Department of Defense relies heavily on the Federal Aviation Administration and the Department of Homeland Security (Transportation Security Administration) for early identification of air threats. As in the maritime environment, cooperation and operational coordination with our interagency partners, as well as our neighbors and other allies, is critical to protecting the United States from air threats.

Within US territory, we face the challenge of interdicting and defeating terrorists deter-

mined to undermine the American way of life and diminish US leadership in the world. This is in marked contrast to previous periods of American history, when threats on US territory came primarily from foreign militaries, insurrectionists, and rioters. Although we must not dismiss traditional foreign military threats, in the period covered by this strategy, domestic employment of the US military in a homeland defense role will likely come in response to transnational terrorist, rogue state, or other asymmetric threats that exceed the capabilities of domestic counterterrorism and law enforcement authorities.

Therefore, the Department must approach the interdiction and defeat of threats to US territory from a joint, interagency, and, ultimately, intergovernmental perspective. DoD cannot conduct operations in separate and distinct land, sea, and air operational domains. Over the coming decade, the Department will continue to develop joint concepts of operations, working with critical interagency and international partners as appropriate.

Objective 3: Provide mission assurance

The Department cannot fulfill any of the Strategy’s key objectives without having the core capabilities in place to assure mission success. **Mission assurance, the certainty that DoD components can perform assigned tasks or duties in accordance with the intended purpose or plan, is therefore itself a key objective.** The Department of Defense’s framework for mission assurance includes a range of programs and efforts aimed at securing DoD warfighting capabilities even when under attack or after disruption. These include force protection measures, installation preparedness, information assurance,

continuity of operations, and defense critical infrastructure protection.

Force Protection and Installation

Preparedness. The Department of Defense's greatest asset is our people. Successfully executing the National Defense Strategy requires agile military forces that are trained and ready for a wide range of missions. Complementing US military capabilities are the expertise and support services provided by the Department's civilian workforce. An attack on DoD military and civilian personnel or the facilities where they work could directly affect the Department's ability to project power overseas or carry out vital homeland defense functions. Of particular concern is the threat to DoD personnel posed by domestic CBRNE attacks. To achieve an appropriate level of personnel protection on domestic bases and installations, the Department will develop and implement a comprehensive plan for protection from CBRNE attacks. In accordance with DoD responsibilities in the National Biodefense Policy, the Department is especially attentive to the unique challenges posed by biological agents.

Crisis Management and Continuity of Operations. During a homeland or other national security emergency, the Nation's leaders, including DoD decision-makers, must be able to carry out vital government functions. **The Department must provide the President and Secretary of Defense with survivable and enduring national command and control of DoD assets and US military forces.** DoD also plays an important supporting role in ensuring Continuity of Government and Enduring Constitutional Government in times of crisis. In the Cold War era, DoD continuity efforts focused on survival of senior leadership to prosecute war

in the aftermath of a massive nuclear attack. Today, DoD's crisis management efforts are broader, responsive to the full range of potential threats to the Nation. Meeting the Department's crisis management objectives requires ready DoD transportation assets, capable and survivable remote operation sites, and advanced communications capabilities throughout the DoD continuity architecture. DoD will continue to explore innovative concepts in communications and netcentric operations to improve national-level crisis management.

Critical Infrastructure Protection. The Department of Defense has the responsibility for assuring *defense critical infrastructure* as set forth in Homeland Security Presidential Directive - 7. This is defined as DoD and non-DoD cyber and physical assets and associated infrastructure essential to project and support military forces worldwide. It comprises DoD-owned infrastructures and assets and non-DoD infrastructures and assets that are critical to the execution of the National Defense Strategy. In some scenarios, assurance of non-DoD infrastructures might involve protection activities, in close coordination with other Federal, State, Local, or private sector partners. Non-DoD infrastructure categories include:

- *The Defense Industrial Base (DIB)*—The DIB provides defense-related products and services that are essential to mobilize, deploy, and sustain military operations.
- *Selected Civil and Commercial Infrastructure*—Some civil and commercial infrastructures provide the power, communications, transportation, and other utilities that military forces and DoD support

organizations rely upon to meet their operational needs.

In addition, the President or Secretary of Defense might direct US military forces to protect a third class of infrastructure:

- *Non-DoD Assets of National Significance* — The President has designated fourteen categories of non-defense Critical Infrastructures and Key Assets. Although these facilities and assets are not required for the support of DoD missions, they are so vital to the Nation that their incapacitation, exploitation, or destruction could have a debilitating effect on the security and economic well being of the United States.

Support

Objective 4: Support consequence management for CBRNE mass-casualty attacks

The Department has traditionally supported civil authorities in a wide variety of domestic contingencies, usually natural disasters. DoD typically does so using military forces and DoD capabilities designed for use in expeditionary warfighting missions. That support continues today. The level and type of traditional defense support of civil authorities does not impede DoD's ability to execute other missions specified in the National Defense Strategy.

The 21st century terrorist threat environment has fundamentally altered the terms under which Department of Defense assets and capabilities might be called upon to support civil authorities. **The potential for multiple, near simultaneous, CBRNE attacks on US territory is real.** The Department will

therefore focus on that portion of the threat spectrum where DoD has unique capabilities to bring to bear. In particular, in an environment where terrorists endeavor to inflict mass casualties by employing CBRNE means, it is imperative that the Department of Defense be prepared to support civilian responders.

Support to domestic authorities for consequence management is a core element of active, layered defense within the US homeland. The Department of Defense maintains considerable CBRNE recovery expertise and equipment. When directed by the President or Secretary of Defense, DoD will employ these capabilities to assist the Secretary of Homeland Security, the principal federal official for domestic incident management, or other domestic authorities. **DoD must be prepared to support its interagency partners in responding to a range of CBRNE incidents, including multiple, near simultaneous mass casualty attacks within the United States.**

Enable

Objective 5: Improve national and international capabilities for homeland defense and homeland security

Enabling better national capabilities for homeland security missions is an important complement to DoD's lead and support activities. The broad range of threats posed by terrorists and other transnational actors has expanded our traditional, concept of national security. In the past, the Department of Defense could largely fulfill its responsibility for protecting the nation by integrating its activities with the Department of State and the Intelligence Community. Today, the expertise and corresponding responsibility

III. Strategic Goal and Key Objectives

for managing 21st century security challenges is much more widely shared among federal departments and agencies. State, local, and tribal authorities, the private sector, and our allies and friends abroad are also critical contributors to US national security.

In such an environment, DoD must unify its efforts with those of its key interagency partners and international friends and allies to ensure the nation's security. Sharing technology, capabilities, and expertise strengthens the nation's ability to respond to hostile threats and domestic emergencies. Congress recently concluded that DoD's contributions to the counter-drug mission could have great relevance to the defeat of terrorist movements across our borders. As a result, Congress passed legislation allowing DoD joint task forces the ability to support law enforcement in counter-terrorism activities, in addition to their current capability to support counter-drug activities.

In turn, DoD can readily leverage the expertise of other federal, state, and local authorities and international partners to improve its own capabilities for counterterrorism, maritime interdiction, and other missions critical to an active, layered defense. **As the Department's first priority, homeland defense must be a central, carefully considered element of our defense-to-defense relationships with key allies and friends abroad.** The United States fosters strong defense relationships worldwide for many reasons of national security interest. Two such reasons are to strengthen allied military contributions to collective security and to enhance US capabilities through exposure to partners' expertise. Thus, DoD has an active security cooperation program, directed through the Secretary of Defense's

Security Cooperation Guidance that encourages mutual improvements to support coalition operations and to ensure continued interoperability. Clearly, our homeland defense can be substantially strengthened through the cooperation and assistance of international allies.

Effective security cooperation contributes substantially to operations in all layers of an active, layered defense, particularly in the forward regions and the approaches to the United States. The US-Canadian experience in NORAD is an outstanding example of how such cooperation can foster meaningful and mutual improvements in homeland defense. **The Department of Defense will seek to build on the NORAD concept and pursue additional opportunities for bi-national and multi-national homeland defense mechanisms wherever possible.** Expanded cooperation with Mexico is particularly important in this regard.

The United States also benefits from more modest cooperative ventures. The expansion of information and intelligence sharing with neighbors, allies, and other friendly nations is critical to the success of this Strategy. Allies often possess significant information relating to counterterrorism, smuggling, and other US concerns. Incorporating this information into our base of knowledge could significantly improve US readiness both for homeland defense and civil support missions.

The Department of Defense, and especially geographic combatant commanders, will therefore ensure that US homeland defense concerns are at the forefront in defense interactions with allies and friends throughout North America, South America, the Pacific, Europe, and elsewhere. We will focus particular attention on our North

American neighbors, Canada and Mexico,
who share our borders and a strong mutual
interest in homeland defense and civil
support.



IV. Core Capabilities

"Some believe that, with the U.S. in the midst of a dangerous war on terrorism, now is not the time to transform our armed forces. I believe that quite the opposite is true. Now is precisely the time to make changes. The impetus and the urgency added by the events of September 11th powerfully make the case for action."

*Secretary of Defense Donald Rumsfeld
January 31, 2002*

The Department of Defense will provide the homeland defense and civil support capabilities necessary to support implementation of the National Security Strategy, the National Strategy for Homeland Security, and the National Defense Strategy. Over the next ten years, DoD will protect the United States from attack by focusing on the core capabilities necessary to achieve each of the key objectives detailed in Section III.

Capabilities for Achieving Maximum Awareness of Threats

Core Capability: Focus and orient intelligence efforts on homeland defense operations

Protecting the United States against the full range of 21st century threats requires the US Intelligence Community to restore its human intelligence capabilities, reprioritize intelligence collection to emphasize probable homeland defense threats, and invest in new deep penetration, long-dwell, and moving target detection capabilities. In the Cold War, we knew both the nature of the threat to our country and the source of that threat. Today, intelligence and warning must extend beyond conventional military and strategic nuclear threats to cover a wide range of other state-

and non-state challenges that may manifest themselves overseas or at home.

The Intelligence Community is adjusting to this changing strategic landscape to meet the Nation's homeland security needs. The establishment of the interagency Terrorist Threat Integration Center (TTIC), the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate, and the DoD's Joint Intelligence Task Force for Combating Terrorism (JITF-CT) exemplify this shift. Further, the President's August 2004 announcement of the creation of a National Intelligence Director and Executive Orders for strengthened management of the Intelligence Community and the establishment of a National Counterterrorism Center (NCTC) also ensure a more collaborative, comprehensive approach to intelligence support for national security. While these changes are taking place, the Department will reorient DoD intelligence capabilities in line with the full range of homeland defense priorities. Specifically, the Department will:

- Focus on integrated collection management and its application to homeland defense;
- Better utilize national intelligence assets and capabilities to collect global information on threats to the US

homeland and provide for early warning and tracking;

- Provide continuous, persistent, and on-demand intelligence;
- Collect homeland defense threat information from relevant private and public sector sources, consistent with US privacy law;
- Enhance remote detection of emerging or existing CBRNE threats and adapt sensors to better meet homeland defense requirements; and
- Develop automated tools to improve data analysis and management, in order to systematically track large amounts of data, and to detect, fuse, and analyze aberrant patterns of activity, consistent with US privacy protections.

Core Capability: Improve human intelligence collection and ensure a comprehensive analysis and understanding of potential threats

Improving our understanding of America’s foreign enemies—in advance of an attack—is at the heart of DoD’s efforts to achieve

maximum awareness of potential threats. In accordance with the National Strategy for Combating Terrorism (2002), we are strengthening DoD’s knowledge of foreign terrorist networks and the inner workings of their operations.

Improved human intelligence, particularly in the forward regions of the world, is the single most important factor in understanding terrorist organizations. As discussed in the Homeland Defense Intelligence Objectives below, the Department of Defense is currently undertaking a focused review of DoD human intelligence capabilities, including reforms to improve HUMINT policies, practices, and organizations. In addition, we will **develop a cadre of specialized homeland defense and terrorism intelligence analysts within the defense intelligence community** and deploy these analysts to interagency centers for homeland defense and counterterrorism analysis and operations. DoD will also ensure that these analysts and defense intelligence operators have relevant linguistic, cultural, and analytic skills. Additionally, the Department will invest in automated collaborative analysis tools, predictive models, and tools that help policymakers and

Homeland Defense Intelligence Objectives

- Redirect and expand our current strategic intelligence capabilities to include a complete understanding of all threats to and vulnerabilities of the homeland with an emphasis on building our HUMINT capability
- Develop a strategic competency for Homeland Defense warning that allows us to defeat the spectrum of 21st century threats
- Create a intelligence system agile enough to prepare for surprise attacks on the homeland and rapidly and decisively defeat emerging threats
- Build a system robust enough to support an agile global posture of forward deterrence and defense, providing greater lead time to meet and defeat threats before they reach the homeland
- Ensure that adversaries and future technological developments do not compromise US technology, information systems, and operations supporting Homeland Defense

operators to put threats in the context of transnational terrorism and domestic vulnerabilities, to include critical infrastructure protection.

Core Capability: Detect, identify, and track objects in the air and maritime approaches and within US airspace

We face challenges in our ability to detect, identify, and track objects in all operational environments, but especially the air and maritime domains. Every day, thousands of US and foreign vessels and aircraft approach and depart American ports and airports and those of our closest neighbors. The sheer volume of cargo and diversity of passengers is challenging.

Detecting and tracking anticipated air and maritime threats requires the effective forward deployment of advanced technologies and existing capabilities to cue, surveil, identify, engage, and assess potential threats in real time. Detection and tracking capabilities must be all-weather, around-the-clock, and effective against moving targets. The United States must also have the ability to detect CBRNE threats emanating from any operating environment. **This requires a comprehensive, all-domain CBRNE detection architecture, from collection to analysis.**

The maritime picture is multi-jurisdictional, with various US agencies responsible for tracking vessels from their departure at foreign ports to their arrival in the United States. Recognizing the potential vulnerability this situation creates, DoD is working closely with interagency partners, especially the United States Coast Guard, to establish a unified concept for maritime domain awareness (MDA)—the effective

understanding of the global maritime threat environment (on, below, and above the sea), and its potential impact on the security, safety, economy, and environment of the United States.

Based on the emerging MDA concept, the Department of Defense will work with interagency partners to develop a comprehensive intelligence, surveillance, and reconnaissance capability to detect threats as far forward of the US homeland as possible, ideally before threat vessels depart foreign ports. **DoD will ensure persistent wide-area surveillance of the US maritime approaches, layered and periodically varied in such a manner that an adversary cannot predict or evade observation.** Surveillance will also be long-range in all dimensions—above, below, and on the ocean’s surface. DoD will benefit from the Department of Homeland Security’s work to institute worldwide cargo and crew reliability mechanisms. Finally, DoD, again in concert with the Department of Homeland Security, will receive and share data from improved identification systems for small commercial and other vessels. The United States has recently employed such a system for maritime vessels weighing over 300 tons.

Achieving threat awareness in the air operational domain presents similar challenges. Throughout the Cold War, the Department of Defense focused on maintaining awareness of external threats that entered US airspace from overseas. The attacks on September 11, 2001, however, originated in US airspace, highlighted weaknesses in domestic radar coverage and interagency air defense coordination.

Since the attacks of September 11, 2001, DoD has coordinated with interagency partners to significantly improve the air

defense of the United States. DoD has worked with the Federal Aviation Administration (FAA) to integrate domestic radar coverage, and has conducted Operation Noble Eagle air patrols to protect designated US cities and critical assets. Particular emphasis has been placed on implementing a robust air defense capability for the National Capital Region, using both air and ground air defense forces. DoD has also worked closely with interagency partners to exchange a wide range of information regarding potential threats.

The security environment projected for the next decade points to continued state-sponsored and transnational terrorist threats to domestic air security. Rogue state and non-state actors could threaten the United States with manned or unmanned air vehicles. Air threats could originate externally or within US territory. Additionally, adversaries might maintain low altitude flight profiles, employ stealth and other defense countermeasures, or engage in deception to challenge US air defenses. Though substantial, the requirements for domestic air defense are achievable.

In the air, the Department of Defense will work with domestic and international partners to develop a persistent, wide-area surveillance and reconnaissance capability for the airspace within US borders, as well as for the nation's land and maritime approaches. This capability requires the development of advanced technology sensors to detect and track low altitude air vehicles across a wide geographic area. For example, DoD is currently conducting an Advanced Concept Technology Demonstration for High Altitude Airships. If proven effective, High Altitude Airships or other similar platforms could provide the basis for an over-the-

horizon engagement capability, to detect enemy threats in the approaches or over US territory, enabling their defeat. The United States and our allies must also integrate sensor and intelligence data to identify hostile air vehicles by observing their performance characteristics, suspicious activities, or other attributes. These capabilities in the air domain will provide timely threat detection, extending the depth of air defenses and the time for response, thereby providing multiple engagement opportunities to defeat identified threats.

Core Capability: Ensure shared situational awareness within DoD and with domestic and foreign partners

Shared situational awareness is defined as a common perception of the environment and its implications. All domestic and foreign partners within the homeland defense mission space require situational awareness for three reasons: to identify threats as early and as distant from US borders as possible; to provide ample time for an optimal course of action; and to allow for a flexible operational response. From the March 2003 Homeland Security Information Sharing Memorandum of Agreement to the aggressive and unprecedented information sharing underway at the interagency Terrorist Threat Integration Center, the US Government continues to make great strides in overcoming obstacles to shared situational awareness.

During the Cold War, the Department of Defense sought shared situational awareness with the Department of State, the Intelligence Community, and allied nations in order to deter and defeat threats posed by the Soviet Union and other nations. At the same time, the American law enforcement community worked with its international counterparts to

thwart international drug cartels and a growing number of worldwide crime syndicates.

Today, transnational terrorists have blurred the traditional distinction between national security and international law enforcement. Together with a significant proliferation in the number and type of potential foreign threats, **this expanded national security challenge necessitates an unprecedented degree of shared situational awareness among federal agencies and between the United States and its key foreign partners.**

As a first step, the Department of Defense must provide seamless connectivity and timely, accurate, and trusted information to all DoD components—any time, any place—in order to achieve maximum awareness of potential attacks against the United States. As indicated previously, to facilitate this connectivity, information technology systems, services, and facilities in DoD’s information technology and intelligence communities must communicate effectively. The Department will therefore ensure that DoD’s information infrastructure provides an integrated, interoperable worldwide network of information technology products and management services. This will allow users across DoD to process information and move it to warfighters, policymakers, and support personnel on demand. Network connectivity must be flexible enough to support global operations while allowing for local requirements and innovation. **It must also create a real-time link between sensors, decision makers, and warfighters to facilitate the rapid engagement of enemy targets.**

Beyond building an integrated information infrastructure, DoD must also populate that

network with accurate, timely, and actionable data. Today, information relevant to protecting the United States is widely dispersed. The Department, in concert with the intelligence and law enforcement communities and foreign partners, will build on the great strides already made to diminish existing cultural, technological, and bureaucratic obstacles to information sharing. **The Intelligence Community and Department of Defense will drive improved information sharing within a “need to share,” not a “need to know” context.** The resulting information exchange, commonly referred to as “horizontal integration of intelligence,” will provide analysts across the US government and partner nations with timely and accurate all-source information, vastly improving the creation of a coherent and fully integrated threat picture. Such an expansion in information sharing requires appropriate safeguards to ensure that DoD intelligence components rigorously apply laws that protect Americans’ civil liberties and privacy.

Capabilities for Interdicting and Defeating Threats at a Safe Distance

Active, Layered Defense across all operational domains. The Department of Defense must provide an active, layered defense that encompasses the global battlespace and fully integrates maritime, air, and land operational domains. **This proactive defense begins with the forward regions, seamlessly transitions through the approaches to the American homeland, and concludes with the domestic transfer of lead responsibility to the Department of Homeland Security.** This includes, if

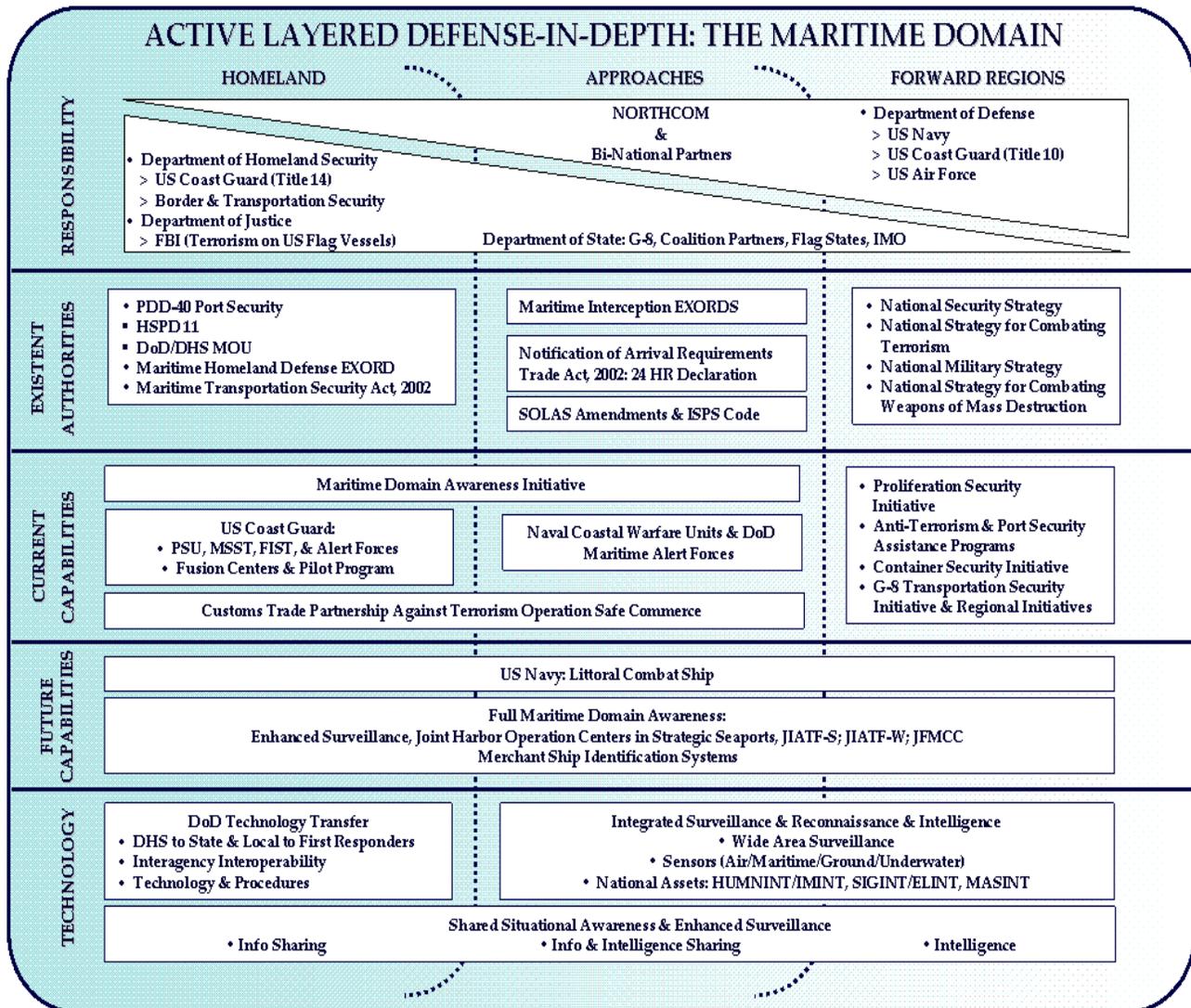
necessary, the lawful and effective use of military forces to interdict and defeat threats on US territory, when directed by the President or Secretary of Defense.

Core Capability: Interdict and defeat national security threats in the maritime, air, and land approaches and within US territory

Maritime Operational Domain. We must fully integrate our surface, subsurface, air, and surveillance assets, focus them forward, and extend the Nation’s maritime defensive perimeter further out to sea in order to deter and defeat maritime threats at a safe distance

from the US coast. This requires improvements in shared situational awareness to link operational and tactical levels. **Awareness must support an effective maritime intercept operations (MIO) capability tailored to the demands of the 21st century threat spectrum, most especially the foreseeable threat of transnational terrorists, detected on the high seas, armed with weapons of mass destruction.**

Enhancing our ability to interdict enemies in the maritime domain requires a seamless system of overlapping defenses—both adaptable and flexible—to frustrate enemy observation and avoid predictability. This



IV. Core Capabilities

begins in the forward regions with improved surveillance capability, increased HUMINT collection, and enhanced international partnerships through programs like the Container Security Initiative and Proliferation Security Initiative. We must also successfully exploit the cyber domain in order to focus and enhance our maritime capabilities. **To maximize maritime domain awareness, successive layers of surveillance must be fully coordinated with the operational activity of our forward deployed forces.**

Consistent with applicable law, and working with domestic and international partners, we will systematically interdict high interest vessels in the maritime approaches. DoD has established standing orders for conducting maritime homeland defense and maritime interdiction operations. Given this guidance, geographic combatant commanders will include interdiction exercises in their theater security cooperation plans and conduct such exercises on a periodic basis. The US Navy and US Coast Guard will conduct routine and frequent maritime interdiction exercises to ensure a high state of training and readiness.

To interdict and defeat transnational threats, the Department of Defense and Department of Homeland Security must have a predetermined process for ensuring rapid, effective US Coast Guard support to the US Navy and vice versa. Although DoD has the lead role in defending the United States from external maritime attack, we recognize the US Coast Guard's lead responsibility for maritime law enforcement and homeland security. We will continue to support the US Coast Guard in fulfilling its homeland security responsibilities. Together with the US Coast Guard, we must build upon the security in our ports and littorals, expanding maritime defense capabilities further

seaward. **This includes strengthening the 96-hour notice of US arrival requirement by including a "consent to board" provision as a prerequisite for entry into a US port.**

Routine assignment of naval forces to US Northern Command for the performance of its maritime defense mission is imperative. DoD will consider the designation of US Naval Reserve forces to undertake unique roles in maritime homeland defense. In addition, the US Navy can assess the integrated benefit of forces currently available in support of Operation Noble Eagle, available coastal patrol craft, and the utility of the Navy's littoral combat ship to execute the maritime homeland defense missions. The US Navy's new generation of littoral combat ships has outstanding potential as a platform for maritime interdiction operations and other homeland defense missions.



Figure 6: Littoral Combat Ship

DoD forces conducting maritime interdiction operations must have advanced capabilities, to include non-lethal weapons for boarding parties, deployable sensor capability for CBRNE detection, and an integrated and comprehensive hull to emitter correlation (HULTEC) database to enhance identification of potential threat vessels. During permissive searches, boarding parties will minimize the display of lethal force while maximizing their CBRNE interdiction capability.

Finally, DoD must continually seek to address new, unpredictable maritime threats by utilizing academic institutions and interagency organizations that have developed competencies in maritime intercept operations and domain awareness. Examples include the Naval Postgraduate School, the Naval War College, the Joint Interagency Task Force-South, and the National Maritime Intelligence Center.

Air Operational Domain. The Department of Defense will defeat air threats to the United States, such as ballistic and cruise missiles and attacking military aircraft. DoD must also be prepared to interdict non-traditional air threats, even when the intent to harm the United States is more uncertain, as initially occurred on September 11, 2001. These threats could include commercial or chartered aircraft, general aviation, ultra light airplanes, unmanned aerial vehicles, radio controlled aircraft, or even balloons. Early detection and successful interdiction of these types of potential threats requires very close cooperation with DoD's interagency partners.

Since September 11, 2001, the Department of Defense, through Operation Noble Eagle, has conducted combat air patrols to protect major US population centers, critical infrastructure, and other sites. Working with our inter-agency partners, DoD will continue these patrols to intercept air threats to the US homeland as long as required by the projected threat. In addition, DoD will enhance our capability to defend against low-altitude air threats, particularly cruise missiles. Finally, the initial operational capability of the US ballistic missile defense system, forthcoming this fall, will afford additional protection in the air operational domain.

The integrated air defense of the National Capital Region (NCR) is an excellent example

of ongoing DoD and interagency efforts to protect a major US population area and associated critical infrastructure.

Within the NCR, the Federal Aviation Administration is usually the first organization to identify deviations in expected flight patterns. To provide the level of certainty necessary to make lethal interdiction decisions in the National Capital Region, NORAD works with the Federal Aviation Administration and the Department of Homeland Security's National Capital Region Coordination Center to identify potential threats and establish their intent. The Coordination Center provides law enforcement information about the background and possible intent of air targets of interest. DoD then works within a layered, interagency approach to provide threat interdiction. DoD provides the base layer of defense through ground-to-air defense units. The Department of Homeland Security's Bureau of Immigration and Customs Enforcement provides helicopters to interdict low-altitude, slow flying aircraft. Finally, the Department of Defense provides combat fighter aircraft as a top layer of defense. A similar layered air defense approach is used during selected special events across the United States.

DoD's approach to improving our air defense capabilities within the United States is multifaceted. First, the Department continues to work with interagency and multinational partners to enhance the layered air defense described above. For example, DoD is working in partnership with the Department of Homeland Security to investigate the establishment of a Homeland Air Security Coordination Center (HASCC). The HASCC would integrate information from throughout the interagency relating to potential air

threats and help coordinate efforts to prevent or respond to attacks.

Second, **the Department of Defense will continue to improve the air-to-air and ground-to-air capabilities and associated forces necessary to interdict and defeat all domestic air threats.** For combat air patrol missions, DoD will use more capable aircraft as they are fielded, such as the F/A-22 and F-35, and explore the potential for employing unmanned combat air vehicles. DoD is also upgrading ground-based air defense assets with improved detection and targeting capabilities.

Third, **DoD must be able to defend the United States against cruise missile attack.** Defense against cruise missiles poses unique challenges, given that their low-altitude and smaller size make them more difficult to identify and track than traditional air threats. The Department of Defense is developing integrated capabilities to defend against cruise missiles, as well as other types of unmanned aerial vehicles. As an interim step, DoD is developing a deployable air and cruise missile defense capability to protect designated areas. This will integrate Service tactical air defense assets, the NORAD air defense system, interagency information sources, and advanced technology sensors. **Future air and cruise missile defense assets will be fully interoperable and increase the size of the defended area as well as engage threats at increased range.**

Finally, technology initiatives drive the long-term success of US air interdiction and defense capabilities. DoD must continue to work with interagency partners to develop a common air surveillance picture that will enhance our ability to identify and, ultimately, defeat enemy targets. Improved

sensors are also required to detect and track potential air threats within the United States. The current radars maintained by the Federal Aviation Administration to track air traffic within the United States are aging, with high maintenance costs, poor reliability, and reduced capability to track emerging threats. **DoD is working with the Federal Aviation Administration and the Department of Homeland Security to develop advanced, follow-on sensors to the current generation of radars in order to improve tracking and identification of low-altitude threats.** The Over-the-Horizon Radar (OTHR), Joint Land Attack Elevated Netted Sensor (JLENS), and the High Altitude Airship are examples of systems that could detect and track these types of threats within the United States.

Land Operational Domain. Protection of US territory from ground-based attacks is integrated into the Department of Defense's concept of an active, layered defense. The nation must work closely and cooperatively with our neighbors to the north and south, establish seamless relationships and organizational structures with interagency partners, and be prepared to respond with military forces quickly, responsively, and in a manner coordinated with civilian law enforcement agencies to ensure terrorists, are deterred and defeated on our own soil.

Historically, the United States relied, almost exclusively, on forward-deployed forces to confront and defeat nation-state adversaries overseas. While power projection remains crucial, transnational terrorism has significantly reduced the effectiveness of this singular approach. Now and in the future, we must be prepared in every domain—most especially the US homeland—to deter, prevent, and defeat terrorist or other asymmetric threats. **An effective land**

defense strategy requires a seamless, interagency, and international approach to border security; and a clear recognition that the nation's local, state, and federal law enforcement are the lead agencies for domestic counterterrorism.

In the post-Cold War era, a cornerstone of the United States' national security strategy has been coordinated security cooperation relationships with allies and partners. Security cooperation programs and activities serve to advance US objectives, establish bi-lateral and multi-lateral relationships conducive for combined operations, and enhance the military capabilities of our allies and partners.

Interdiction and defeat of ground-based threats on US territory begins with robust, well-coordinated security cooperation relationships with our neighbors Canada and Mexico. Security cooperation efforts address our mutual security interests and the resulting synergy will ensure the land-based defenses of all three nations are more effective.

Within the US, by law and national policy, DoD's roles in the land domain are significantly more circumscribed than in the air and maritime domains. In addition to private security provided by the domestic property owner, a three-tiered approach exists to interdict and defeat threats on US territory.

Tier 1: Local and federal law enforcement. State, local, and federal law enforcement agencies are the primary responders to defeat terrorist threats within US territory. When directed by the President or the Secretary of Defense, DoD will provide appropriate defense assets in support of domestic law enforcement authority,

normally in support of a lead federal agency such as the FBI. Under these circumstances, military forces and assets will remain under the command and control of a DoD authority.

Tier 2: National Guard forces responding in State and Title 32 status. Historically, the National Guard has served two-major roles—as (1) a strategic reserve in the event of war or major overseas contingency and (2) support of its state in times of natural disasters or civil disturbance. When directed by the Governor or appropriate state authority, National Guard forces and assets can respond quickly to interdict and defeat terrorist threats on the ground.

Operating under either State Active Duty or Title 32 status, National Guard forces can provide support to civilian law enforcement authorities in two key areas. First, National Guard counternarcotics efforts can enhance the effectiveness of counterterrorism initiatives through information-sharing, logistics support, and combined operations. Second, by virtue of their status under state law and Title 32 of US Code, National Guard forces provide civilian authorities with a flexible option under the Military Support for Civilian Law Enforcement Agencies (MSCLEA) construct.

Expanded authorities under a revised Title 32—and the National Guard's on-going transformation into a truly 21st century force—will provide Governors and state authorities with flexible, responsive, multi-capable units to deter and defeat localized terrorist attacks. For example, National Guard reaction forces—scalable in terms of size and mix of

skills—can provide security for critical infrastructure, support civilian law enforcement agencies in responding to terrorist acts, and offer their neighbors immediate assurance of safety and security.

Tier 3: US military forces responding to Presidential direction. If circumstances warrant, the President or Secretary of Defense may direct military forces and assets to interdict and defeat threats on US territory. **When conducting land defense missions on US territory, DoD does so as a core, warfighting mission, fulfilling its constitutional and statutory obligation to defend the nation.** To fulfill this responsibility, DoD will ensure the availability of appropriately sized, trained, equipped, and ready quick reaction forces (QRFs) and rapid reaction forces (RRFs). The QRFs/RRFs will employ a mix of Active and Reserve Component assets, assigned on a rotating basis. Domestic employment of military forces is uniquely constrained consistent in a manner with American history, culture, and laws, most notably the Posse Comitatus Act (18 USC 1385). However, when employing US military forces in a warfighting mission within the US, the “military purpose doctrine” recognizes that the purpose of this activity is distinct from traditional law enforcement and independent of the constraints of the Posse Comitatus Act. The purpose, in short, is not to engage in law enforcement but rather to militarily defeat our enemies.

Minimizing potential civilian casualties is critical in the execution of DoD’s homeland defense mission. Today, the Department has a limited range of weaponry to engage terrorists located in close proximity to

population centers or domestic infrastructure. **Non-lethal capabilities can provide commanders with the more precise and tailored use of force required for domestic land defense.** The Department will continue to examine and advance our non-lethal and less-than-lethal capabilities to support foreseeable land missions against foreign adversaries, which may be conducted in close proximity to US civilians. DoD will also work with the National Guard Bureau and the law enforcement community to develop and share expertise regarding doctrinal employment of non-lethal capabilities.

Capabilities for Providing Mission Assurance

Core Capability: Protect DoD domestic personnel and installations from CBRNE attacks

Effective mission assurance will identify mission critical nodes, vulnerabilities of that node, and the mission impact should that node be degraded or eliminated. Appropriate actions can then be taken to test the known vulnerabilities against the full spectrum of potential threats: transnational terrorism, nation-state, domestic, manmade-hazards, and natural disasters. Understanding the mission impact, the vulnerability, and the threat will support risk management decisions.

Therefore, improving DoD’s capabilities for mitigating and, if necessary, operating in a CBRNE-contaminated environment will require progress in detecting and identifying threats (sense), providing early warning (shape), protecting forces and installations (shield), and ensuring the ability to operate in a contaminated environment (sustain).

Sense. DoD currently has a range of capabilities to detect, identify, and quantify airborne, waterborne, and other hazards. Needed improvements include advanced standoff and point detection capabilities for chemical and biological threats. DoD is also working to develop and field standoff detection capabilities for explosives. Advances in standoff detection capability will enhance the Department's ability to detect nuclear devices as well as weapons using explosives to disperse chemical, biological, and radioactive materials. Finally, the Department is improving medical surveillance capabilities to provide early detection and identification of CBRN events in the workforce.

Shape: DoD characterizes CBRN attacks by assimilating information drawn from sensors and elsewhere to inform commanders of impending or approaching threats. The Department is continuing to improve on early CBRN threat characterization by developing an integrated concept of operations for sensing, reporting, and warning of CBRN attacks, ensuring compatibility with national-level CBRN sensor architectures currently in operation, such as BIOWATCH, and those under development.

Shield: The Department will continue to provide force protection in advance of a potential CBRNE attack, whether overseas or at domestic installations. Already, 750,000 US military personnel have been vaccinated against anthrax; 650,000 are vaccinated against smallpox. The Department is now focusing on the development of vaccines and other capabilities that can address new and

emerging biological and chemical threats. DoD is also preparing to field capabilities that protect US forces from chemical agents that can be absorbed through the skin.

Lastly, the Department is deepening and expanding collaboration on biodefense research with the Department of Homeland Security and the Department of Health and Human Services. This includes significant investments by these civilian agencies in biodefense research and the creation of a new research consortium. The construction of a National Interagency Biodefense Campus, collocated with the US Army Medical Research Institute of Infectious Diseases (USAMRIID), will significantly facilitate civil-military cooperation in this area. A revitalized and recapitalized USAMRIID, along with major Department of Homeland Security and Department of Health and Human Services investments, will provide DoD and the Nation with added research capacity, additional biopharmaceutical development, increased testing and evaluation of potential biodefense medical products, and large surge lab capacity for bioterrorism incident response.

Sustain: DoD must be able to sustain operations during and after a CBRNE attack in the United States. Medical therapeutics that allow DoD personnel to continue mission-essential tasks in a CBRNE environment are of highest priority. DoD will also expand pilot programs for CBRNE installation preparedness to protect DoD personnel and facilities in the event of an attack. The Department is currently preparing 200 critical installations in the United States

and abroad against CBRNE attacks. The Department will aggressively expand the scope of this installation preparedness program, increasing both the level of protection and the number of DoD installations it covers.

The Department is working on all areas of CBRNE preparedness, but defense against biological weapons is of particular importance. DoD's efforts fully support all aspects of the President's *National Biodefense Policy* (2004): threat awareness, prevention and protection, surveillance and detection, and response and recovery.

Core Capability: Ensure crisis management and DoD continuity preparedness

The Department's crisis management and continuity of operations programs are central to mission assurance. DoD must provide capabilities necessary to support senior leadership decision-making and military command and control and to perform essential DoD functions to support national-level crisis managers. DoD is working to enhance its information management and communications capabilities to support senior leadership in crises. It is also improving the survivability and flexibility of military command and control capabilities.

A significant element of mission assurance is **continuity of operations**—maintaining the ability to carry out DoD mission essential functions in the event of a national emergency or terrorist attack. Fulfilling this objective in the current security environment necessitates new and innovative approaches. Some of these approaches include policies for personnel dispersion, leveraging advances in information technology to improve crisis

coordination, and improving relocation facilities. The Department recently conducted a zero-based assessment of DoD continuity capabilities. The results of this assessment detail numerous capability improvements that the Department can pursue in order to ensure the continuity of DoD operations in times of crisis. It also provides recommendations that will transform DoD's approach to continuity operations from a Cold War-oriented operational concept to one better suited to address the current and evolving terrorist threat. The recommendations include the use of new and emerging technologies and the development of more flexible relocation options.

Core Capability: Implement a protective risk management strategy for defense critical infrastructure

Because resources are constrained, uniform protection of all defense critical infrastructure is not possible. **The Department must prioritize the protection of assets based on their criticality to executing the National Defense Strategy** through the Defense Critical Infrastructure Program Integrated Risk Management Strategy (2004). The strategy's goal is to minimize the vulnerability to and impact of critical asset failures or disruptions by:

- Identifying infrastructure critical to the accomplishment of DoD missions, based on a warfighter mission area analysis.
- Assessing the potential effect of a loss or degradation of critical infrastructure on DoD operations. Assessments are conducted to determine specific vulnerabilities especially from terrorist attack. Vulnerability and antiterrorism force

protection assessments have been completed for hundreds of CONUS bases, and the Department is developing new standards for use in future assessments.

- Managing the risk of loss, degradation, or disruption of critical assets through remediation or mitigation efforts, such as changes in tactics, techniques, and procedures; minimizing single points of service; and creating appropriate redundancies, where feasible.
- Providing physical protection when directed by the President, in the case where the nature of the threat exceeds the capabilities of an asset owner and civil law enforcement.
- Enabling real-time incident management operations by integrating current and emerging threat monitoring and reporting with existing critical infrastructure network data and analysis through the Mission Assurance Support Center within the Defense Program Office for Mission Assurance.

The Services, Defense Agencies, and other DoD components are now implementing the Protective Risk Management Strategy through modifications to their programs and budgets.

Core Capability: Ensure preparedness of the Defense Industrial Base

The 2003 National Strategy for the Physical Protection of Critical Infrastructure and Key Assets currently notes that the Department of Defense relies heavily on the private sector defense industry. **Without the important contributions of the private sector, DoD**

cannot effectively execute core defense missions. Private industry manufactures and provides the majority of the equipment, materials, services, and weapons for the US armed forces. Ensuring that military forces are properly equipped is critical to maintaining DoD power projection and homeland defense capabilities. In that regard, the President recently designated DoD as the Sector-Specific Agency for the Defense Industrial Base. **In this role, DoD is responsible for national infrastructure protection activities for critical defense industries as set forth in Homeland Security Presidential Directive - 7.** This includes:

- Collaborating with all relevant federal departments and agencies, state and local governments, and the private sector;
- Conducting or facilitating vulnerability assessments of the Defense Industrial Base; and
- Encouraging protective risk management strategies to prevent, and mitigate the effects of, attacks on the Defense Industrial Base.

DoD is aggressively fulfilling these assigned responsibilities to address vulnerabilities in the Defense Industrial Base. Preventing the loss of critical assets that are single points of failure is the top priority. To assure that mission critical supplies/services are available, DoD contracts are being modified to ensure that appropriate protective measures are in place at key facilities and appropriate information is shared with the DoD to assess the security of the DIB. In addition, the Defense Logistics Agency and other DoD contracting activities are revising the contract process to ensure that civilian defense contractors are able to operate for the

duration of a national emergency. **Defense contractors must be able to maintain adequate response times, ensure supply and labor availability, and provide direct logistic support in times of crisis.** Contracts will also require DoD program managers to be accountable for ensuring the protection of supporting infrastructure, including key suppliers. DoD base and installation commanders, and those who contract for non-DoD infrastructure services and assets, will monitor assurance activities through compliance with contract language that clearly identifies reliable service availability, priority of restoration, and asset protection.

Core Capability: Conduct protection operations for designated national critical infrastructure

The Department has historically focused on preventing unauthorized personnel from gaining access to DoD installations and protecting those installations from traditional military attacks. Throughout the 20th Century, the United States took measures to provide for the quick and effective mobilization of the Defense Industrial Base, including protection from acts of sabotage. **In the post September 11, 2001 era, DoD is expanding the traditional concept of critical asset protection to include protection from acts of transnational terrorism.** Countering terrorist reconnaissance activity is central to the successful defense of critical infrastructure. This strategy also anticipates that adversaries may attempt to convert aircraft, land vehicles and maritime vessels, or other civilian infrastructure into weapons that could strike critical targets. Therefore the department must prevent enemies from employing CBRNE materials or weapons to cause mass

panic, contamination, or substantial loss of life.

As outlined in the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, DoD pursues a multifaceted approach to critical infrastructure protection:

- **DoD Infrastructure.** The Department bears primary and ultimate responsibility for protecting DoD assets, infrastructure, and personnel. At the Department's request, domestic law enforcement may assist with protection functions.
- **Non-DoD Infrastructure.** DoD's infrastructure protection role is more limited for non-DoD assets. This includes both defense critical infrastructures—such as in the Defense Industrial Base or Selected Civil and Commercial Industry—and non-defense critical infrastructure.

The initial responsibility for protection of this infrastructure rests with the owners who employ active and passive measures designed to meet DoD protection requirements, in the case of defense critical assets, or Department of Homeland Security standards, in the case of other National Security Assets. **Civilian law enforcement authorities augment and reinforce the efforts of asset owners,** creating a second tier of protection.

The growing sophistication of the transnational terrorist threat will, at times, make these first two layers of protection inadequate.

Should protection requirements exceed the capabilities of asset owners and civilian law enforcement, state authorities provide a third tier of defense. In addition to a governor's authority to employ National

Guard forces in a state active duty status, Title 32 of US Code provides an additional means to quickly mobilize National Guard forces under the control of the governor using federal funding to defeat a foreign terrorist threat. Therefore, the Department of Defense is working in collaboration with Congress and the National Guard Bureau to expand Title 32 authorities in order to allow National Guard forces to conduct a wider range of national security operations while in this status.

To achieve critical infrastructure protection in the most serious situations, the Department of Defense maintains trained and ready combat forces for homeland defense missions. These include air assets capable of conducting combat air patrols over selected sites, naval forces to provide close-in protection against air and maritime threats, and ground-based rapid reaction forces to counter terrorist or other threats to defense critical or national security infrastructure.

Capabilities for CBRNE Consequence Management

Core Capability: When directed by the President or Secretary of Defense, assist in consequence management for CBRNE mass casualty attacks

Acknowledging the challenges presented by the current security environment, the Department of Defense must be able to conduct most major combat operations in a CBRNE environment. US military forces organize, train, and equip to operate in contaminated environments, as well as manage the consequences of CBRNE incidents, on a level unmatched by any other single domestic agency or international

partner. **If directed by the President or Secretary of Defense, the Department of Defense must be prepared to use these capabilities to assist interagency partners in the aftermath of CBRNE mass casualty attacks.** DoD's CBRNE capabilities include specialized agent detection and identification systems as well as casualty extraction and mass decontamination abilities. DoD can also provide significant support to domestic consequence management by providing emergency medical support, such as equipment, mobile hospitals, medical personnel, engineering support, and mortuary services.

Not all domestic CBRNE incidents will necessitate a federal response; many scenarios may be well within the capabilities of state and local responders. Those incidents that do require a US government response will be coordinated by a lead federal agency. In most catastrophic scenarios, DoD may be called upon to provide support to the Department of Homeland Security or another lead federal agency. **The Department will work closely with interagency partners—through participation in the National Response Plan, the National Incident Management System, and the Catastrophic Incident Response Supplement—to ensure proficiency and interoperability in responding to multiple CBRNE incidents.**

The Commander, US Northern Command and/or the Commander, US Pacific Command would have operational control of all US military units operating in Title 10 (federal) status and assigned to such a response. The Department will ensure that CBRNE civil support assets—such as Joint Task Force Civil Support and the National Guard Civil Support Teams (CSTs)—are sized, trained,

equipped, and ready for the domestic consequence management mission. This will include planning for the augmentation of existing CSTs with additional National Guard capabilities and forces.

As a priority, DoD will identify well-trained and capable forces to support Joint Task Force Consequence Management-East, and Joint Task Force Consequence Management-West, to provide support to civilian authorities in the event of multiple, near simultaneous CBRNE attacks within the US.

Lastly, the Department will ensure that additional military units of the Total Force—currently sized and shaped primarily for overseas missions—are appropriately identified and trained to support CBRNE consequence management. This will provide added utility for overseas deployment or domestic missions. Adjustments to Active and Reserve Component training, procedures that allow for faster mobilization of National Guard and Reserve Forces, and improved command relationships that make optimal use of the National Guard in joint operations with the Active Component will improve DoD effectiveness for supporting domestic CBRNE contingencies.

Capabilities for Enhancing US and International Capabilities for Homeland Defense and Homeland Security

Core Capability: Improve interagency planning and interoperability

Recognizing the critical importance of interoperability, DoD will share training, planning, and appropriate resources with interagency partners to standardize

operational concepts, develop technology requirements, and coordinate budget planning for homeland missions. Interagency efforts must focus on closing any remaining seams in air, cyber, land, space, and sea domains and must enhance national preparedness and incident management efforts. Development of a coordinated training and exercise program is an essential step toward enhanced cooperation in executing homeland defense and civil support missions.

Active DoD participation in the interagency improves planning and interoperability and will ensure that procedures for providing support to civil authorities are consistent with the framework for domestic incident response outlined in the National Response Plan and the National Incident Management System. DoD will work closely with interagency partners to identify how best to coordinate interagency civil support activities.

Recognizing the essential role of coordinated planning, the Department of Defense has made significant strides within the interagency since September 11, 2001:

- Medical consequence management consists of initiatives that mitigate the health consequences of any domestic event to include terrorist use of CBRNE. **DoD must closely collaborate with other federal agencies in the formulation of policy and comprehensive planning efforts for medical consequence management.** Currently, DoD is working in close coordination with the Department of Health and Human Services, the Department of Homeland Security, and the

Homeland Security Council to ensure public health and crisis management and response planning support the National Response Plan (to include all Supplements and Annexes) and the National Incident Management System.

- DoD participates in the National Capital Region Coordination Center to coordinate air surveillance and defense of the Washington, DC area. DoD, along with its interagency partners, is also investigating the establishment of a national Homeland Air Security Coordination Center.
- The Department is assisting in the development of a national strategy for maritime security through the interagency Maritime Security Working Group. DoD also co-chairs an interagency steering group with the Department of Homeland Security to develop requirements, plans, and priorities for maritime domain awareness.
- The existing Joint Interagency Task Force (JIATF) organizational construct, currently employed for counterdrug operations, is an outstanding mechanism for interagency and multinational security coordination. Indeed, the JIATF is now authorized to support law enforcement agencies conducting counterterrorism activities. The Department will apply the JIATF model to other relevant homeland security and defense missions, particularly in the maritime domain.
- Finally, the Department will examine the outcomes of the Homeland

Security/Homeland Defense Command and Control Advanced Concept Technology Demonstration (ACTD) for benefits to the execution of homeland defense, homeland security, critical infrastructure protection, and antiterrorism/force protection missions. This ACTD, due to conclude in September 2005, is designed to provide DoD components, the Department of Homeland Security, and other federal, state, local, and tribal authorities with improved interoperability and superior command and control.

Core Capability: Leverage DoD expertise to enhance the US civil sector's prevention, preparedness, response, and recovery capabilities

The Department of Defense has identified three tenets to enhance defense support of civil authorities:

- Augment civil capabilities with unique DoD expertise where necessary
- Ensure the seamless operational integration of defense support capabilities with those of the civil sector
- Assist in the civil sector's development, procurement, and sourcing of new technologies and equipment.

Within this civil support framework, the Department will actively seek to identify opportunities for cooperation with the civil sector. Several initiatives to enhance civilian capabilities are already underway. Examples include:

IV. Core Capabilities

- DoD assistance to the Department of Homeland Security to develop CBRNE victim rescue capabilities, similar to those of the US Marine Corps' Chemical Biological Incident Response Force.
- Joint DoD and Department of Homeland Security efforts to develop improved diagnostic capabilities for biological threat agents. DoD's lead biological defense laboratory, the US Army Medical Research Institute of Infectious Diseases (USAMRIID), is now co-located with the Department of Homeland Security's National Bioterrorism Analysis and Countermeasures Center's (NBACC) bio-forensics laboratory. Working with scientists from USAMRIID, NBACC is developing deployable technologies and systems to protect America's citizens, agricultural products, and national economy from the effects of bioterrorism.
- DoD assistance to the Department of Homeland Security to develop patient evacuation capabilities, using DoD's medical evacuation units as a model.
- Joint DoD and Department of Homeland Security research and development on, and civilian acquisition of, (1) unmanned aerial vehicles for law enforcement and (2) ground surveillance systems for border security.
- DoD efforts through the Interagency Counter Man-Portable Air Defense System (MANPADS) Task Force to help develop an attack prevention and recovery plan, provide technical advice and analysis to the Department of Homeland Security regarding

MANPAD countermeasures, and operational assistance to stem the proliferation of MANPADS overseas.

In compliance with Section 1401 of the National Defense Authorization Act of 2003, DoD will continue to engage in efforts to transfer competencies between DoD and the civil sector—through technology transfer as well as sharing DoD's "lessons learned" from applicable exercises and program management. **Such collaborative efforts can increase the overall effectiveness of national capabilities and potentially reduce other agencies' dependencies on limited DoD assets.** To succeed, the Department will need a systematic approach to ensure close coordination with the Department of Homeland Security and other interagency, state, and local partners, specifically:

- Identifying candidate missions, technologies, and capabilities for which state-based National Guard Joint Force Headquarters can provide needed expertise to the civil sector;
- Facilitating the Department of Homeland Security's efforts to identify and provide appropriate and applicable defense technologies to state and local first responders;
- Nurturing new collaborative research and development opportunities with the Department of Homeland Security;
- Developing, in concert with our federal partners, a detailed, interagency roadmap to improve civil sector capabilities over the coming decade; and
- Ensuring the smooth transition of appropriate missions, technologies, and capabilities to the civil sector.

Core Capability: Enhance international partner capabilities for homeland defense and homeland security

Our neighbors, Canada and Mexico, are vital to the protection of the US homeland and the continent. The Department places special emphasis on expanding defense relationships with Canada and Mexico in information sharing, counterterrorism, and cross-border delivery of civil support, particularly for CBRNE consequence management.

Today, the US–Canadian North American Aerospace Defense Command is an excellent example of bi-national defense. Dedicated to the defense of US and Canadian airspace, NORAD has evolved from a Cold War institution to an agile 21st century counterterrorism capability reflecting an integrated, flexible bi-national approach to air defense. Over the next decade, the Department of Defense, in conjunction with the Department of State and the Department of Homeland Security and working with our Canadian partners, will further refine and build on the NORAD concept. This effort will identify mechanisms for sharing information across all operational domains—air, maritime, and land, with shared awareness of the North American maritime domain as the first priority.

Given the vital importance of Mexico to US homeland defense, US-Mexican counterterrorism cooperation is essential. The Department will work with the Department of Homeland Security and Mexico to anticipate and plan for crisis coordination and consequence management following a terrorist attack. Cooperation with Mexico on law enforcement and immigration issues is substantial, especially in counternarcotics and border control operations. Defense-to-defense cooperation requires similar emphasis and must be pursued with due respect for the Mexican government’s policy goals and legal constraints. Traditional security assistance tools are pivotal in further developing mutually beneficial defense capabilities and arrangements.

With these and other key defense partners around the globe, particularly in the Pacific, the Department will expand combined training and experimentation initiatives to improve US and partners’ capabilities for homeland defense missions. **We will also strengthen DoD’s Security Cooperation Guidance to emphasize homeland defense and civil support issues, with emphasis upon improved information sharing, in defense-to-defense interactions.**



V. Implications of the Strategy

“The threats and enemies we must confront have changed, and so must our forces.”

The National Security Strategy of the United States of America

September 2002

The Strategy for Homeland Defense and Civil Support requires adjustments in DoD forces and capabilities, resource allocation, and technology development. Given resource constraints, meeting the Strategy’s homeland defense and civil support objectives will require accommodation of competing demands within the National Defense Strategy.

Force Structure

An understanding of the force structure implications of the Strategy for Homeland Defense and Civil Support is critical to the Department’s ability to size and shape forces correctly for diverse military missions. **This strategy reflects a Total Force approach to homeland defense missions, incorporating the capabilities of Active Duty, National Guard, and Reserve forces that will be trained and equipped primarily for warfighting missions in the forward regions and approaches.** Identified forces must also be prepared to conduct the full spectrum of domestic civil support missions when directed by the President or Secretary of Defense to do so. The types of forces employed for any given homeland defense mission will be situation-dependent. Additionally, the type, scope, and location of events, competing DoD missions, resident civilian capabilities, and a host of other variables will affect requests for defense support of civil authorities.

To execute this diverse range of missions effectively, DoD must ensure the Total Force, both reserve and active components, is:

- **Timely** in response and readily accessible. Homeland defense and civil support missions require a rapid response, often measured in hours, not days.
- **Trained and equipped** to meet the full range of potential missions. The Department must train and exercise forces to achieve the highest degree of readiness in a broad array of mission sets. In particular, these forces must be equipped and prepared to operate in contaminated CBRNE environments, whether overseas or in the US homeland.
- **Transformed** to meet the terrorist challenges of a post-Cold War security environment.

Implications by Major Mission Area

Consistent with the objectives of this Strategy, and in preparation for the next Quadrennial Defense Review, the Department will undertake a thorough analysis of force requirements for homeland defense missions. This analysis will take into account the projected capabilities of civilian agencies where those capabilities may affect DoD’s force requirements. **A preliminary assessment suggests modest**

changes in several major mission areas and the potential for more substantial adjustments to maritime defense forces:

- **Air Defense:** Currently, Air National Guard units conduct most domestic air defense operations, with augmentation by Active and other Reserve Component units for extended or surge-level operations. This level of air defense is projected to be appropriate for the next ten years. The challenges related to countering threats from cruise missiles and other low-flying airborne vehicles will be reduced through advances in interdiction technology and will not require significant additional force structure.
- **Land Defense:** In the projected environment of the next decade, DoD can meet the domestic land defense missions with the designated forces currently available, to include the National Guard in support of homeland defense missions. Nonetheless, continuing overseas deployments may require the Department to identify some additional elements of the Total Force for homeland defense missions to ensure their availability in times of crisis.
- **Maritime Defense:** To implement this strategy fully, the Department will need to adjust force structure and capabilities for maritime defense. Specialized vessels, manned and unmanned aircraft, and highly trained naval personnel are required for maritime interdiction, weapons of mass destruction detection, defense of territorial

waters, and protection of critical defense infrastructure. **Moreover, timeliness of response and effective deployment of forces require the routine assignment of necessary assets to Combatant Commanders in order to achieve an active, layered defense. The passive identification of US maritime assets for possible Combatant Commander employment, as an alternative to actual assignment, is insufficient.** In addition, advances in MDA technology, such as over-the-horizon radar systems, could increase the requirement for maritime defense capabilities, particularly for maritime interdiction operations.

- **Consequence Management:** The Department must evaluate the timeliness and the adequacy of DoD response in the event of multiple mass casualty attacks within the US homeland. Major areas of concern are medical and CBRNE decontamination capabilities where DoD has unique operational competencies that civilian agencies are likely to request following a mass casualty attack. Potential shortfalls related to field hospital facilities, mass decontamination, disposal of contaminants, patient triage, extraction, mortuary affairs, site security, casualty evacuation, and transportation may require adjustments to DoD force structure. **The Department will prepare for civil support missions related to multiple, near simultaneous attacks and preliminarily plan for**

additional follow-on attacks at geographically dispersed locations.

Focused Reliance upon the Reserve Component

For many homeland defense and civil support missions, the Department will expand our reliance on the competencies of the National Guard and other Reserve Component organizations. The most promising areas include:

- *Air and Missile Defense*, including surveillance and manning of ground-based defense systems.
- *Maritime Security*, including Naval Reserve augmentation of active component and Coast Guard capabilities engaged in intelligence and surveillance, critical infrastructure protection, port security, and maritime intercept operations. Given the continuing requirements of these homeland defense missions, DoD will consider appropriate Naval Reserve mission assignments on or above the maritime approaches. **Traditional Cold War missions for the Naval Reserve should be transformed to reflect the 21st century transnational, terrorist threat, most especially the maritime transportation of weapons of mass destruction to the United States.** Therefore, DoD will evaluate the operational benefit of employing Naval Reserve maritime and aviation capabilities in support of emerging homeland defense missions.
- *Land defense*, including missions requiring Quick Reaction Forces/Rapid Reaction Forces. **The National Guard Bureau's current initiative to use existing force structure to form modular Rapid Reaction Forces will provide effective capabilities in every state and territory to support land defense mission requirements**, in particular DoD responsibilities assigned as the sector-specific lead for the defense industrial base.
- *CBRNE response*, including the specific capabilities for detection, extraction, decontamination, and medical care mentioned previously. **The National Guard Chemical-Biological-Radiological-High Explosives Enhanced Force Packages (NGCERFPs) effort is a promising initiative well tailored to this mission.** The Department will invest in developing the NGCERFPs, formed by providing selected WMD-Civil Support Teams with additional capabilities and modeled after the US Marine Corps' Chemical Biological Incident Response Force (CBIRF) teams. **The effective employment of National Guard forces in Title 32 status will maximize Title 10 availability for overseas deployments.** Chemical companies resident in the Army Reserve also provide significant capabilities and are trained and equipped for CBRN assessment as well as extraction and decontamination of mass casualties. The Reserve Component can also offer significant assistance with security, engineering, trans-

portation, communications and other general-purpose homeland defense requirements related to CBRNE response.

- ***Critical Infrastructure Protection***, including the performance of comprehensive assessments at critical infrastructure sites and utilization of Reserve Component forces for quick reaction requirements and, when justified, local security at key defense and non-defense critical infrastructure sites.
- ***Support to law enforcement***, including coordinated efforts with federal, state, and local law enforcement agencies to deter and respond to acts of terrorism and, when necessary, provide security associated with the aftermath of natural disasters and CBRNE attacks. **For example, the National Guard will be prepared to provide security for pharmaceutical and logistics distribution following a catastrophic attack.**

Appendix B provides an expanded discussion of how best to leverage the Reserve Component, and the National Guard in particular, for homeland defense missions.

Technology

Implementation of the Strategy for Homeland Defense and Civil Support requires significant technological investment in three areas: advanced information and communications technology, new generations of sensors, and non-lethal capabilities. The Strategy also leverages

significant activities already underway in the form of Advanced Concept Technology Demonstrations (ACTDs) and aims to invigorate the inclusion of homeland defense mission requirements in the development of new ACTDs.

Advanced Information and Communications Technology

Technological and organizational improvements for homeland security and homeland defense will benefit from focused investment in advanced information technology. **Improved information technology is essential to prevent, interdict, and respond to terrorist activity.** Whether the objective is improved maritime domain awareness and operations, interdiction of weapons of mass destruction, response to chemical or biological attacks, or continuity of operations and government, improvement in information technology is the most efficient way to address current capability shortfalls. Advanced modeling and simulation techniques for threat identification, pattern analysis, risk assessment, dependency analysis, and cost/benefit calculus are critical for addressing issues of data sharing, security, and interoperability. Without these tools, the return on investments in other areas, such as improved sensors, detectors, command and control, and human intelligence (HUMINT) collection and analysis, will be incomplete and insufficient. All of these activities related to improved information technology will be undertaken consistent with the constitution and laws of the US and will be subject to appropriate congressional oversight.

Equally pivotal are potential advances in communications technologies, particularly

those supporting ground-mobile and airborne communications. DoD must also work to reduce the size and power requirements of mobile communications systems. It must also invest in technologies that shield them against electromagnetic effects.

Sensors

New generations of sensors and sensor platforms will enhance threat awareness in the air, maritime, and land domains by helping to close current gaps over much of the maritime domain and in domestic airspace, particularly at low altitudes. Shared sensor technology will also play an important role in enabling improved border surveillance by civilian agencies.

The placement of sensors on high altitude platforms, including new generations of unmanned aerial vehicles, satellites, and aerostats, will allow sustained surveillance of wide areas of the earth's surface. These sensors will also enhance defenses against low-flying cruise missiles. Some new ground sensors will have an over the horizon capability with applications for homeland defense and homeland security missions.

New sensor technologies are also required for maritime defense, including the non-acoustic detection of underwater vehicles, objects, and swimmers. New sensor capabilities will be needed for a wide range of other tasks, such as remote detection of concealed CBRN weapons aboard ships and for mapping the location and extent of contamination should adversaries use these weapons. Finally, **DoD must fully integrate sensors with information networks to coordinate their use and rapidly distribute**

information to operational and policy users.

Non-Lethal Capabilities

The transnational terrorist attack of September 11, 2001, made it clear that the US homeland is now part of the enemy battle space. Therefore, we may be required to defeat attacks in close proximity to major civilian population centers. To achieve this mission requirement, while minimizing risk to innocent citizens, less than lethal weapons must be operationally deployed for use against terrorist adversaries.

Non-lethal technologies with potential application to homeland defense missions include:

- **Counter-personnel technology**, used to deny entry into a particular area, temporarily incapacitate individuals or groups, and clear facilities, structures, and areas.
- **Counter-material technology**, to disable, neutralize, or deny an area to vehicles, vessels, and aircraft, or disable particular items of equipment.
- **Counter-capability technology**, to disable or neutralize facilities, systems, and CBRNE.

The Department will expand basic research into the physiological effects of non-lethal weapons. The Department should also identify opportunities to share appropriate non-lethal capabilities with domestic law enforcement agencies, consistent with applicable law. It is now clear that non-lethal weapons can be an operationally effective alternative to deadly force.

Rapid Prototyping of Emerging Capabilities

Advanced Concept Technology Demonstrations are a key DoD vehicle for rapidly fielding promising technologies. The objectives of an ACTD are to conduct meaningful demonstrations of the capability, develop and test concepts of operations to optimize military effectiveness, and, if warranted, prepare to transition the capability into acquisition without loss of momentum. Currently, there are over 25 ACTDs with relevance to homeland defense and homeland security such as the Homeland Security/Homeland Defense Command and Control Advanced Concept Technology Demonstration. The Department will ensure that requirements for homeland defense and civil support are properly addressed in the ACTD process in the decade ahead. The Department will continue working with the Department of Homeland Security and other domestic and international partners to encourage their participation in ACTDs as appropriate. **DoD will also continue to leverage innovative capabilities arising from private sector initiatives, many of which are fostered through the interagency Technical Support Working Group (TSWG).**

Funding

The integration of this homeland defense strategy into the global battle space means that all funding appropriated to DoD has an ultimate value in the protection of the US homeland, most especially the funding dedicated to power projection.

Nevertheless, with many important programs competing for finite resources,

proper funding and budget oversight for homeland defense missions is vital. Currently, the Department accounts for homeland defense activities through a variety of widely dispersed programs and funding lines. Funding for homeland defense is not accounted for consistently; it can be found in every Service and combatant command and numerous initiatives under the purview of the Office of the Secretary of Defense.

The Department will evaluate the utility of specifically designating a portion of the DoD budget to consolidate and sustain selected homeland defense capabilities in order to clearly identify core homeland defense programs and assets in each Service and component budget. **To ensure overall supervision and effective use of DoD resources, the Department must make consolidated budget tracking of key homeland defense initiatives a high priority.**

Funding Implications

In developing planning and programming guidance to implement the Homeland Defense and Civil Support Strategy, DoD must thoroughly assess the fiscal implications of attaining the requisite core capabilities. An initial assessment indicates that the most significant potential costs associated with this Strategy arise in the following areas:

- **Expanding communications infrastructure** and enhancing DoD's ability to share vital information while protecting the integrity of the Global Information Grid;

- **Improving intelligence assets** to increase overall threat awareness throughout all domains;
- Achieving maximum awareness of potential threats through the use of **advanced technologies** such as high-altitude sensors;
- Ensuring the necessary capabilities, types, and number of transformational forces needed to effectively conduct a **maritime defense-in-depth** against transnational threats;
- Implementing DoD's **Defense Critical Infrastructure Protection** responsibilities;
- Increasing resources for **non-lethal weapons** research and capabilities;
- Providing support for **continuity of federal government operations** in the event of a national emergency or catastrophe; and
- Implementing **National Guard Bureau transformation** initiatives, such as NGCERFPs.

In the course of implementing this strategy, the Department must not take on responsibilities and costs for homeland security missions better addressed by other federal, state, local, or tribal authorities. This will require close coordination and continuing cooperation with the Department of Homeland Security and other interagency partners.



VI. Implementing the Strategy

"Our greatest responsibility is the active defense of the American people."

President George W. Bush

January 20, 2004

Managing Homeland Defense and Civil Support Risk

The Department must employ a risk management strategy that appropriately acknowledges the importance of an active, layered homeland defense. Risk management based on clear objectives allows the Department to concentrate available resources to provide the most robust defense. The Strategy places a premium on achieving its objectives on a prioritized basis. These priorities reflect the Department's primary responsibility for protecting the homeland from attack. They also emphasize the DoD's most challenging civil support mission—CBRNE consequence management. A more specific discussion of the Strategy's risk management approach is detailed below:

Lead. The Department's key lead objectives are to achieve maximum awareness of threats, interdict and defeat threats at a safe distance, and provide mission assurance. **The Department's foremost priority, and the foundation of all of DoD's lead responsibilities, is to ensure DoD's ability to interdict and defeat threats at a safe distance from US territory.** DoD cannot accept undue risk in its active defense of the US homeland from foreign air, land, or maritime threats. The most critical enabler to the interdiction and defeat of these

threats is shared situational awareness. Therefore, the Department will focus special attention on improved domain awareness for US military forces. Recognizing the resource-intensive requirements posed by the Department's range of critical homeland defense and overseas missions, DoD accepts some operational risk in providing mission assurance.

Support. Transnational terrorists have a demonstrated intent to acquire weapons of mass destruction and exploit US vulnerabilities in order to employ such weapons against potential domestic targets. The Department seeks to minimize risk by ensuring competent consequence management capabilities for responding to multiple simultaneous CBRNE mass casualty attacks in the United States. **DoD will maintain a ready, capable, and agile command and control structure, along with competently trained forces, to assist civilian authorities with catastrophic incident response. However, with the exception of a dedicated command and control element (currently the Joint Task Force-Civil Support) DoD will continue to rely on dual-capable forces for consequence management and other defense support of civil authorities.** The Department minimizes the risk that dual-capable forces may be assigned to other high priority missions by ensuring the deconfliction of overseas and domestic force requirements. DoD will nevertheless continue to improve

the scope and depth of planning, coordination, and exercises for domestic civil support.

Enable. Enabling domestic and international partner capabilities is an important priority for the Department. **The Department aims to decrease long-term risk by improving the capabilities of our interagency and international partners.** Although enabling efforts require relatively few dedicated forces, technology, and resources, DoD accepts some risk in achieving the “Enable” objective in order to attend to address other, more immediate, “Lead” and “Support” objectives.

To optimize DoD’s capabilities, the Department must not only prioritize *within* homeland defense and civil support missions, but also balance risk *across* the breadth of the defense program. **An active, layered defense integrates homeland defense and power projection operations conceptually and operationally.** Therefore, the Department will assess homeland defense and civil support mission risks and resources in context with other requirements outlined in the National Defense Strategy.

Actions for Immediate Implementation

Transformation of DoD capabilities for homeland defense and defense support of civil authorities requires a focused effort to adapt to the changing security environment, leverage advances in technology, and improve coordination with international and interagency partners. Accordingly, **the Department will fully integrate strategy, planning, and operational capabilities for homeland defense and civil support into DoD’s broader implementation processes for the National Defense Strategy.** This requires the Department to foster resident expertise on homeland defense issues in policy and planning organizations, focus resources on resolving the challenges outlined in this Strategy, and balance risk according to the priorities articulated in the National Defense Strategy.

The following major issues, discussed in priority order and by capability, take precedence for resolution. Each of these actions will be coordinated with interagency and international partners as appropriate:

Managing Risk: Prioritized Objectives for Homeland Defense and Civil Support

1. Achieve maximum awareness of potential threats (Lead);
2. Interdict and defeat threats, wherever possible at a safe distance from the United States, its territories, and its possessions (Lead);
3. Provide mission assurance (Lead);
4. Ensure the Department of Defense’s ability to support civil authorities in domestic CBRNE consequence management (Support);
5. Improve domestic as well as North American and Pacific partners’ capabilities for homeland defense and homeland security (Enable).

Maximum Threat Awareness

All-Domain Awareness: The Chairman, Joint Chiefs of Staff will initiate a zero-based assessment of the sensors and other capabilities needed to detect, identify, and track objects in the air, land, sea, and space surrounding the United States, US territories, and US possessions. This effort must be closely coordinated within the DoD and with the Department of Homeland Security and other US government agencies. Based on this assessment, **the Chairman, Joint Chiefs of Staff will develop a coordinated, all-domain sensor architecture for homeland defense** for presentation to the Secretary of Defense no later than March 15, 2005.

Expansion of the Common Information Infrastructure: The inadequacy of US civilian agencies' network enterprises, and specifically their inability to communicate with DoD's advanced information architecture, impairs the Department's conduct of homeland defense and civil support missions. Accordingly, **the Assistant Secretary of Defense for Networks and Information Integration, working through the Federal Corporate Information Officer Council and with the Office of Management and Budget, will assess the architectural requirements and investment options for ensuring interoperability between DoD and interagency partners in the homeland defense mission space.** The analysis will also evaluate the creation of a national continuity telecommunications architecture. The Assistant Secretary for Networks and Information Integration will present this analysis and any associated Department-level recommendations to the Secretary of Defense no later than March 15, 2005.

Improved Intelligence: **The Under Secretary of Defense for Intelligence, in coordination with the broader Intelligence Community (IC), will identify initiatives to improve defense intelligence and IC capabilities for homeland defense.** The effort will assess the utility of establishing a dedicated homeland defense cell within the Defense Intelligence Agency and will refine essential elements of intelligence for homeland defense missions. The Under Secretary of Defense for Intelligence will present his findings to the Secretary of Defense no later than March 15, 2005.

Interdict and Defeat Threats

Improved Maritime Defense: **The Commander, US Northern Command, will assess the maritime requirements of US Northern Command.** The assessment will be based on a unified concept of operations for the NORTHCOM maritime domain and will include an analysis of needed capabilities. The Combatant Commander, US NORTHCOM will present his coordinated recommendations to the Secretary of Defense no later than March 15, 2005.

Improved Air and Cruise Missile Defense: **The Commander, NORAD will develop joint concepts of operations and requirements for a joint, rapidly deployable area air and cruise missile defense (DAACMD) architecture.** The DAACMD will defend geographic regions within the United States or special events as directed by the President or Secretary of Defense, and should be capable of defeating the full spectrum of anticipated air threats, including low-observable and low-altitude air vehicles. The DAACMD concept of operations and associated systems will form

the foundation for a future national air and cruise missile defense architecture. The concept of operations will be consistent with interagency air security strategies and should include the employment of reserve component assets. The Commander, NORAD will present his coordinated concept of operations to the Secretary of Defense no later than March 15, 2005.

Focused Reliance upon the National Guard and Reserve Capabilities: In coordination with the Under Secretary of Defense for Personnel and Readiness, **the Under Secretary of Defense for Policy will develop a detailed roadmap to expand the use of National Guard and other Reserve Component capabilities for homeland defense and civil support missions.** The roadmap shall include recommendations on adjustments to force structure and capabilities, mobilization processes for the rapid domestic deployment of reserve units operating in Title 10 (Federal) status, training, and potential resource implications. The Under Secretary of Defense for Policy will present his coordinated roadmap to the Secretary of Defense no later than March 15, 2005.

Non-Lethal Weapons Capabilities: **The Commanders, US Northern Command and US Pacific Command will develop a concept of operations and identify requirements for the domestic military employment of non-lethal capabilities.** They will present this concept to the Secretary of Defense no later than June 30, 2005. Based on direction provided by the Secretary of Defense, the Director, Program Analysis and Evaluation, in concert with the Chairman, Joint Chiefs of Staff, the Secretaries of the Military Departments, the Under Secretary of Defense for Acquisition,

Technology and Logistics, the Under Secretary of Defense for Policy, and the Executive Agent for Non-Lethal Weapons, will develop an investment plan for the development, procurement, and fielding of non-lethal capabilities for use in the domestic arena. The Director, Program Analysis and Evaluation will present this plan to the Secretary of Defense during the FY2007-2011 Program Review.

Provide Mission Assurance

Critical Infrastructure Protection: The Under Secretary of Defense for Policy will ensure that the Department of Defense fully implements the Defense Critical Infrastructure Program Integrated Risk Management Strategy for FY2006-FY2011.

Improve Continuity and Crisis Management Capabilities: The Under Secretary of Defense for Policy, in coordination with the Chairman of the Joint Chiefs of Staff and the Director, Washington Headquarters Service, will analyze current DoD capabilities for continuity and crisis management. The assessment will identify potential vulnerabilities and propose crisis management procedures, capabilities, training and exercise initiatives, and communications capabilities to eliminate those vulnerabilities. The Under Secretary of Defense for Policy will present his findings to the Secretary of Defense no later than March 15, 2005.

Provide Support for Domestic CBRNE Consequence Management

Counter-CBRNE and Consequence Management Capabilities: The Department of Defense will ensure the protection of high priority DoD installations and

personnel from CBRNE attacks. The Department will address this issue in the Enhanced Planning Process, aiming to improve sense, shape, shield, and sustain capabilities significantly over the five years covered by the next Future Years Defense Program. **In addition, the Chairman, Joint Chiefs of Staff, will examine the training and readiness standards required for those military forces whose capabilities are likely to be called upon by civilian authorities in the event of multiple, near simultaneous, domestic CBRNE mass casualty attacks. These coordinated efforts will be completed with a sense of urgency and appropriate recommendations will be presented to the Secretary of Defense no later than March 15, 2005.**

Improve Relevant National and International Capabilities

Systematic Approach to Homeland Defense Exercises: **The Commander, US Northern Command and Commander, US Pacific Command will jointly implement a comprehensive and systematic homeland defense exercise program by FY2006.** These exercises should fully integrate National Guard forces as appropriate. It should also integrate Canadian and Mexican participation, the Caribbean nations, and

our Pacific partners in order to assess mutual capabilities to detect, track, interdict, and defeat transnational terrorist and state-based threats to the US homeland from the land, sea, or air and deal with the consequences of an attack. **The homeland defense exercise program will complement DoD's participation in the National Exercise Program for Homeland Security, directed in Homeland Security Presidential Directive 8.**

* * * *

Each of the DoD capabilities referenced in this section will be reviewed in detail with our interagency partners, especially the Department of Homeland Security and the Department of Justice. **The Department seeks to implement this strategy consistent with the themes set forth in the National Security Strategy for Homeland Security.** The Department also recognizes the importance of Section 1401 of the National Defense Authorization Act of 2003, which focuses on technology transfer to other agencies. **The ultimate success of this strategy depends on the ability to effectively integrate the Department of Defense's capabilities with its interagency partners.**



VII. Conclusion

“The battle is now joined on many fronts. We will not waver; we will not tire; we will not falter; and we will not fail. Peace and freedom will prevail.”

*President George W. Bush
October 7, 2001*

The United States faces ruthless enemies who seek to break our will and exploit America’s fundamental freedoms. Our terrorist adversaries, driven by a totalitarian ideology, are eager to employ violence against Americans at home. In this environment, the Department of Defense’s paramount goal will continue to be the defense of the US homeland from external attack.

A new kind of enemy requires a new concept for defending the homeland. **The terrorist enemy now considers the US homeland a preeminent part of the global theater of combat, and so must we.** We cannot depend on passive or reactive defenses but must seize the initiative from adversaries. Multiple, unpredictable barriers to attack must be employed across the globe, creating a seamless web of land, sea, and air assets that are arrayed to detect, deter, and defeat hostile action.

The active, layered defense articulated in this Strategy does just that—seamlessly integrating US capabilities in the forward regions of the world, the global commons of space and cyberspace, and the geographic approaches to the US territory, and within the United States. Whether in a leading, supporting, or enabling role, the Department of Defense, guided by this Strategy and consistent with US law, will work with an intense focus to protect the US homeland and

the American people. We will accomplish the key objectives set forth in this Strategy:

- Achieving maximum awareness of potential threats;
- Interdicting and defeating threats at a safe distance from the US homeland;
- Providing mission assurance;
- Effectively supporting civil authorities in domestic CBRNE consequence management; and
- Improving interagency and international partner capabilities for homeland defense and homeland security.

When fully realized, this Strategy will transform the Department’s homeland defense and civil support capabilities. The Nation will have effective intelligence, surveillance, and reconnaissance capabilities for homeland defense; and information will be widely shared with relevant decision-makers. The Department will have well-trained and responsive forces for homeland defense missions that will use improved technology and operational concepts to eliminate potential seams between the maritime, air, and land domains. Additionally, **the Department will achieve unity of effort with our interagency and international partners in the execution of**

homeland defense and civil support missions.

In formulating the Strategy for Homeland Defense and Civil Support, the Department has carefully considered its potential implications for force structure, technology development, and funding. Our initial analysis points to the need for modest but important adjustments in forces, technology investments, and programs. The Strategy's most radical call for change, however, is not in these areas. Rather, it is in the Department's conceptual and cultural

approach to homeland defense. The Department can no longer think in terms of the "home" game and the "away" game. There is only one game.

The effectiveness of any strategy is ultimately in the hands of those charged with its implementation. The Strategy for Homeland Defense and Civil Support is a call for fundamental transformation in military capabilities in order to meet the 21st century threat. Defending the US homeland — our people, property, and freedom — is a fundamental duty. Failure is not an option.



Appendix A. Legal Authorities

The primary legal authority to conduct military missions in defense of U.S. territory and interests is the U.S. Constitution. Specifically, Article II, Section 2 of the Constitution provides that the President “shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual Service of the United States....” As Commander-in-Chief, the President has broad authority to conduct military homeland defense missions.

In addition to the broad Constitutional power of the President, Congress has provided another authority for certain homeland defense missions. Specifically, Public Law 107-40, a joint resolution entitled “Authorization for Use of Military Force” provides authority for the President to use “all necessary and appropriate force against those nations, organizations or people” responsible for the terrorist attacks of September 11, 2001. Finally, U.S. military forces retain the right to engage in self-defense without advance approval of the President or Secretary of Defense.

When the Department is conducting homeland defense military missions, it is engaged in the statutory obligation to defend the Nation and is conducting its core, war-fighting mission. In contrast, when the Department is conducting civil support operations, it must have separate statutory authorization for those operations. For these missions, the Department acts when a request for assistance from a domestic civil authority is approved by the Secretary of Defense.

“Immediate Response” operations are a distinct, and very limited, category of civil support operations. Under imminently serious conditions, where communication with superior authorities is not possible within time constraints necessary to save lives, prevent human suffering, and mitigate great property damage, local commanders have Immediate Response authority. Although it is a well-established principle, of which Congress is well aware, there is no explicit statutory authority for Immediate Response. The authority to authorize such response is derivative of Presidential authority to respond to emergency situations, and is clearly grounded in the common law principle of “necessity.”

Civil support missions are diverse and are supported by multiple authorities. Examples of civil support missions the Department conducts, and the statutes that authorize them, include:

- The foundational legal authority for the Department to provide disaster assistance is the Stafford Act (42 USC 5121 et. seq.).
- Numerous statutes authorize the Department to provide assistance to civil law enforcement. However, unless there is a Constitutional or statutory exception to the Posse Comitatus Act (18 USC 1385), that support must be “indirect.”
- Among the authorities for conducting counternarcotics operations, 10 USC 124, authorizes the Department to detect and

monitor the aerial and maritime transit of illegal drugs.

- For counterterrorism operations, Public Law 108-136, Section 1022, authorizes Joint Task Forces that support counternarcotics operations to support law enforcement agencies conducting counterterrorism activities as well.
- The Insurrection Act (10 USC 331-334) provides authority for the President to direct the Department to support civil law enforcement agencies in restoring and maintaining order in the event of civil disturbances.

Article II of Constitution also gives the President the authority to command the

militias of each state when called to federal service. The National Guard of the various states is the modern-day embodiment of the militia referenced in the Constitution. When federalized, the National Guard is subject to the same laws, including the Posse Comitatus Act, as the active duty force. However, until the National Guard is placed in federal active service, it is governed by state law. Although the laws of each state vary, most allow the National Guard, while serving under the direction of the Governor, to enforce state laws. When serving under state command and control, the provisions of the Posse Comitatus Act do not apply, although there may be state restrictions that do apply.



Appendix B. New Roles for the Guard and Reserve

The Department of Defense must ensure that US military forces are able to defeat 21st century challenges across the full range of threats. The transformation of the Reserve Component is central to achieving this end. Our geographically dispersed National Guard and Reserve Components are indispensable in executing the active, layered defense of the US homeland. Therefore, the Department will ensure that the National Guard and Reserve Components are properly trained and equipped for homeland defense and civil support missions and are able to act in a timely manner to defeat the threats presented by transnational terrorism. Designated personnel and units of the Army National Guard and Air National Guard, as well as of each Reserve Component (Army, Air Force, Navy, Marine Corps, and Coast Guard), will be prepared to conduct homeland defense missions and the full spectrum of domestic civil support missions when directed by the President or Secretary of Defense. Each of the seven Reserve Components will play key roles in our emerging homeland defense posture:

- *Air Force Reserve* – Timely airlift, logistics, and aero-medical support. Air refueling for air defense.
- *Air National Guard* – Primary air defense provider. Significant CBRNE consequence management support capabilities, including security, engineering, medical, and communications units.
- *Army Reserve* – Significant CBRNE consequence management support capabilities, including transportation, security, medical, and decontamination units.
- *Army National Guard* – State-based capabilities for infrastructure protection, response forces, and CBRNE consequence management.
- *Naval Reserve* – Intelligence analysis capabilities to identify and anticipate hostile threats in the forward regions and approaches. Maritime security capabilities in the approaches, in order to support and conduct maritime interdiction operations and airborne surveillance.
- *Marine Corps Reserve* – Command and control capabilities, including for CBRNE consequence management. Reaction force capabilities (QRF/RRF). Aviation capabilities for potential air defense missions. Capabilities for planning and executing maritime interdiction operations.
- *Coast Guard Reserve* – Primary Reserve Component force for security of ports and other key maritime infrastructure.

Potential Guard and Reserve Focus Areas

The list that follows provides key examples of homeland defense and civil support mission areas in which DoD can better employ National Guard and Reserve Components:

- ***In the expansion of air defense capabilities, including those designed to counter threats from cruise missiles and other low-flying airborne vehicles, increase reliance on the National Guard for key missions.*** The Air National Guard provides key capabilities in enforcing the air sovereignty of the United States, including its territories and possessions. The post-September 11, 2001 era demonstrated a need for improved air defense, including ground-based air defense in the National Capital Region, at designated National Security Special Events, and around high interest/high threat locations. For example, Army National Guard Air Defense units have demonstrated essential capabilities for the ground-based air defense mission. The use of National Guard rotary wing platforms for air intercept operations against low flying and slow moving threats could also be beneficial. As the United States develops and fields additional ballistic and cruise missile defenses, DoD should employ National Guard personnel to man ground-based stations, as they are doing through the Missile Defense Space Battalion in Alaska.
- ***Integrate Naval Reserve and Marine Corps Reserve personnel and capabilities into maritime defense plans and operations.*** Naval Reserve forces are well suited for intelligence analysis, particularly the identification of threats in the forward regions and approaches. In addition, Naval Reserve and Marine Corps Reserve assets could be employed in the maritime approaches to provide airborne surveillance (both manned and unmanned aircraft) and to participate in CBRNE-related maritime interdiction operations.
- ***Integrate key Reserve Component capabilities – particularly those of the Army Reserve – in the response to CBRNE incidents.*** The US Army Reserve’s core competencies in Combat Support and Combat Service Support will be of significant value in the aftermath of CBRNE attacks or other catastrophic events. These competencies include aviation, biological detection and identification, chemical, civil affairs, decontamination, engineering, information operations, logistics, military police, signal, psychological operations, and mortuary affairs. Similar capabilities exist in the Army National Guard, Air National Guard, and Air Force Reserve. The Department may also employ Marine Corps Reserve as reaction forces (QRF/RRF), in command and control roles, and as CBRNE response forces in the event of a domestic CBRNE attack.

- ***Utilize National Guard installations, systems, and forces to provide forward-deployed logistics support—Reception, Staging, and Onward Integration (RSOI), Base Support Installation (BSI), and other relevant forms of logistical support—for use in domestic emergencies.*** The National Guard in each state is capable of providing support for the RSOI of military forces responding to domestic events, a task similar to the requirements for mobilizing forces for employment outside the United States. One of the core advantages of the National Guard Joint Force Headquarters in each state is the ability to provide support to all committed forces on an area basis. The United States Property and Fiscal Officer, a Title 10 officer, has the ability to provide logistical support to all forces in a designated area of operations.
- ***In the development of biological incident response plans, include provisions for National Guard and other Reserve Component forces to support affected populations.*** In the event of a large-scale contagious biological attack, there may be requirements for National Guard and other Reserve Component forces to distribute food, prophylaxes and other medical supplies, and other sustainment materiel. Guard forces could also provide associated security support.
- ***Tap the National Guard's training and exercise capabilities and established relationships with the civilian sectors to enhance the nation's homeland defense and homeland security posture.*** The Guard has an impressive record of providing training and exercises to virtually all relevant interagency audiences and has put in place associated systems and infrastructure. More importantly, the Guard has also built a reservoir of trust, goodwill, and cooperation with key civilian agencies and organizations at the federal, state, and local levels that is invaluable in planning for and responding to threats on US territory. The organization's capabilities, resources, and established interagency relationships must be recognized, resourced, and integrated into homeland defense approaches, policies, and plans.
- ***Significantly expand RC-based cyber defense capabilities, leveraging the civilian sector training, experience, and perspectives of traditional RC personnel.*** Many reservists, employed full-time in the civilian sector, have knowledge and skills that can and should be leveraged for cyber defense purposes. This pool of expertise and experience has the potential to greatly improve DoD programs to defend critical computer-based systems and infrastructure.
- ***Leverage the Air National Guard's emerging capabilities in global communications, intelligence, surveillance, and reconnaissance to ensure seamless situational***

awareness across all operational domains, from the forward regions and approaches to the homeland.

Specific capabilities that may prove beneficial include deployable command and control systems, training in information operations and intelligence analysis, and information systems vulnerability assessments.

- *Field specialized RC units (with bilingual capabilities when required) to conduct combined operations with neighboring countries to identify and interdict terrorists and terrorist-related materiel.* The Guard's State Partnership Program, a highly effective tool in Combatant Commander security cooperation kits in US European Command, US Southern Command, and US Pacific Command, could serve as a model for building and tapping relationships with US neighbors. Personnel with language skills could establish military-to-military, military-to-civilian, and civilian-to-civilian contacts, assisting the effort to identify and defeat terrorists attempting to infiltrate US borders.
- *Leverage capabilities resident in the National Guard's counternarcotics mission to enhance counterterrorism intelligence gathering and CBRNE consequence management.* Given the established connection between narcotics trafficking and terrorism, Guard aviation assets used in counternarcotics are ideally suited to support the counterterrorism mission. Congress, recognizing the narcotics-terrorism nexus, recently

passed legislation facilitating the use of specific DoD counternarcotics capabilities in support of counterterrorism. National Guard counternarcotics assets, used in support of civil authorities, could be particularly effective as counterterrorism surveillance platforms and would also be effective for security, communications, and maritime search and interdiction. Non-aviation assets in the Guard could be used in times of crisis for cargo inspection duties at selected air and sea terminals.

Enabling Mission Success

To ensure that the Nation has access to forces that are timely, trained, and transformed for homeland defense and civil support, the Department must take full advantage of National Guard and Reserve Component capabilities. Accordingly, DoD must eliminate obstacles to the employment of the Reserve Component, resolving the following set of issues:

- *Command and control relationships*— The National Guard's decision to create a "Joint Force Headquarters-State" in each of the 54 states and territories provides an opportunity to coordinate the homeland defense capabilities of all the services and agencies within each of those jurisdictions. A joint headquarters would be able to track all DoD resources—active and reserve, deployable units and support elements—within a state. The joint headquarters could coordinate the planning and execution of homeland security, civil

support, and homeland defense missions in a state, as appropriate. A joint headquarters could also serve to closely coordinate DoD efforts with state and local capabilities.

It is therefore important to establish relationships between the Joint Force Headquarters-State organization, US Northern Command and/or US Pacific Command, to incorporate into a unified plan all Title 10 and Title 32 forces assigned to a homeland security, civil support, or homeland defense mission. The command and control relationship used for the June 2004 G8 Summit held on Sea Island, Georgia provides a useful template for future efforts. The National Guard's "Joint CONUS Communications Support Element" initiative could serve as the information technology infrastructure to support these command relationships and serve as a single point of contact for US Northern Command, US Pacific Command, and other inter-agency stakeholders to receive current and accurate information from any of the 54 states and territories. And finally, the US Army Reserve's existing Regional Readiness Commands (one in each Federal Emergency Management Agency region) should be leveraged for civil support training, planning, and mobilization.

- ***A 21st century Title 32 and Title 10 Construct***—Operating under either State Active Duty or Title 32 status, National Guard forces can provide support to civilian law enforcement authorities in two key areas. First,

National Guard counternarcotics efforts can enhance the effectiveness of counterterrorism initiatives through information-sharing, logistics support, and combined operations. Second, by virtue of their status under state law and Title 32 of US Code, National Guard forces provide civilian authorities with operational flexibility in their use for Military Support to Civilian Law Enforcement Agencies.

Expanded authorities under a revised Title 32, along with the National Guard's ongoing transformation into a truly 21st century force, will provide Governors and state authorities with flexible, responsive, multi-capable units to deter and defeat localized terrorist attacks. For example, National Guard reaction forces—scalable in terms of size and mix of skills—can provide security for critical infrastructure, support civilian law enforcement agencies in responding to terrorist acts, and offer their neighbors immediate assurance of safety and security.

- ***Processes for notification, mobilization, and demobilization***—The essence of homeland defense is timely response. Cold War timelines have become irrelevant to the transnational threat. The Department must transform the processes for notifying, mobilizing, and de-mobilizing our Reserve Component forces to meet the requirements of the 21st century threat environment. The Department should undertake a

comprehensive review of these processes and implement appropriate transformational measures.

- ***Predictability and accessibility***—To the extent possible, Active Component and Reserve Component leaders should establish mobilization cycles that provide predictability for every level in the chain-of-command, from the individual service member and his or her employer to the Combatant Commander. As US Northern Command and US Pacific Command develop operational plans for homeland defense, the Commands need operational assurance that Reserve Component forces will be available where and when required, with the necessary training and equipment to complete the assigned mission. Governors also require some level of assurance that they will have access to National Guard capabilities in the event of natural disasters or civil disturbance. Interstate compacts must be reviewed to ensure they are responsive to the current threat environment. These compacts support the centralized planning of interstate deployments for emergencies affecting the Nation as a whole.
- ***Systematic approach to training and exercises***—In the event of a catastrophic CBRNE attack, there is no room for error or delay in the Department's ability to support civil authorities. Ensuring its preparedness for such a catastrophic

incident requires the Department to properly plan, resource, conduct, and evaluate a systematic and rigorous homeland defense training and exercise regimen. This training and exercise program must have a Total Force scope, taking into account every echelon and element of the Reserve Component, and must be closely integrated into the first responder and emergency management communities at the local, state, and federal levels.

The National Guard and Reserve Components are a critical link to the Nation's federal, state, and local authorities. The successful execution of 21st century homeland defense and civil support missions will require the Department to expand its reliance on these forces, while preserving their oversea warfighting skills. The collective Reserve Component contribution is essential to the Nation's effective execution of an active, layered defense.



Appendix C. Strategic Planning Guidance Tasking

The Department of Defense Strategic Planning Guidance (SPG) for Fiscal Years 2006-2011 required that the Strategy for Homeland Defense and Civil Support specifically address the following areas:

- An integrated Intelligence Community threat assessment;
- A concept for achieving domain awareness across the information, land, sea, and aerospace realms;
- Horizontal integration of intelligence across the US Government and among local, state, and federal actors;
- The DoD chemical, biological, radiological, and nuclear protection capabilities needed to support the strategy;
- The role of the Reserve component in homeland defense and civil support;
- Efforts to improve national preparedness through the migration of selected civil support missions to other federal agencies;
- A risk management strategy for critical infrastructure protection;
- DoD's role in protection of the Defense Industrial Base;
- A zero-based review of DoD's continuity of operations plans; and
- A concept of operation for domestic use of non-lethal technologies.

FINAL COORDINATION DRAFT

Strategy for Homeland Defense and Civil Support



**Department of Defense
Washington, D.C.**

Current as of: 4 January 2005

FINAL COORDINATION DRAFT



Table of Contents

- Executive Summary1
 - Protect the United States from Attack through an Active, Layered Defense.....1
 - Organizing Construct—Lead, Support, and Enable2
 - Key Objectives of the Strategy2
 - Capability Themes for Homeland Defense and Civil Support3
 - Projected Implications of the Strategy4
- I. Context5
 - Key Definitions.....5
 - Standing Guidance from National and Defense Strategies5
 - Security Environment.....7
 - Organizing for Homeland Defense and Civil Support7
 - Assumptions9
- II. Active, Layered Defense.....10
- III. Strategic Goal and Key Objectives.....13
 - Lead.....15
 - Support17
 - Enable18
- IV. Core Capabilities.....19
 - Capabilities for Achieving Maximum Awareness of Threats19
 - Capabilities for Intercepting and Defeating Threats at a Safe Distance.....23
 - Capabilities for Providing Mission Assurance26
 - Capabilities for CBRNE Consequence Management.....30
 - Enhancing US and International Capabilities for Homeland Defense and Homeland Security31
- V. Implications of the Strategy34
 - Force Structure34
 - Technology36
 - Funding38
 - Managing Homeland Defense and Civil Support Risk.....39
 - Conclusion40



Executive Summary

"The world changed on September 11, 2001. We learned that a threat that gathers on the other side of the earth can strike our own cities and kill our own citizens. It's an important lesson; one we can never forget. Oceans no longer protect America from the dangers of this world. We're protected by daily vigilance at home. And we will be protected by resolute and decisive action against threats abroad."

President George W. Bush

September 17, 2002

Protecting the United States homeland from attack is the highest priority of the Department of Defense (DoD). On September 11, 2001, the world changed dramatically. For the first time since Pearl Harbor, we experienced catastrophic, direct attacks against our territory. This time, however, the foe was not another nation but terrorists seeking to undermine America's political will and destroy our way of life. As a result, the United States has become a nation at war, a war whose length and scope may be unprecedented.

We now confront an enemy who will attempt to engage us not only far from US shores, but also at home. Terrorists will seek to employ asymmetric means to penetrate our defenses and exploit the openness of our society to their advantage. By attacking our citizens, our economic institutions, our physical infrastructure, and our social fabric, they seek to destroy American democracy. We dare not underestimate the devastation that terrorists seek to bring to Americans at home.

To defeat 21st century threats, we must think and act innovatively. Our adversaries consider US territory an integral part of a global theater of combat. We must therefore have a strategy that applies to the domestic context the key principles that have shaped

the successful transformation of US power projection and joint expeditionary warfare.

Protect the United States from Attack through an Active, Layered Defense

This Strategy for Homeland Defense and Civil Support focuses on achieving the Defense Department's paramount goal: securing the United States from direct attack. The strategy is rooted in the following:

- Respect for America's constitutional principles;
- Adherence to Presidential and Secretary of Defense guidance;
- Recognition of terrorist and state-based threats to the United States; and
- Commitment to continue transformation of US military capabilities.

Protecting the United States in the ten-year timeframe covered by this Strategy requires a strategic concept for an active, layered defense. **This active, layered defense is global, seamlessly integrating US capabilities in the forward regions of the world, the global commons of space and cyberspace, in the geographic approaches to**

US territory, and within the United States. It is a defense in depth. To be effective, it requires superior intelligence collection and analysis, calculated deterrence of enemies, a layered system of mutually supporting defensive measures that are neither passive nor ad hoc, and the capability to mass and focus sufficient warfighting assets to defeat any attack.

This active, layered defense employs tactical defenses in a strategic offense. It maximizes threat awareness and seizes the initiative from those who would harm us. In so doing, it intends to defeat potential challengers before they threaten the United States at home.

Organizing Construct—Lead, Support, and Enable

Although the active, layered defense extends across the globe, this Strategy for Homeland Defense and Civil Support focuses primarily on DoD's activities in the homeland and the approaches to US territory. In those geographic layers, the Department undertakes a range of activities to protect the United States from attack. These generally divide into the following categories:

- **Lead:** At the direction of the President or the Secretary of Defense, the Department of Defense executes military missions that prevent, deter, defend, and defeat attacks upon the United States, our population, and our defense critical infrastructure.
- **Support:** At the direction of the President or the Secretary of Defense, the Department of Defense provides support to civil authorities. This support is part of a comprehensive

national response to prevent and protect against terrorist incidents or recover from an attack or disaster. DoD provides support to a lead federal agency when directed by the President or the Secretary of Defense.

- **Enable:** The Department of Defense actively seeks to improve the homeland defense and homeland security contributions of our domestic and international partners and, in turn, to improve DoD capabilities by sharing expertise and relevant technology, as appropriate, across military and civilian boundaries.

Key Objectives of the Strategy

Within the lead, support, and enable framework for homeland defense and civil support, the Department is focused on the following paramount objectives, listed in order of priority:

- **Achieve maximum awareness of potential threats.** Together with the Intelligence Community and civil authorities, DoD works to obtain and promptly exploit all actionable information needed to protect the United States. Timely and actionable intelligence, together with early warning, is the most critical enabler to protecting the United States at a safe distance.
- **Intercept and defeat threats at a safe distance.** The Department of Defense will defend the United States in our air and maritime approaches. When directed by the President or the Secretary of Defense, we also defeat direct threats within US airspace and on US territory. In both cases, the

Department of Defense acts in accordance with applicable laws.

- **Provide mission assurance.** The Department of Defense performs assigned duties even under attack or after disruption. We protect our forces, installations, and information; ensure crisis management, continuity of operations (COOP), and continuity of government (COG); and ensure the security of defense critical infrastructure.
- **Support civil authorities in recovering from domestic chemical, biological, radiological, nuclear or high-yield explosive (CBRNE) mass casualty attacks.** The Department of Defense will be prepared to provide forces and capabilities in support of domestic CBRNE consequence management, with an emphasis on preparing for multiple, simultaneous mass casualty incidents. US military forces must be trained, equipped, and ready to provide timely assistance to civil authorities in times of domestic CBRNE catastrophes, programming specifically for this capability as necessary.
- **Improve national and international capabilities for homeland defense and homeland security.** The Department of Defense is learning from the experiences of domestic and international partners and sharing expertise with federal, state, local, and tribal authorities, the private sector, and US allies and friends abroad. By sharing expertise, we improve the ability of the Department

of Defense to carry out an active, layered defense.

Capability Themes for Homeland Defense and Civil Support

Several important themes underlie the objectives and capabilities established by this Strategy:

- **Intelligence, Surveillance, and Reconnaissance Capabilities.** The Department of Defense requires current and actionable intelligence defining potential threats to US territory. DoD must also ensure that it can identify and track suspect traffic in the air and maritime approaches and conduct reconnaissance and surveillance to examine wide areas of the maritime and air domains to discover potential threats before they reach the United States.
- **Information-Sharing.** Together with domestic and international partners, DoD will integrate information collected from a wide range of sources. The events of September 11, 2001 highlighted the need to share information across federal agencies and, increasingly, with state, local, and tribal authorities, the private sector, and international partners.
- **Joint Operational Capabilities for Homeland Defense.** DoD will continue to transform US military forces to execute homeland defense and civil support missions in the air and maritime approaches, within US airspace, and on US territory.

- **Interagency and Intergovernmental Coordination.** The Department of Defense and our domestic and international partners will continue to coordinate closely in the execution of homeland defense and civil support missions.

When fully realized, this Strategy for Homeland Defense and Civil Support will transform and improve DoD capabilities in each of these areas.

Projected Implications of the Strategy

In developing this Strategy, the Department took into account its likely force structure, resource, and technology implications in order to ensure the appropriate alignment of scarce Department resources with the priorities set forth in the National Defense Strategy. As DoD components implement the strategic tenets outlined in this document, a more precise accounting of the forces, technological advances, and financial resources it requires will be needed.

Because DoD's forces and resources are finite, the Strategy recognizes the need to manage

risk within the homeland defense and civil support mission areas. It does so by allocating DoD forces and resources in accordance with the Strategy's prioritized objectives, focusing resources on fulfilling its lead responsibilities for homeland defense. As a second priority, we will ensure the Department's ability to support civil authorities in recovering from multiple, catastrophic mass casualty CBRNE incidents within the United States.

The Department of Defense will expeditiously implement the Strategy for Homeland Defense and Civil Support. Fundamentally, this will require the Department to integrate strategy, planning, and operational capabilities for homeland defense and civil support more fully into DoD processes. **Even as the Department of Defense implements this Strategy, it will continue to adapt to changes in the strategic environment, incorporate lessons learned from operational experience, and capitalize on emerging technology and operational concepts.**



I. Context

“For most of the twentieth century, the world was divided by a great struggle over ideas: destructive totalitarian visions or freedom and equality. That great struggle is over. The militant visions of class, nation, and race which promised utopia have been defeated and discredited. America is now threatened less by conquering states than we are by failing ones. We are menaced less by fleets and armies than by catastrophic technologies in the hands of the embittered few. We must defeat these threats to our Nation, allies, and friends.”

*The National Security Strategy of the United States of America
September 2002*

The Strategy for Homeland Defense and Civil Support embodies the core principles articulated in the US Constitution, the Nation’s laws, and in Presidential and Secretary of Defense guidance. It also responds to the challenges posed by the security environment over the next decade.

Key Definitions

Homeland security, as defined in the National Strategy for 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 Department of Homeland Security is the lead federal agency for homeland security. In addition, its responsibilities extend beyond terrorism to preventing, preparing for, responding to, and recovering from a wide range of major domestic disasters and other emergencies.

Homeland defense is the protection of US sovereignty, territory, domestic population, and critical defense infrastructure against direct threats and aggression. The Department of Defense is responsible for homeland defense.

Defense support of civil authorities, often referred to as civil support, is DoD support provided during and in the aftermath of domestic emergencies—such as terrorist attacks or major disasters—and for designated law enforcement and other activities. When directed by the President or the Secretary of Defense, DoD provides support of civil authorities by employing the Nation’s federal military forces, the Department’s career civilian and contractor personnel, and DoD agency and component assets.

Standing Guidance from National and Defense Strategies

The Strategy for Homeland Defense and Civil Support integrates the objectives and guidance expressed in the National Security Strategy, the National Strategy for Homeland Security, and the National Defense Strategy to guide Department of Defense operations to protect the US homeland.

- The National Security Strategy (2001) expands the scope of US foreign and security policy to encompass forward-reaching preventive activities,

including pre-emption, against hostile states and terrorist groups.

- The National Strategy for Homeland Security (2002) guides the national effort to secure the US homeland against terrorist attacks. It provides a framework for action at all levels of government that play a role in homeland security.
- The National Defense Strategy (2004) identifies as its top priority the dissuasion, deterrence, and defeat of direct threats to the United States. The Strategy's implementation hinges on

an active, layered defense that is designed to defeat the most dangerous challenges early and at a safe distance, before they are allowed to mature. It directs military leadership to properly shape, size, and globally posture to 1) defend the US homeland; 2) operate in and from four forward regions; 3) swiftly defeat adversaries in overlapping military campaigns while preserving the president's option to call for a decisive result in a single operation; and 4) conduct a limited number of lesser contingencies.

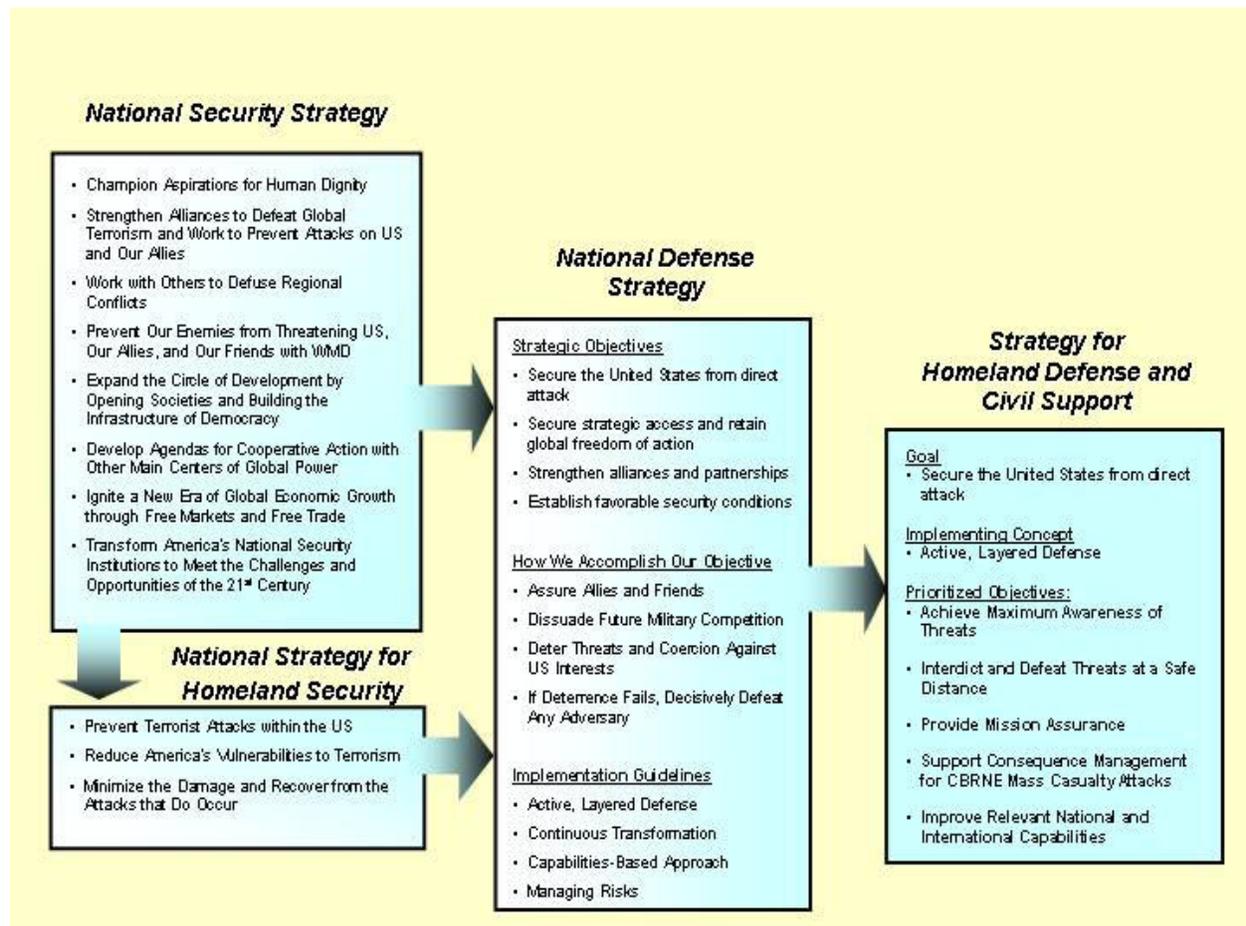


Figure 1: Strategic Underpinnings of the Strategy for Homeland Defense and Civil Support

In addition to these overarching strategies, the Strategy for Homeland Defense and Civil Support is informed by, and complements, other key strategic and planning documents. These include standing National Security and Homeland Security Presidential Directives, the National Military Strategy, the DoD Homeland Security Joint Operating Concept, and *Military Transformation: A Strategic Approach* (Office of the Director for Force Transformation).

Security Environment

The defining characteristic of the security environment over the next ten years is the certainty of substantial diverse and asymmetric challenges to the United States, our allies, and interests. At the same time, we are faced with great *uncertainty* regarding the specific character, timing, and sources of potential attacks. This Strategy for Homeland Defense and Civil Support addresses the full range of challenges to the US homeland over the next decade.

Nation-state military threats to the United States will persist throughout the next decade. Rogue nations, for example, pose immediate and continuing challenges to the United States and our allies, friends, and interests. In addition, we must prepare for the potential emergence of regional peer competitors.

The United States will also face a range of asymmetric, transnational threats. Of greatest concern is the availability of weapons of mass destruction, heretofore the exclusive domain of nation-states, to terrorist groups. **In the next ten years, these terrorist groups, poised to attack the United States and actively seeking to inflict mass casualties or disrupt**

US military operations, represent the most immediate challenge to the nation's security.

Transnational terrorist groups view the world as an integrated, global battlespace in which to exploit perceived US vulnerabilities, wherever they may be. This battlespace includes the US homeland. Terrorists seek to attack the United States and its centers of gravity at home and abroad and will use asymmetric means to achieve their ends, such as simultaneous, mass casualty attacks. On September 11, 2001, terrorists demonstrated both the intent and capability to conduct complex, geographically dispersed attacks against the United States and our allies. It is foreseeable that adversaries will also develop or otherwise obtain chemical, biological, radiological, nuclear, or high-yield explosives (CBRNE) capabilities, with the intent of causing mass panic or catastrophic loss of life. Although America's allies and interests abroad will be the most likely targets of terrorism in the coming decade, we must also anticipate enemy attacks aimed at Americans at home.

Organizing for Homeland Defense and Civil Support

In light of the importance of homeland defense and DoD's contributions to homeland security, the Secretary of Defense, with the support of Congress, has improved the Department's organization and oversight structure for homeland defense and civil support.

- **The Assistant Secretary of Defense for Homeland Defense.** As stated in the 2003 National Defense Authorization Act, the Assistant Secretary of Defense for Homeland Defense provides overall supervision

of DoD's homeland defense activities. The establishment of the Assistant Secretary of Defense for Homeland Defense responded to the need for improved policy guidance to DoD Components on homeland defense and civil support issues.

- **US Northern Command**, headquartered in Colorado Springs, Colorado. Established in 2002, US Northern Command (USNORTHCOM) is responsible for planning, organizing, and executing all aspects of homeland defense and performing civil support missions within the continental United States, Alaska, and territorial waters. It also coordinates security cooperation with Canada and Mexico. In addition to the land masses of the United States, Canada, and Mexico, US Northern Command's area of responsibility includes the coastal approaches, the Gulf of Mexico, Puerto Rico, and the US Virgin Islands.
- **US Pacific Command**, headquartered in Honolulu, Hawaii. US Pacific Command (USPACOM) has homeland defense and civil support responsibilities for Hawaii and US territories, possessions, and freely associated states in the Pacific.
- **North American Aerospace Defense Command**, headquartered in Colorado Springs, Colorado. The binational North American Aerospace Command (NORAD) is responsible for protecting the North American airspace over the United States and Canada. Aerospace warning and control are the cornerstones of the NORAD mission.

In addition to these organizations, all other regional and functional combatant commands, the Military Departments, and DoD elements contribute to the protection of the US homeland from attack.

- Other regional combatant commanders can promote international cooperation on homeland defense through exercises and military-to-military contact programs. Together with the functional combatant commanders, these regional commanders can also intercept and defeat adversaries intent on attacking US territory. Of particular note, US Strategic Command is responsible for early warning of and defense against missile attack and long-range conventional attacks. It is further charged with deterring and defending against the proliferation of weapons of mass destruction and conducting information operations as well as computer network operations.
- The Military Departments organize, train, and equip US military forces across operational domains. The Military Departments provide the bulk of the DoD capabilities likely to be requested for civil support.
- Other DoD Components contribute to homeland defense through intelligence collection, analysis, and prioritization; capability assessments; and oversight of relevant policy, acquisition, logistics, personnel, readiness, and financial matters.

The Strategy for Homeland Defense and Civil Support will guide all DoD Components across the full range of

homeland defense and civil support activities.

Assumptions

This Strategy makes the following key assumptions:

- The United States will continue to face traditional military challenges emanating from hostile nation-states. Nation-state adversaries will incorporate asymmetric threats into their broader strategies of competition and confrontation with the United States.
- Terrorists will seek and likely gain surreptitious entry into the United States to conduct mass casualty attacks against Americans on US soil.
 - Terrorists will leverage vulnerabilities to create new methods of attack.
 - Terrorists and/or rogue states will attempt multiple, simultaneous mass casualty CBRNE attacks against the US homeland.
 - Terrorists will try to shape and degrade American political will in order to diminish American resistance to terrorist ideologies and agendas.
- Allies and friends will cooperate with the United States in mutually beneficial security cooperation arrangements.
- US Northern Command, the North American Aerospace Command, and US Pacific Command will continue to develop mature homeland defense capabilities in the air, land, and maritime domains, with appropriate support provided by other combatant commands.
- The Department of Homeland Security and other federal, state, local, and tribal authorities will continue to improve their prevention, preparedness, response, and recovery capabilities throughout the decade.
- The Department of Defense will promote the integration and sharing of applicable DoD capabilities, equipment, and technologies with federal, state, local, and tribal authorities and the private sector.
- In the event of major catastrophes, the President or the Secretary of Defense will direct DoD to provide substantial support to civil authorities. DoD's responses will be planned, practiced, and carefully integrated into the national response.
- The likelihood of US military operations overseas will be high throughout the next ten years.



II. Active, Layered Defense

"The war on terror will not be won on the defensive. We must take the battle to the enemy, disrupt his plans, and confront the worst threats before they emerge. In the world we have entered, the only path to safety is the path of action. And this nation will act."

President George W. Bush

June 1, 2002

As set forth in the National Defense Strategy (2004), the Department of Defense is transforming its approach to homeland defense just as it is transforming national defense capabilities overall. **Guiding homeland defense planning is the concept of an active, layered defense, predicated on seizing the initiative from adversaries.**

"Our most important contribution to the security of the US homeland is our capacity to disrupt and defeat threats early and at a safe distance, as far from the US and its partners as possible. Our ability to identify and defeat threats abroad—before they can strike—while making critical contributions to the direct defense of our territory and population is the sine qua non of our nation's security."

The National Defense Strategy

The case for an active, layered defense is clear. The United States has multiple points of vulnerability that adversaries seek to exploit. Significantly, these vulnerabilities exist in America's key centers of gravity. Commerce relies on the flow of goods and people across the nation's borders, through our seaports and airports, and on our streets and highways. The US free market economy requires trust in the uninterrupted electronic movement of financial data and funds through cyberspace. The symbols of American heritage—monuments and public

buildings—are a source of national pride and are open to all. Vast and potentially vulnerable natural resources provide power to our homes and food for our tables.

To safeguard the American way of life and to secure our freedom we cannot depend on passive or reactive defenses. A strictly defensive strategy is easily subject to enemy reconnaissance and inevitable defeat. By contrast, an active, layered defense relies on early warning of an emerging threat in order to quickly deploy and execute a decisive response.

The United States must keep potential adversaries off balance by both an effective defense of US territory and, when necessary, by projecting power across the globe. **We must seize the initiative from adversaries and apply all aspects of national power to prevent, intercept, and disrupt attacks against us and our allies and friends. In short, the United States must act in ways that an enemy cannot predict, circumvent, or overcome.** Multiple barriers to attack must be deployed across the globe—in the forward regions, the approaches to the United States, in the US homeland, and in the global commons—to create an unpredictable web of land, maritime, and air assets that are arrayed to aggressively detect, deter, and defeat hostile action.

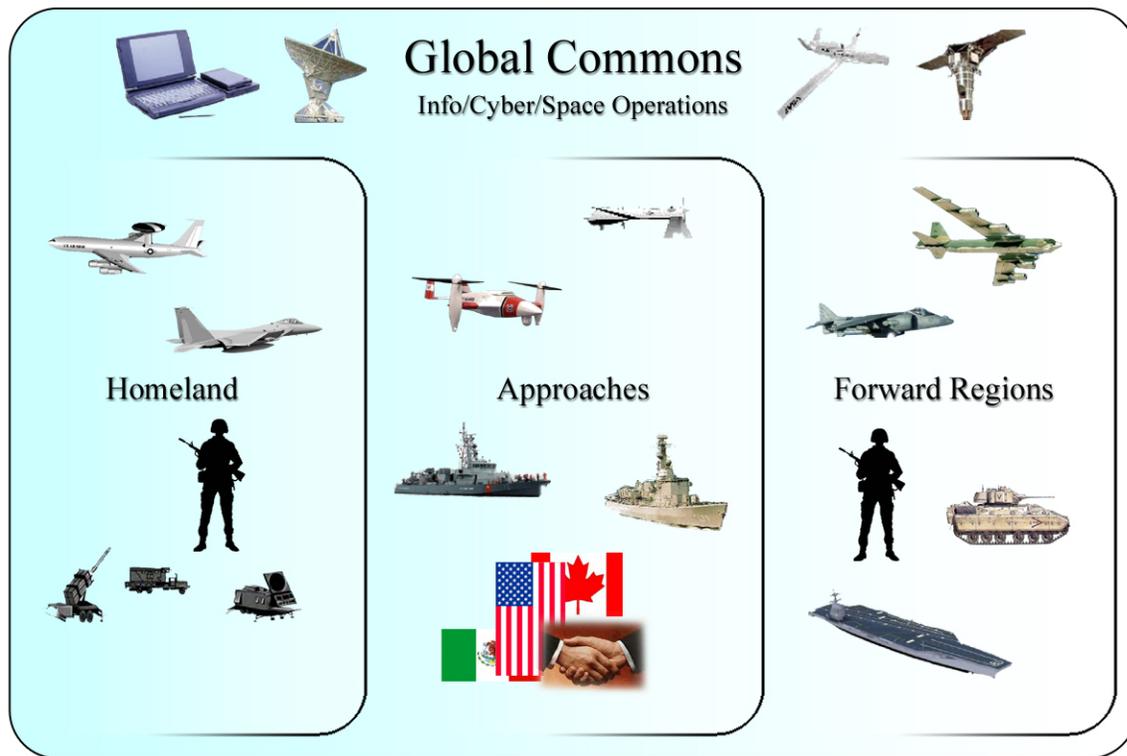


Figure 2: Active, Layered Defense Concept

The Forward Regions. The forward regions are foreign land areas, sovereign airspace, and sovereign waters outside the US homeland. The Department of Defense is a key contributor to the President’s integrated national security effort abroad. To respond quickly to rising threats, the United States requires timely and actionable intelligence. Improved human intelligence (HUMINT) collection, improved analysis of terrorist threats and targets, and improved technical collection against potential CBRN weapons are all critical in this regard. In addition, the United States must counter and delegitimize the ideological support for terrorist groups, disrupt their flow of funding, and create an environment that curtails recruitment. US military forces must be trained, ready, and postured to intercept potential enemies, eliminate enemy sanctuaries, and maintain

regional stability, in conjunction with allies and friendly states.

The Approaches. The waters and airspace geographically contiguous to the United States are critical homeland defense battle-spaces. In these approaches, US Northern Command, the North American Aerospace Defense Command, and US Pacific Command, supported by the Intelligence Community, the US Coast Guard, and other combatant commands, have the opportunity to detect, deter, and, if necessary, defeat threats en route—before they reach the United States. **This requires maximum awareness of threats in the air and maritime avenues of approach as well as the interception capabilities necessary to maintain US freedom of action, secure the rights and obligations of the United States, and protect the nation at a safe distance.**

The American Homeland. The US homeland includes the United States, its territories and possessions, and the Commonwealths and Compact States of the Pacific. It also includes the surrounding territorial seas. Among its responsibilities within US territory, DoD focuses on the following areas:

- DoD is responsible for defeating direct attacks against the United States, when so directed by the President or the Secretary of Defense. NORAD is the cornerstone of our homeland air defense capability. Our air defense success rests on an integrated system for air surveillance and defense against air threats at all altitudes. DoD also maintains land forces capable of responding rapidly, when so directed, to threats against DoD personnel, defense critical infrastructure, or other domestic targets. Finally, DoD supports the US Coast Guard in the exercise of its maritime authorities under domestic and international law.
- DoD supports civilian law enforcement and counterterrorism authorities consistent with US law. This includes providing expertise, intelligence, equipment, and training facilities to domestic law enforcement when so directed. It can also include the use of US military forces to support civilian law enforcement in responding to civil disturbances, as provided in US law.
- DoD provides critical CBRNE consequence management capabilities in support of civil authorities. With few exceptions, DoD's consequence management capabilities are designed for the wartime protection of the Department's personnel and facilities. Nevertheless, civil authorities are

likely to call upon these capabilities if a domestic CBRNE catastrophe occurs in the ten-year time frame of this strategy. **DoD must therefore equip and train forces, as necessary, for domestic CBRNE consequence management.**

The Global Commons. The global commons consist of space and cyberspace. America's ability to defend the global commons and operate effectively from them is critical to the conduct of all US military missions, from the forward regions to the homeland. This is particularly true given our reliance on net-centric capabilities. **An active, layered defense requires a trustworthy information system, impervious to disabling digital attacks.** Computer network defense must ensure that networks can self-diagnose problems and build immunity to future attacks. At the same time, networks must remain operational and consistently available for the execution of US military missions.

An active defense also requires the ability to detect and defeat threats from space. This includes the need for capable defenses against ballistic missiles. Ground facilities that support US space systems are potential targets of attacks and the Department will protect them.



III. Strategic Goal and Key Objectives

"We must build and maintain our defenses beyond challenge. Our military's highest priority is to defend the United States . . . The threats and enemies we must confront have changed, and so must our forces."

The National Security Strategy of the United States of America

September 2002

The employment of an active, layered defense across the globe is fundamental to homeland defense. The National Defense Strategy emphasizes the Department of Defense's role in the forward regions and the global commons and how that role is critical to the defense of US territory. **This Strategy for Homeland Defense and Civil Support therefore focuses particular attention on the US homeland and its approaches.** In these geographic layers, the Department's activities to protect the United States generally fall into one of the following categories:

- **Lead:** DoD leads military missions to deter, prevent, and defeat attacks on the United States, its population, and its defense critical infrastructure. This includes defending the maritime and air approaches to the United States and protecting US airspace, territorial seas, and territory from attacks. The Department is also responsible for protecting DoD personnel located in US territory.
- **Support:** At the direction of the President or the Secretary of Defense, the Department provides defense support of civil authorities in order to prevent terrorist incidents or manage the consequences of an attack or a disaster. Civil authorities are most likely to request DoD support where we have unique capabilities to

contribute or when civilian responders are overwhelmed. DoD's contributions to the comprehensive national response effort can be critical, particularly in the near-term, as the Department of Homeland Security and other agencies strengthen their preparedness and response capabilities.

- **Enable:** Efforts to share capabilities and expertise with domestic agencies and international partners reinforce the Department's lead and support activities. At home, the Department works to improve civilian capabilities for homeland security by lending expertise and sharing relevant technology. For example, DoD is assisting the Department of Homeland Security in its efforts to develop intelligence analytical capabilities. We are also sharing training and simulation technologies, as well as unmanned aerial vehicle technologies for civilian surveillance along the Nation's borders. Abroad, the Department's security cooperation initiatives improve collective capabilities for homeland defense missions through exercises, information-sharing agreements, and formal defense agreements, such as NORAD.

III. Strategic Goal and Key Objectives

To fulfill the key strategic goal of protecting the United States from attack, the Department of Defense will focus on achieving five key objectives directly related to the lead, support, and enable framework. In order of priority, these objectives are:

1. Achieve maximum awareness of potential threats (Lead);
2. Intercept and defeat threats at a safe distance from the United States, and US territories and possessions (Lead);
3. Provide mission assurance (Lead);
4. Ensure DoD's ability to support civil authorities in domestic CBRNE consequence management (Support); and

5. Improve domestic and international partner capabilities for homeland defense and homeland security (Enable).

These objectives are described in detail below. The defense capabilities required to fulfill them are discussed in detail in Section IV of the Strategy.

<i>ACTIVITIES</i>	<i>OBJECTIVES</i>	<i>CORE CAPABILITIES</i>
LEAD	Achieve Maximum Awareness of Threats	<ul style="list-style-type: none"> • Maintain agile and capable defense intelligence architecture • Analyze and understand potential threats • Detect, identify, and track emerging threats in all operational domains • Ensure shared situational awareness within DoD and with domestic and foreign partners
	Intercept and Defeat Threats at a Safe Distance	<ul style="list-style-type: none"> • Intercept and defeat national security threats in the maritime and air approaches and within US territory
	Provide Mission Assurance	<ul style="list-style-type: none"> • Prepare DoD installations for direct threats, especially CBRNE attacks • Ensure DoD crisis management and continuity preparedness • Prepare and protect defense critical infrastructure • Ensure preparedness of the Defense Industrial Base • Prepare to protect designated national critical infrastructure
SUPPORT	Support Consequence Management for CBRNE Mass Casualty Attacks	<ul style="list-style-type: none"> • Manage consequences of CBRNE mass casualty attacks
ENABLE	Improve Relevant National and International Capabilities	<ul style="list-style-type: none"> • Effective interagency planning and interoperability • Capable federal, state, and local partners and effective domestic relationships • Capable international partners and effective defense-to-defense relationships

Figure 3: DoD Objectives and Core Capabilities for Protecting the United States from Attack

Lead

Objective 1: Achieve maximum awareness of threats

To defend the nation in the 21st century, the Department requires sufficient forewarning and immediate situational awareness of potential attacks. No longer is it sufficient to track the movement of hostile military aircraft and warships. In the 21st century threat environment, transnational terrorists and rogue states may employ a wide range of civilian vessels and aircraft as weapons, engage in cyber attacks, or target civilian infrastructure to achieve devastating effects.

To protect the United States in this environment, the Department of Defense, in cooperation with domestic and international partners, will seek to achieve maximum awareness of threats. By so doing, the United States increases the time available for an effective operational response. **Threat awareness includes the ability to obtain comprehensive, accurate, timely, and actionable intelligence and information; exploiting relevant information; and making it available to the warfighters, policy makers, and interagency and international partners responsible for identifying and responding to threats.**

An active, layered defense requires information to flow freely regardless of operational boundaries. Relevant information may originate in one or several of the operational domains—land, maritime, air, cyberspace, or space. It may originate from an array of domestic and foreign sources. To achieve maximum awareness of threats, information will be posted to DoD's Global Information Grid, integrating operational domains and facilitating information sharing

across traditional military-civilian boundaries. Using fused and shared threat awareness, our domestic and international partners and we can determine the most appropriate means to deter, intercept, or defeat threats and act accordingly.

Objective 2: Intercept and defeat threats at a safe distance

During the Cold War, the United States focused on preventing Soviet submarines, ballistic missiles, and long-range bombers from attacking the American homeland. Although concerns about traditional conventional and nuclear threats to the US homeland remain, we recognize that in the next ten years, adversaries will present a host of new challenges. They may attempt to use commercial vessels to transport terrorists or weapons to the United States. They may attempt to intrude on US airspace with low-altitude aircraft, cruise missiles, and unmanned aerial vehicles. They may attempt to convert maritime vessels, aircraft, and other modes of transportation into weapons. Through these and other means, our enemies will constantly employ asymmetric means to challenge the security of the United States.

In the maritime approaches, DoD is working with the Department of Homeland Security to integrate US maritime defense and to optimize the mutually supporting capabilities of the US Navy and the US Coast Guard. **As the Chief of Naval Operations has stated, "forward deployed naval forces will network with other assets of the Navy and the Coast Guard, as well as the intelligence agencies to identify, track and intercept threats long before they threaten this nation."** This will require a level of situational awareness in the maritime domain similar to that in the air approaches. The goal, as the

CNO explains, is to “**extend the security of the United States far seaward, taking advantage of the time and space purchased by forward deployed assets to protect the U.S. from impending threats.**”

In the air domain, DoD has primary responsibility for defending US airspace and protecting the United States from ballistic missiles, cruise missiles, and other aerospace attacks. For North America, this defense is carried out in partnership with Canada, through NORAD. In addition, the Department of Defense relies heavily on the Federal Aviation Administration and the Department of Homeland Security (Transportation Security Administration) for early identification of air threats. As in the maritime environment, cooperation and operational coordination with our interagency partners, as well as our neighbors and other allies, is critical to protecting the United States from air threats.

Within US territory, we face the challenge of intercepting and defeating enemies determined to cause fear, death, and economic disruption. Although we must not dismiss traditional foreign military threats, in the period covered by this strategy, domestic employment of the US military in a homeland defense role will likely come in response to transnational terrorist, rogue state, or other threats that exceed the capabilities of domestic counterterrorism and law enforcement authorities.

Therefore, the Department must approach the interception and defeat of threats to US territory from a joint, interagency, and, ultimately, intergovernmental perspective. DoD must not conduct operations in separate and distinct land, maritime, and air operational domains. Over the coming

decade, the Department will continue to develop joint concepts of operations, working with critical interagency and international partners as appropriate.

Objective 3: Provide mission assurance

The Department cannot fulfill any of the Strategy’s key objectives without having the core capabilities in place to assure mission success. **Mission assurance, the certainty that DoD components can perform assigned tasks or duties in accordance with the intended purpose or plan, is therefore itself a key objective.** The Department of Defense’s framework for mission assurance includes a range of programs and efforts aimed at securing DoD warfighting capabilities even when under attack or after disruption. These include force protection measures, installation preparedness, continuity of operations, and defense critical infrastructure protection.

Force Protection and Installation

Preparedness. An attack on DoD military and civilian personnel or the facilities where they work could directly affect the Department’s ability to project power overseas or carry out vital homeland defense functions. Of particular concern is the threat to DoD personnel posed by domestic CBRNE attacks. To achieve an appropriate level of personnel protection on domestic bases and installations, the Department will develop and implement a comprehensive preparedness plan for CBRNE attacks. This plan will leverage capabilities and programs throughout the Department (e.g. Critical Infrastructure Protection, Antiterrorism/Force Protection, Project Guardian) including required intelligence support. In accordance with DoD responsibilities in the National Biodefense Policy, the Department is

especially attentive to the unique challenges posed by biological agents.

Crisis Management and Continuity of Operations. During an emergency, the Nation's leaders, including DoD decision-makers, must be able to carry out vital government functions. **The Department must provide the President and Secretary of Defense with survivable and enduring national command and control of DoD assets and US military forces.** DoD also plays an important supporting role in ensuring Continuity of Government and Enduring Constitutional Government in times of crisis. In the Cold War era, DoD continuity efforts focused on survival of senior leadership to prosecute war in the aftermath of a massive nuclear attack. Today, DoD's crisis management efforts are broader, responsive to the full range of potential threats to the nation. Meeting the Department's crisis management objectives requires ready DoD transportation assets, capable and survivable remote operation sites, and advanced communications capabilities throughout the DoD continuity architecture. DoD will continue to explore innovative concepts in communications and netcentric operations to improve national-level crisis management.

Critical Infrastructure Protection. The Department of Defense has the responsibility for assuring it has access to *defense critical infrastructure*. This is defined as DoD and non-DoD cyber and physical assets and associated infrastructure essential to project and support military forces worldwide.

In some scenarios, assurance of non-DoD infrastructures might involve protection activities, in close coordination with other federal, state, local, tribal, or private sector partners. This could include elements of the Defense Industrial Base, which provides

defense-related products and services that are essential to mobilize, deploy, and sustain military operations. It could also include selected civil and commercial infrastructures that provide the power, communications, transportation, and other utilities that military forces and DoD support organizations rely on to meet their operational needs.

In addition, the President or the Secretary of Defense might direct US military forces to protect non-DoD assets of national significance. The President has designated fourteen categories of non-defense Critical Infrastructures and Key Assets. Although these facilities and assets are not required for the support of DoD missions, they are so vital to the nation that their incapacitation, exploitation, or destruction could have a debilitating effect on the security and economic well-being of the United States.

Support

Objective 4: Support consequence management for CBRNE mass-casualty attacks

The Department has traditionally supported civil authorities in a wide variety of domestic contingencies, usually natural disasters. DoD typically does so using military forces and DoD capabilities designed for use in expeditionary warfighting missions. That support continues today. For example, unique national intelligence capabilities that are located within the Defense intelligence community are frequently called upon to support other US government agencies. Although these traditional types of defense support of civil authorities are likely to continue, they are not likely to impede DoD's ability to execute other missions specified in the National Defense Strategy.

At the high end of the threat spectrum, however, the 21st century environment has fundamentally altered the terms under which Department of Defense assets and capabilities might be called upon for support. **The potential for multiple, simultaneous, CBRNE attacks on US territory is real.** It is therefore particularly imperative that the Department of Defense be prepared to support civilian responders in responding to such mass casualty events.

Support to domestic authorities for consequence management is a core element of active, layered defense. The Department of Defense maintains considerable CBRNE recovery expertise and equipment. When directed by the President or the Secretary of Defense, DoD will employ these capabilities to assist the Secretary of Homeland Security, the principal federal official for domestic incident management, or other domestic authorities. **DoD must be prepared to support its interagency partners in responding to a range of CBRNE incidents, including multiple, simultaneous mass casualty attacks within the United States.**

Enable

Objective 5: Improve national and international capabilities for homeland defense and homeland security

Enabling better national capabilities for homeland security missions is an important complement to DoD's lead and support activities. The broad range of threats posed by terrorists and other transnational actors has expanded our traditional concept of national security. In the past, the Department of Defense could largely fulfill its responsibility for protecting the nation

by integrating its activities with the Department of State and the Intelligence Community. Today, the expertise and corresponding responsibility for managing security challenges is much more widely shared among federal departments and agencies. State, local, and tribal authorities, the private sector, and our allies and friends abroad are also critical contributors to US national security.

In such an environment, DoD must unify its efforts with those of its key interagency partners and international friends and allies to ensure the nation's security. Sharing technology, capabilities, and expertise strengthens the nation's ability to respond to hostile threats and domestic emergencies. Likewise, cooperative homeland defense education and training initiatives will foster a common understanding of shared threats and how best to address them. In turn, DoD can readily leverage the expertise of other federal, state, local, and tribal authorities and international partners to improve its own capabilities for counterterrorism, maritime interception, and other missions critical to an active, layered defense.



IV. Core Capabilities

“Some believe that, with the U.S. in the midst of a dangerous war on terrorism, now is not the time to transform our armed forces. I believe that quite the opposite is true. Now is precisely the time to make changes. The impetus and the urgency added by the events of September 11th powerfully make the case for action.”

*Secretary of Defense Donald Rumsfeld
January 31, 2002*

The Department of Defense will provide the homeland defense and civil support capabilities necessary to support implementation of the National Security Strategy, the National Strategy for Homeland Security, and the National Defense Strategy. Over the next ten years, DoD will protect the United States from attack by focusing on the core capabilities necessary to achieve each of the key objectives detailed in Section III.

Capabilities for Achieving Maximum Awareness of Threats

Core Capability: Capable and agile defense intelligence architecture

Protecting the United States against the full range of 21st century threats requires the US Intelligence Community to restore its human intelligence capabilities, reprioritize intelligence collection to emphasize probable homeland defense threats, and invest in new intelligence, reconnaissance, and surveillance (ISR) sensor capabilities. In the Cold War, we knew both the nature of the threat to our country and the source of that threat. Today, intelligence and warning must extend beyond conventional military and strategic nuclear threats to cover a wide range of other state-

and non-state challenges that may manifest themselves overseas or at home.

The Intelligence Community is adjusting to this changing strategic landscape to meet the nation’s homeland security needs. The establishment of a National Intelligence Director, the National Counter-Terrorism Center (NCTC), the Department of Homeland Security’s Information Analysis and Infrastructure Protection Directorate, and the DoD’s Joint Intelligence Task Force for Combating Terrorism (JITF-CT) exemplify this shift. Executive Orders for strengthened management of the Intelligence Community also ensure a more collaborative, comprehensive approach to intelligence support for national security. While these changes are taking place, the Department of Defense is reorienting its intelligence capabilities in line with the full range of homeland defense priorities. Specifically, the Department will:

- Focus on integrated collection management of foreign and military information and its application to homeland defense and homeland security;
- Better utilize national intelligence assets and capabilities to increase early warning and support prevention, interception, and

disruption of potential threats overseas or in the approaches to the United States;

- Collect homeland defense threat information from relevant private and public sector sources, consistent with US constitutional authorities and privacy law;
- Identify capability needs for CBRNE sensors to meet homeland defense requirements; and
- Develop automated tools to improve data analysis and management, in order to systematically track large amounts of data, and to detect, fuse, and analyze aberrant patterns of activity, consistent with US privacy protections.

Core Capability: Collect, analyze, and understand potential threats

Improving our understanding of America's foreign enemies—in advance of an attack—is at the heart of DoD's efforts to achieve maximum awareness of potential threats. In accordance with the National Strategy for Combating Terrorism (2002), we are strengthening DoD's knowledge of foreign terrorist networks and the inner workings of their operations.

Improved human intelligence, particularly in the forward regions of the world, is the single most important factor in understanding terrorist organizations. The Department of Defense is currently undertaking a focused review of DoD human intelligence capabilities, including reforms to improve HUMINT career development, policies, practices, and organizations. It is critical that DoD HUMINT operators have relevant linguistic skills and cultural

understanding as well as the technical skills needed to provide high quality, insightful information to the analysts within the Intelligence Community.

In addition, we will **develop a cadre of specialized terrorism intelligence analysts within the Defense intelligence community** and deploy a number of these analysts to interagency centers for homeland defense and counterterrorism analysis and operations. The Department will continue to maintain significant counterterrorism collection and analytical capability to support military activities overseas and in the approaches to the United States.

National agencies within the Department, such as the National Security Agency and the National Geospatial-Intelligence Agency, will continue to provide their unique capabilities in support of the national homeland security mission in accordance with applicable laws and regulations. The Department will also maintain an analytical capability to identify threats to defense critical infrastructure.

Core Capability: Detection, identification, and tracking of emerging threats in all operational domains

We face challenges in our ability to detect, identify, and track objects in all operational environments, but especially the air and maritime domains. Every day, thousands of US and foreign vessels and aircraft approach and depart American ports and airports and those of our closest neighbors. The sheer volume of cargo and diversity of passengers in these operational domains challenges US capabilities.

To detect and track anticipated air and maritime threats effectively, the United States must have capabilities to cue, surveil,

identify, engage, and assess potential threats in real time. Detection and tracking capabilities must be all-weather, around-the-clock, and effective against moving targets. The United States must also have the ability to detect CBRNE threats emanating from any operating environment. **This requires a comprehensive, all-domain CBRNE detection architecture, from collection to analysis.**

The maritime picture is multi-jurisdictional, with various US agencies responsible for tracking vessels from their departure at foreign ports to their arrival in the United States. Recognizing the potential vulnerability this situation creates, DoD is working closely with interagency partners, especially the Department of Homeland Security, to establish a unified concept for maritime domain awareness (MDA)— the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States.

Based on the emerging MDA concept, the Department of Defense will work with interagency partners to develop a comprehensive intelligence, surveillance, and reconnaissance capability to detect threats as far forward of the US homeland as possible, ideally before threat vessels depart foreign ports. **DoD will ensure persistent wide-area surveillance and reconnaissance of the US maritime approaches, layered and periodically varied in such a manner that an adversary cannot predict or evade observation.** Surveillance will also be long-range in all dimensions of the maritime domain. The nation will benefit from the Department of Homeland Security's work to institute worldwide cargo and crew reliability mechanisms. DoD, in concert with the

Department of Homeland Security, will receive and share data from improved identification systems for small commercial and other vessels, just as it has done for maritime vessels of over 300 gross tons that are on international voyages.

Achieving threat awareness in the air operational domain presents similar challenges. Throughout the Cold War, the Department of Defense focused on maintaining awareness of external threats that entered US airspace from overseas. The attacks on September 11, 2001, however, originated in US airspace and highlighted weaknesses in domestic radar coverage and interagency air defense coordination. Adversaries might maintain low altitude flight profiles, employ stealth and other defense countermeasures, or engage in deception to challenge US air defenses. Though substantial, the requirements for domestic air defense are achievable.

Since the attacks of September 11, 2001, DoD has coordinated with interagency partners to significantly improve the air defense of the United States. DoD has worked with the Federal Aviation Administration (FAA) to integrate domestic radar coverage and has conducted Operation Noble Eagle air patrols to protect designated US cities and critical assets. We have placed particular emphasis on implementing a robust air defense capability for the National Capital Region, using both air and ground air defense forces. DoD has also worked closely with interagency partners to exchange a wide range of information regarding potential threats.

The Department of Defense will continue to work with domestic and international partners to develop a persistent, wide-area

surveillance and reconnaissance capability for the airspace within US borders, as well as over the nation's land and maritime approaches. This capability requires the development of advanced technology sensors to detect and track low altitude air vehicles across a wide geographic area. DoD is investigating various technologies that could provide an over-the-horizon engagement capability to detect enemy threats in the approaches or over US territory, leading to their defeat. The United States and our allies must also integrate sensor and intelligence data to identify hostile air vehicles by observing their performance characteristics, suspicious activities, or other attributes. These capabilities in the air domain will provide timely threat detection, extending the depth of air defenses and the time for response, thereby providing multiple engagement opportunities to defeat identified threats.

Core Capability: Shared situational awareness within DoD and with domestic and foreign partners

Shared situational awareness is defined as a common perception of the environment and its implications. All domestic and foreign partners within the homeland defense mission space require situational awareness for three reasons: to identify threats as early and as distant from US borders as possible; to provide ample time for an optimal course of action; and to allow for a flexible operational response. From the March 2003 Homeland Security Information Sharing Memorandum of Agreement, to the aggressive and unprecedented information sharing underway at the NCTC, the US Government continues to make great strides in overcoming obstacles to shared situational awareness.

During the Cold War, the Department of Defense sought shared situational awareness with the Department of State, the Intelligence Community, and allied nations in order to deter and defeat threats posed by the Soviet Union and other nations. At the same time, the American law enforcement community worked with its international counterparts to thwart international drug cartels and a growing number of worldwide crime syndicates.

Today, transnational terrorists have blurred the traditional distinction between national security and international law enforcement. Together with a significant proliferation in the number and type of potential foreign threats, **this expanded national security challenge necessitates an unprecedented degree of shared situational awareness among federal agencies, with state, local, tribal, and private entities, and between the United States and its key foreign partners.**

As a first step, the Department of Defense must provide seamless connectivity and timely, accurate, and trusted information to all DoD Components—any time, any place—in order to achieve maximum awareness of potential attacks against the United States. The Department will therefore ensure that DoD's information infrastructure provides an integrated, interoperable worldwide network of information technology products and management services. This will allow users across DoD to process information and move it to warfighters, policymakers, and support personnel on demand. Network connectivity must be flexible enough to support global operations while allowing for local requirements and innovation. **It must also create a real-time link among sensors, decision makers, and warfighters to**

facilitate the rapid engagement of enemy targets.

Beyond building an integrated information infrastructure, DoD must also populate that network with accurate, timely, and actionable data. Today, information relevant to protecting the United States is widely dispersed. The Department, in concert with the intelligence and law enforcement communities and foreign partners, will build on the great strides already made to diminish existing cultural, technological, and bureaucratic obstacles to information sharing. The Intelligence Community and Department of Defense will drive improved information sharing within a “need to share” context. The resulting information exchange, commonly referred to as “horizontal integration of intelligence,” will provide analysts across the US government and partner nations with timely and accurate all-source information, vastly improving the creation of a coherent and fully integrated threat picture. Such an expansion in information sharing requires appropriate safeguards to ensure that DoD intelligence components rigorously apply laws that protect Americans’ civil liberties and privacy.

Capabilities for Intercepting and Defeating Threats at a Safe Distance

Core Capability: Interception and defeat of national security threats in the maritime and air approaches and within US territory

Maritime Operational Domain. The United States must be prepared for the foreseeable threat of transnational terrorists, detected on the high seas and armed with weapons of

mass destruction. Accordingly, we will fully integrate our surface, subsurface, air, and surveillance assets, focus them forward, and extend the Nation’s maritime defensive perimeter further out to sea in order to deter and defeat maritime threats at a safe distance from the US coast.

Enhancing our ability to intercept enemies in the maritime domain requires a seamless system of overlapping defenses—both adaptable and flexible—to frustrate enemy observation and avoid predictability. This begins in the forward regions with improved surveillance capability, increased HUMINT collection, and enhanced international partnerships through programs like the Container Security Initiative and Proliferation Security Initiative. To maximize maritime domain awareness, successive layers of surveillance must be fully coordinated with the operational activity of our forward deployed forces.

DoD has established standing orders for conducting maritime homeland defense and maritime interception operations. Given this guidance, geographic combatant commanders will include interception exercises in their theater security cooperation plans and conduct such exercises on a periodic basis. The US Navy and US Coast Guard will conduct routine and frequent maritime interception exercises to ensure a high state of training and readiness.

To intercept and defeat transnational threats, the Department of Defense and Department of Homeland Security must have a predetermined process for ensuring rapid, effective US Coast Guard support to the US Navy and vice versa. Although DoD has the lead role in defending the United States from direct maritime attack, we recognize the US

Coast Guard's lead responsibility for maritime law enforcement and homeland security. We will continue to support the US Coast Guard in fulfilling its homeland security responsibilities. Together with the US Coast Guard, we must build upon the security in our ports and littorals, expanding maritime defense capabilities further seaward in support of national security. **This includes strengthening the 96-hour notice of US arrival requirement by including a "consent to board" provision as a prerequisite for entry into a US port.**

The United States must have a concept of operations for the maritime defense of the homeland. Such a concept may require the routine assignment of naval forces to US Northern Command. DoD will also consider the use of US Naval Reserve forces to undertake unique roles in maritime homeland defense. In addition, the US Navy should assess the integrated benefit of forces currently available in support of Operation Noble Eagle, available coastal patrol craft, and the utility of the Navy's littoral combat ship to execute the maritime homeland defense missions.

Air Operational Domain. The Department of Defense will defeat air threats to the United States, such as ballistic and cruise missiles and attacking military aircraft. DoD must also be prepared to intercept non-traditional air threats, even when the intent to harm the United States is more uncertain, as initially occurred on September 11, 2001. These threats could include commercial or chartered aircraft, general aviation, ultralight airplanes, unmanned aerial vehicles, radio controlled aircraft, or even balloons. Early detection and successful interception of these types of potential threats requires very close cooperation with DoD's interagency partners.

Since September 11, 2001, the Department of Defense, through Operation Noble Eagle, has conducted air patrols to protect major US population centers, critical infrastructure, and other sites. Working with our interagency partners, DoD will continue these patrols to intercept air threats to the US homeland as long as required by the projected threat.

The Department of Defense will continue to improve the air-to-air and ground-to-air capabilities and associated forces necessary to intercept and defeat all domestic air threats. For air patrol missions, DoD will use more capable aircraft as they are fielded and explore the potential for employing unmanned combat air vehicles. DoD is also upgrading ground-based air defense assets with improved detection and targeting capabilities.

The Department of Defense will devote significant attention to defending US territory against cruise missile attacks. Defense against cruise missiles poses unique challenges, given that their low altitude and small size make them more difficult to identify and track than traditional air threats. The Department of Defense is developing integrated capabilities to defend against cruise missiles, as well as other types of unmanned aerial vehicles. As an interim step, DoD is developing a deployable air and cruise missile defense capability to protect designated areas. This will integrate Service tactical air defense assets, the NORAD air defense system, interagency information sources, and advanced technology sensors. **Future air and cruise missile defense assets will be fully interoperable, increase the size of the defended area, and engage threats at increased range.**

DoD will also continue to work with interagency partners to develop a common air surveillance picture that will enhance our ability to identify and, ultimately, defeat enemy targets. Improved sensors are also required to detect and track potential air threats within the United States. The current radars maintained by the Federal Aviation Administration to track air traffic within the United States are aging, with high maintenance costs, poor reliability, and reduced capability to track emerging threats. **The nation will need to develop advanced, follow-on sensors to the current generation of radars in order to improve tracking and identification of low-altitude threats.**

Land Operational Domain. The Department of Defense will be prepared to deter and defeat direct, land-based attacks against the United States. We must work closely and cooperatively with our neighbors, establish seamless relationships and organizational structures with interagency partners, and be prepared to respond with military forces on our own soil quickly, responsively, and in a manner that is well coordinated with civilian law enforcement agencies.

Historically, the United States relied almost exclusively on forward deployed forces to confront and defeat nation-state adversaries overseas. Although military power projection remains crucial, transnational terrorism has significantly reduced the effectiveness of this singular approach. Now and in the future, we must be prepared in every part of the globe—most especially the US homeland—to deter, prevent, and defeat terrorist or other asymmetric threats.

The majority of infrastructure in the United States is privately owned. Consequently, private owners provide the first line of

defense for most of the nation's assets. Should that defense prove insufficient, or public welfare is threatened, local, state, and, if necessary, federal authorities will assist in intercepting and defeating threats on US territory. By law and national policy, DoD's role on US soil is relatively circumscribed. The following three-tiered approach provides the parameters under which the military would likely operate:

Tier 1: Local and federal law enforcement.

When directed by the President or the Secretary of Defense, DoD will provide appropriate defense assets in support of domestic law enforcement authority, normally in support of a lead federal agency such as the FBI. Under these circumstances, military forces and assets will remain under the command and control of a DoD authority.

Tier 2: National Guard forces not on active duty. When directed by the Governor or appropriate state authority, National Guard forces and assets can respond quickly to intercept and defeat terrorist threats within US territory.

Operating in either State Active Duty or Title 32 status, National Guard forces can provide support to civilian law enforcement authorities in two key areas. First, National Guard counternarcotics efforts can enhance the effectiveness of counterterrorism initiatives through information-sharing, logistics support, and combined operations. Second, by virtue of their status under state law and Title 32 of US Code, National Guard forces provide civilian authorities with a flexible option under the Military Support for Civilian Law Enforcement Agencies (MSCLEA) construct.

Newly expanded authorities under Title 32 of US Code—and the National Guard’s on-going transformation into a truly 21st century force—will provide Governors and state authorities with flexible, responsive, multi-capable units to deter and defeat localized terrorist attacks. For example, National Guard reaction forces—scalable in terms of size and mix of skills—can provide security for critical infrastructure, support civilian law enforcement agencies in responding to terrorist acts, and offer their neighbors immediate assurance of safety and security.

Tier 3: US military forces responding to Presidential direction. If circumstances warrant, the President or the Secretary of Defense may direct military forces and assets to intercept and defeat threats on US territory. **When conducting land defense missions on US territory, DoD does so as a core, warfighting mission, fulfilling the Commander in Chief’s Constitutional obligation to defend the nation.** To fulfill this responsibility, DoD will ensure the availability of appropriately sized, trained, equipped, and ready quick reaction forces (QRFs) and rapid reaction forces (RRFs).

Capabilities for Providing Mission Assurance

Core Capability: Enhanced preparedness of DoD installations for direct threats, especially CBRNE attacks

Improving DoD’s capabilities for mitigating and, if necessary, operating in a CBRNE-contaminated environment will require progress in detecting and identifying threats

(sense), providing early warning (shape), protecting forces and installations (shield), and ensuring the ability to operate in a contaminated environment (sustain). DoD’s Joint Chemical and Biological Defense Program is focused on developing and fielding technologies to mitigate, and if necessary, allow forces to operate in CBRNE contaminated environments.

Sense. DoD currently has a range of capabilities to detect, identify, and quantify airborne, waterborne, and other hazards. Needed improvements include advanced standoff and point detection capabilities for chemical and biological threats. DoD is also working to develop and field standoff detection capabilities for explosives. Advances in standoff detection capability will enhance the Department’s ability to detect nuclear devices as well as weapons using explosives to disperse chemical, biological, and radioactive materials. Finally, the Department is improving medical surveillance capabilities both on installations and within surrounding communities to provide early detection and identification of CBRNE events in the workforce.

Shape: DoD characterizes CBRNE attacks by assimilating information drawn from sensors and elsewhere to inform commanders of impending or approaching threats. The Department is continuing to improve on early CBRNE threat characterization by developing an integrated concept of operations for sensing, reporting, and warning of CBRNE attacks, ensuring compatibility with national-level CBRNE sensor architectures currently in operation, such

as BLOWATCH, and those under development.

Shield: The Department will continue to provide force protection in advance of a potential CBRNE attack, whether overseas or at domestic installations. Already, 750,000 US military personnel have been vaccinated against anthrax; 650,000 are vaccinated against smallpox. The Department is now focusing on the development of vaccines and other capabilities that can address new and emerging biological and chemical threats. This includes significant research on technologies for improved chemical and biological agent detection and personal and collective protection equipment. DoD is also preparing to field capabilities that protect US forces from chemical agents that can be absorbed through the skin.

Lastly, the Department is deepening and expanding collaboration on biodefense research with the Department of Homeland Security and the Department of Health and Human Services. This includes significant new investments by these civilian agencies and the creation of a new research consortium. The construction of a National Interagency Biodefense Campus, collocated with the US Army Medical Research Institute of Infectious Diseases (USAMRIID), will significantly facilitate civil-military cooperation in this area. A revitalized and recapitalized USAMRIID, along with major Department of Homeland Security and Department of Health and Human Services investments, will provide DoD and the nation with added research capacity, additional biopharmaceutical development, increased testing and evaluation of potential biodefense medical

products, and large surge lab capacity for bioterrorism incident response.

Sustain: DoD must be able to sustain operations during and after a CBRNE attack in the United States. Medical therapeutics that allow DoD personnel to continue mission-essential tasks in a CBRNE environment are of highest priority. DoD will also expand pilot programs for CBRNE installation preparedness to protect DoD personnel and facilities in the event of an attack. In addition to providing enhanced CBRNE defense capabilities at 200 critical installations in the United States and abroad, DoD will improve preparedness and protection of all installations through updated doctrine and guidance. The Department will examine an aggressive expansion of this installation preparedness program to increase both the level of protection and the number of DoD installations it covers.

Core Capability: Crisis management and DoD continuity preparedness

The Department's crisis management and continuity of operations programs are central to mission assurance. DoD must provide capabilities necessary to support senior leadership decision-making and military command and control and to perform essential DoD functions to support national-level crisis managers. DoD is working to enhance its information management and communications capabilities to support senior leadership in crises. It is also improving the survivability and flexibility of military command and control capabilities.

A significant element of mission assurance is **continuity of operations**—maintaining the ability to carry out DoD mission essential

functions in the event of a national emergency or terrorist attack. Fulfilling this objective in the current security environment necessitates new and innovative approaches. Some of these approaches include policies for personnel dispersion, leveraging advances in information technology to improve crisis coordination, and improving relocation facilities. The Department recently conducted a zero-based assessment of DoD continuity capabilities. The results of this assessment detail numerous capability improvements that the Department can pursue in order to ensure the continuity of DoD operations in times of crisis. It also provides recommendations that will transform DoD's approach to continuity operations from a Cold War-oriented operational concept to one better suited to address the current and evolving terrorist threat. The recommendations include the use of new and emerging technologies and the development of more flexible relocation options.

Core Capability: Preparedness and protection of defense critical infrastructure

Because resources are constrained, uniform protection of all defense critical infrastructure is not possible. **The Department must prioritize the protection of assets based on their criticality to executing the National Defense Strategy and seek to minimize the vulnerability of critical assets in accordance with integrated risk management approach.** To this end the Department will devise a strategy to:

- Identify infrastructure critical to the accomplishment of DoD missions, based on a warfighter mission area analysis.

- Assess the potential effect of a loss or degradation of critical infrastructure on DoD operations to determine specific vulnerabilities, especially from terrorist attack.
- Manage the risk of loss, degradation, or disruption of critical assets through remediation or mitigation efforts, such as changes in tactics, techniques, and procedures; minimizing single points of service; and creating appropriate redundancies, where feasible.
- Protect infrastructure at the direction of the President or the Secretary of Defense where the nature of the threat exceeds the capabilities of an asset owner and civilian law enforcement are insufficient.
- Enable real-time incident management operations by integrating current and emerging threat monitoring and reporting with existing critical infrastructure network data and analysis through the Mission Assurance Support Center within the Defense Program Office for Mission Assurance.

The Military Departments, Defense Agencies, and other DoD components are now implementing the Protective Risk Management Strategy through modifications to their programs and budgets.

Core Capability: Preparedness of the Defense Industrial Base

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (2003) notes that, **without the important contributions of the private sector, DoD cannot effectively execute core defense missions.** Private industry

manufactures and provides the majority of the equipment, materials, services, and weapons for the US armed forces. Ensuring that military forces are properly equipped is critical to maintaining DoD power projection and homeland defense capabilities. In that regard, the President recently designated DoD as the Sector-Specific Agency for the Defense Industrial Base (DIB). **In this role, DoD is responsible for national infrastructure protection activities for critical defense industries as set forth in Homeland Security Presidential Directive-7.**

To assure that mission critical supplies and services are available, DoD contracts are being modified to ensure that appropriate protective measures are in place at key facilities and appropriate information is shared with the DoD to assess the security of the DIB. In addition, the Defense Logistics Agency and other DoD contracting activities are revising the contract process to ensure that civilian defense contractors are able to operate for the duration of a national emergency. **Defense contractors must be able to maintain adequate response times, ensure supply and labor availability, and provide direct logistic support in times of crisis.** Contracts will also require DoD program managers to be accountable for ensuring the protection of supporting infrastructure, including key suppliers. DoD base and installation commanders, and those who contract for non-DoD infrastructure services and assets, will monitor assurance activities through compliance with contract language that clearly identifies reliable service availability, priority of restoration, and asset protection.

Core Capability: Preparedness to protect designated national critical infrastructure

The Department has historically focused on preventing unauthorized personnel from gaining access to DoD installations and protecting those installations from traditional military attacks. **In the post-September 11, 2001 era, DoD is expanding the traditional concept of critical asset protection to include protection from acts of transnational terrorism.** Countering terrorist reconnaissance activity is central to the successful defense of critical infrastructure.

As outlined in the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2003), DoD bears responsibility for protecting its own assets, infrastructure, and personnel. At the Department's request, domestic law enforcement may assist with protection functions at DoD facilities.

For non-DoD infrastructure, to include private and public assets that are critical to the execution of the defense strategy, DoD's protection role is more limited. The initial responsibility for protection of non-DoD infrastructure rests with asset owners. Civilian law enforcement authorities augment and reinforce the efforts of asset owners, creating a second tier of protection.

Should protection requirements exceed the capabilities of asset owners and civilian law enforcement, state authorities provide an additional layer of defense. In addition to a governor's authority to employ National Guard forces in a state active duty status, recent changes to Title 32 of US Code will provide an additional, expeditious means to mobilize National Guard forces under the

control of the governor using federal funding to defeat a foreign terrorist threat.

To achieve critical infrastructure protection in the most serious situations, the Department of Defense maintains trained and ready combat forces for homeland defense missions.

Capabilities for CBRNE Consequence Management

Core Capability: Consequence management assistance for domestic CBRNE mass casualty attacks

Acknowledging the challenges presented by the current security environment, the Department of Defense must be able to conduct most major combat operations in a CBRNE environment. US military forces organize, train, and equip to operate in contaminated environments, as well as manage the consequences of CBRNE incidents, on a level unmatched by any other single domestic agency or international partner. **If directed by the President or the Secretary of Defense, the Department of Defense must be prepared to use these capabilities to assist interagency partners in the aftermath of domestic CBRNE mass casualty attacks.** DoD's CBRNE capabilities include specialized agent detection and identification systems as well as casualty extraction and mass decontamination abilities. DoD can also provide significant support to domestic consequence management by providing emergency medical support, such as equipment, mobile hospitals, medical personnel, engineering support, and mortuary services.

Not all domestic CBRNE incidents will necessitate a federal response; many

scenarios may be well within the capabilities of state and local responders.

Those incidents that do require a US government response will be coordinated by a lead federal agency. In most catastrophic scenarios, DoD may be called upon to provide support to the Department of Homeland Security or another lead federal agency. **The Department will work closely with interagency partners—through the National Response Plan and the National Incident Management System—to ensure proficiency and interoperability in responding to multiple CBRNE incidents.**

The Department will ensure that its dedicated CBRNE civil support assets are sized, trained, equipped, and ready for the domestic consequence management mission. This will include planning for the potential augmentation of existing National Guard WMD Civil Support Teams (CSTs) with other National Guard capabilities and forces that are task-organized for this mission.

DoD will also identify, train, and equip an additional, discrete number of military forces for the potential requirements associated with multiple, simultaneous CBRNE attacks within the United States. These forces will be dual-mission in nature—these warfighters and support elements will not be dedicated to the civil support role but they will nevertheless be ready to perform domestic consequence management missions when required.

Lastly, the Department will ensure that other elements of the Total Force—currently sized and shaped primarily for overseas missions—are identified, exercised, and ready to support CBRNE consequence management as necessary. This capability will provide added utility for overseas deployments or domestic missions. Within this Total Force context,

DoD's effectiveness in responding to domestic CBRNE contingencies will be greatly improved through adjustments to Active and Reserve Component training, procedures that allow for faster mobilization of National Guard and Reserve Forces, and improved command relationships that make optimal use of the Reserve Component. This includes leveraging the National Guard's Joint Force Headquarters-State organizations.

Enhancing US and International Capabilities for Homeland Defense and Homeland Security

Core Capability: Interagency planning and interoperability

Recognizing the critical importance of interoperability, DoD will share training, planning, and other appropriate resources with interagency partners to standardize operational concepts, develop technology requirements, and coordinate budget planning for homeland missions. Interagency efforts must focus on closing any remaining seams in air, land, maritime, cyberspace and space operational domains and must enhance national preparedness and incident management efforts. Development of a coordinated training and exercise program is an essential step toward enhanced cooperation in executing homeland defense and civil support missions.

Active DoD participation in the interagency process improves planning and interoperability and will ensure that procedures for supporting civil authorities are consistent with the framework for domestic incident response outlined in the

National Response Plan and the National Incident Management System. DoD will work closely with interagency partners to identify how best to coordinate interagency civil support activities.

Core Capability: Capable federal, state, and local partners and effective domestic relationships

The Department of Defense has identified three tenets to enhance defense support of civil authorities:

- Augment civil capabilities with DoD expertise where necessary;
- Ensure the seamless operational integration of defense support capabilities with those of the civil sector;
- Assist in the civil sector's development, procurement, and sourcing of new technologies and equipment.

Within this civil support framework, the Department will actively seek to identify opportunities for cooperation with the civil sector. Several initiatives to enhance civilian capabilities are already underway. Examples include:

- DoD assistance to the Department of Homeland Security to develop CBRNE victim rescue capabilities, similar to those of the US Marine Corps' Chemical Biological Incident Response Force.
- Joint DoD and Department of Homeland Security research and development on, and civilian acquisition of unmanned aerial vehicles for law enforcement and

IV. Core Capabilities

ground surveillance systems for border security.

- DoD efforts through the Interagency Counter Man-Portable Air Defense System (MANPADS) Task Force to help develop an attack prevention and recovery plan, provide technical advice and analysis to the Department of Homeland Security regarding MANPAD countermeasures, and operational assistance to stem the proliferation of MANPADS overseas.

In compliance with Section 1401 of the National Defense Authorization Act for FY 2003, DoD will continue to engage in efforts to transfer competencies between DoD and the civil sector—through technology transfer as well as sharing DoD's "lessons learned" from applicable exercises and program management. **Such collaborative efforts can increase the overall effectiveness of national capabilities and potentially reduce other agencies' dependencies on limited DoD assets.**

To succeed, the Department will need a systematic approach to ensure close coordination with the Department of Homeland Security and other interagency, state, and local partners, specifically:

- Facilitating the Department of Homeland Security's efforts to identify and provide appropriate and applicable defense technologies to state and local first responders;
- Nurturing new collaborative research, development, experimentation, test and acquisition opportunities with the Department of Homeland Security, while avoiding duplication of effort in these areas; and

- Ensuring the smooth transition of appropriate missions, technologies, and capabilities to the civil sector.

Complementing these activities will be a long-term effort with our federal partners to identify specific, frequently requested DoD capabilities for possible transition to the civil sector.

Core Capability: Capable international partners and effective defense-to-defense relationships

Because it is the Department's first priority, homeland defense must be a central, carefully considered element of our defense-to-defense relationships with key allies and friends abroad. The United States fosters strong defense relationships worldwide for many reasons of national security interest. Two such reasons are to strengthen allied military contributions to collective security and to enhance US capabilities through exposure to partners' expertise. Thus, DoD has an active security cooperation program, directed through the Secretary of Defense's Security Cooperation Guidance, that encourages mutual improvements to support coalition operations and to ensure continued interoperability. Clearly, our homeland defense will be substantially strengthened through the cooperation and assistance of international allies. **We will therefore strengthen DoD's emphasis in the Security Cooperation Guidance on homeland defense and civil support issues, with particular focus on improved information sharing in defense-to-defense interactions.**

Our North American neighbors, Canada and Mexico, are particularly vital to the protection of the US homeland and the continent. The Department also places special emphasis on

IV. Core Capabilities

cooperative homeland defense efforts with friendly nations in the Pacific and the Caribbean and with our NATO allies.

The primary mechanism for US-Canadian cooperation on homeland defense is the North American Aerospace Defense Command. Dedicated to the defense of US and Canadian airspace, NORAD has evolved from a Cold War institution to an agile 21st century counterterrorism capability reflecting an integrated, flexible bi-national approach to air defense. Over the next decade, the Department of Defense, in conjunction with the Department of State and the Department of Homeland Security and working with our Canadian partners, will further refine and build on the NORAD concept. This effort will identify mechanisms for sharing information across all operational domains—air, maritime, and land, with shared awareness of the North American maritime domain as the first priority.

Given the importance of Mexico to US homeland defense, US-Mexican counterterrorism cooperation is essential. The Department will work with the Department of Homeland Security and Mexico to anticipate and plan for crisis coordination and consequence management following a terrorist attack. Cooperation with Mexico on law enforcement and immigration issues is substantial, especially in counternarcotics and

border control operations. Defense-to-defense cooperation requires similar emphasis and must be pursued with due respect for the Mexican government's policy goals and legal constraints. Traditional security assistance tools are pivotal in further developing mutually beneficial defense capabilities and arrangements.

Just as US defense of the homeland begins well beyond our geographic boundaries, so too must our cooperative efforts to improve that defense. The expansion of information and intelligence sharing with foreign partners is critical to the success of this Strategy. Friendly and allied nations often possess significant information relating to counterterrorism, smuggling, and other US concerns. Incorporating this information into our base of knowledge could significantly improve US readiness both for homeland defense and civil support missions.

Beyond the information realm, some nations have significant expertise to share with the United States in counterterrorism and other mission areas related to homeland defense. The United States likewise has much to gain in increasing the homeland defense capabilities of friendly nations. The Department will therefore expand combined education, exercise, training, and experimentation initiatives related to homeland defense.



V. Implications of the Strategy

"The threats and enemies we must confront have changed, and so must our forces."

The National Security Strategy of the United States of America

September 2002

The Strategy for Homeland Defense and Civil Support requires adjustments in DoD forces and capabilities, resource allocation, and technology development. Given resource constraints, meeting the Strategy's homeland defense and civil support objectives will require accommodation of competing demands within the National Defense Strategy.

Force Structure

An understanding of the force structure implications of the Strategy for Homeland Defense and Civil Support is critical to the Department's ability to size and shape forces correctly for diverse military missions. **This strategy reflects a Total Force approach to homeland defense missions, incorporating the capabilities of Active Duty, National Guard, and Reserve forces that will be trained and equipped primarily for warfighting missions in the forward regions and approaches.** Identified forces must also be prepared to conduct the full spectrum of domestic civil support missions when directed by the President or the Secretary of Defense to do so. The types of forces employed for any given homeland defense mission will be situation-dependent. Additionally, the type, scope, and location of events, competing DoD missions, resident civilian capabilities, and

a host of other variables will affect requests for defense support of civil authorities. To execute this diverse range of missions effectively, DoD must ensure the Total Force, both reserve and active components, is:

- **Timely** in response and readily accessible. Homeland defense and civil support missions require a rapid response, often measured in hours, not days.
- **Trained and equipped** to achieve the highest degree of readiness in a broad array of mission sets.
- **Transformed** to meet the terrorist challenges of a post-Cold War security environment. Forces must be agile and interoperable, taking advantage of networked capabilities.
- Consistent with the objectives of this Strategy, and in preparation for the next Quadrennial Defense Review, the Department will undertake a thorough analysis of force requirements for homeland defense missions. This analysis will take into account the projected capabilities of civilian agencies where those capabilities may affect DoD's force requirements. **A preliminary assessment suggests modest changes in several major mission areas and the potential for more**

substantial adjustments to maritime defense forces.

Focused Reliance upon the Reserve Component

Homeland defense and civil support are Total Force responsibilities. However, the nation needs to focus particular attention on better utilizing the competencies of the National Guard and Reserve Component organizations. The National Guard is particularly well suited for civil support missions. It is forward deployed in 3,200 communities through the nation, readily accessible in State Active Duty and Title 32 status, routinely exercised with local law enforcement, first responders, and the remainder of the Total Force, and experienced in supporting neighboring communities in times of crisis. In addition, Reserve forces currently provide many of the key capabilities needed for homeland defense and civil support, including intelligence, military policing, medical expertise, and chemical decontamination. The most promising areas for employment of the National Guard and Reserve forces include the following missions:

- *Air and Missile Defense*, including surveillance and manning of ground-based defense systems.
- *Maritime Security*, including Naval Reserve augmentation of active component and Coast Guard capabilities engaged in intelligence and surveillance, critical infrastructure protection, port security, and maritime intercept operations. **Traditional Cold War missions for the Naval Reserve should be transformed to reflect the 21st century transnational terrorist**

threat, most especially the maritime transportation of weapons of mass destruction to the United States.

Therefore, DoD will evaluate the operational benefit of employing Naval Reserve maritime and aviation capabilities in support of emerging homeland defense missions.

- *Land defense*, including missions requiring Quick Reaction Forces/Rapid Reaction Forces. **The National Guard Bureau has recommended that the Army use existing National Guard force structure to form modular Reaction Forces, an initiative that could provide additional capabilities to support land defense mission requirements.** Other Reserve forces, including the Army Reserve and Marine Corps Reserve, are also capable of serving in reaction force roles.
- *CBRNE response*, including specific capabilities for detection, extraction, decontamination, and medical care. **The Army National Guard Chemical-Biological-Radiological-High Explosives Enhanced Force Packages (NGCERFPs) effort is a promising initiative well tailored to CBRNE response.** The NGCERFPs are task-organized, using existing National Guard force structure. **The effective employment of National Guard forces in state or Title 32 status could increase the availability of US military forces for overseas deployments.**

Chemical companies resident in the Army Reserve can provide

significant capabilities and are trained and equipped for CBRN assessment as well as extraction and decontamination of mass casualties. The Reserve Component can also offer significant assistance with security, engineering, transportation, communications and other general-purpose homeland defense requirements related to CBRNE response.

- *Critical Infrastructure Protection*, including the performance of comprehensive assessments at critical infrastructure sites and utilization of Reserve Component forces for quick reaction requirements and local security at key defense and non-defense critical infrastructure sites, when directed.

Technology

Implementation of the Strategy for Homeland Defense and Civil Support may require several new technological investments. Three areas of particular interest for further exploration are advanced information and communications technology, new generations of sensors, and non-lethal capabilities.

Advanced Information and Communications Technology

Technological and organizational improvements for homeland security and homeland defense will benefit from focused investment in advanced information technology especially to prevent, intercept, and respond to terrorist activity. Whether the objective is improved maritime domain awareness and operations, interception of

weapons of mass destruction, response to chemical or biological attacks, or continuity of operations and government, improvement in information technology is a critical enabler to addressing current capability shortfalls. Advanced modeling and simulation techniques for threat identification, pattern analysis, risk assessment, dependency analysis, and cost/benefit calculus are critical for addressing issues of data sharing, security, and interoperability. Without these tools, the return on investments in other areas, such as improved sensors, detectors, command and control, and human intelligence (HUMINT) collection and analysis, will be incomplete and insufficient.

Equally pivotal are potential advances in communications technologies, particularly those supporting ground-mobile and airborne communications. DoD must also work to reduce the size and power requirements of mobile communications systems. It must also invest in technologies that shield them against electromagnetic effects.

Sensors

New generations of sensors and sensor platforms will enhance threat awareness in the air, maritime, and land domains by helping to close current gaps over much of the maritime domain and in domestic airspace, particularly at low altitudes. Shared sensor technology will also play an important role in enabling improved border surveillance by civilian agencies.

The placement of sensors on high altitude platforms, including new generations of unmanned aerial vehicles, satellites, and aerostats, will allow sustained surveillance

of wide areas of the earth's surface. These sensors will also enhance defenses against low-flying cruise missiles. Some new ground sensors will have an over the horizon capability with applications for homeland defense and homeland security missions.

New sensor technologies are also required for maritime defense, including the non-acoustic detection of underwater vehicles, objects, and swimmers. New sensor capabilities will be needed for a wide range of other tasks, such as remote detection of concealed CBRNE weapons aboard ships and for mapping the location and extent of contamination should adversaries use these weapons. Finally, **DoD must fully integrate its sensors as well as others on which it relies with information networks in order to coordinate their use and rapidly distribute information to operational and policy users.**

Non-Lethal Capabilities

The transnational terrorist attack of September 11, 2001, made it clear that the US homeland is now part of the enemy battle space. Therefore, we may be required to defeat attacks in close proximity to major civilian population centers. Non-lethal capabilities hold some promise as an effective alternative to deadly force. The Department will therefore examine the potential operational employment of non-lethal weapons for homeland defense missions, particularly those where civilian loss of life can be effectively minimized.

Non-lethal technologies with potential application to homeland defense missions include:

- **Counter-personnel technology**, used to deny entry into a particular area, temporarily incapacitate individuals or groups, and clear facilities, structures, and areas.
- **Counter-material technology**, to disable, neutralize, or deny an area to vehicles, vessels, and aircraft, or disable particular items of equipment.
- **Counter-capability technology**, to disable or neutralize facilities, systems, and CBRNE.

The Department will expand basic research into the physiological effects of non-lethal weapons. The Department should also identify opportunities to share appropriate non-lethal capabilities with domestic law enforcement agencies, consistent with applicable law.

Rapid Prototyping of Emerging Capabilities

Advanced Concept Technology Demonstrations (ACTDs) are a key DoD vehicle for rapidly fielding promising technologies. The objectives of an ACTD are to conduct meaningful demonstrations of the capability, develop and test concepts of operations to optimize military effectiveness, and, if warranted, prepare to transition the capability into acquisition without loss of momentum. Currently, there are over 25 ACTDs with relevance to homeland defense and homeland security such as the Homeland Security/Homeland Defense Command and Control Advanced Concept Technology Demonstration. The Department will ensure that requirements for homeland defense and civil support are properly addressed in the ACTD process in

the decade ahead. The Department will continue working with the Department of Homeland Security and other domestic and international partners to encourage their participation in ACTDs as appropriate. **DoD will also continue to leverage innovative capabilities arising from private sector initiatives, many of which are fostered through the interagency Technical Support Working Group (TSWG).**

Funding

With many important programs competing for finite resources, proper funding and budget oversight for homeland defense and CBRNE consequence management missions is vital. Currently, the Department accounts for homeland defense activities through a variety of widely dispersed programs and funding lines. Funding for homeland defense is not accounted for consistently; it can be found in every Military Department and combatant command and numerous initiatives under the purview of the Office of the Secretary of Defense.

Funding Implications

In developing planning and programming guidance to implement the Strategy for Homeland Defense and Civil Support, DoD must thoroughly assess the fiscal implications of attaining and sustaining requisite core capabilities. Determining the relative costs and benefits of each of the following areas merit immediate attention:

- **Expanding communications infrastructure** and enhancing DoD's ability to share vital information while protecting the integrity of the Global Information Grid;

- **Improving intelligence assets** to enhance overall threat awareness throughout all domains;
- Developing and procuring **advanced technologies** to maximize awareness of potential threats;
- Ensuring the necessary capabilities, types, and number of transformational forces needed to effectively conduct an active, layered **maritime defense** against transnational threats, including CBRNE attacks;
- Implementing DoD's **Defense Critical Infrastructure Protection** responsibilities;
- Furthering investments in **non-lethal weapons** research and capabilities;
- Providing support for DoD **continuity of operations** in the event of a national emergency or catastrophe; and
- Implementing **National Guard Bureau transformation** initiatives, such as NGCERFPs, as appropriate.

In the course of implementing this strategy, the Department must not take on responsibilities and costs for homeland security missions better addressed by other federal, state, local, or tribal authorities. This will require close coordination and continuing cooperation with the Department of Homeland Security and other interagency partners, including finding efficiencies in the research, development, testing, acquisition, and deployment of capabilities that span multiple agencies.

Managing Homeland Defense and Civil Support Risk

The Department must employ a risk management strategy that appropriately acknowledges the importance of an active, layered homeland defense. **An active, layered defense integrates homeland defense and forward operations conceptually and operationally.** Therefore, the Department will assess homeland defense and civil support mission risks and resources in the context of all of the requirements outlined in the National Defense Strategy.

The Strategy places a premium on the Department's primary responsibility for protecting the homeland from attack. A second priority is to meet DoD's most challenging civil support mission—CBRNE consequence management. Specifically, the Strategy's risk management approach is as follows:

Lead. The Department's key lead objectives are to achieve maximum awareness of threats, intercept and defeat threats at a safe distance, and provide mission assurance. **DoD must not accept undue risk in its active defense of the US homeland from direct air, land, or maritime threats.** The capability and readiness of US forces to intercept and defeat these threats must be assured. Further, because the most critical element of successfully defeating threats to the homeland is shared situational awareness, the Department will focus

special attention in this area. DoD accepts some operational risk in providing mission assurance.

Support. Transnational terrorists have a demonstrated intent to acquire weapons of mass destruction and exploit US vulnerabilities in order to employ such weapons against potential domestic targets. Accordingly, the Department will reduce risk by improving its consequence management capabilities for responding to multiple, simultaneous CBRNE mass casualty attacks in the United States. **DoD will maintain a ready, capable, and agile command and control structure, along with competently trained forces, to assist civilian authorities with catastrophic incident response. However, with the exception of a dedicated command and control element (currently the Joint Task Force-Civil Support), DoD will continue to rely on dual-capable forces for consequence management and other defense support of civil authorities.** The Department minimizes the risk that dual-capable forces may be assigned to other high priority missions by deconflicting overseas and domestic force requirements wherever possible.

Enable. Enabling domestic and international partner capabilities is an important priority for the Department. **The Department aims to decrease long-term risk by improving the capabilities of our interagency and international partners.** DoD accepts some risk in achieving the "Enable" objective in order to address other, more immediate, "Lead" and "Support" objectives.



VI. Conclusion

"The battle is now joined on many fronts. We will not waver; we will not tire; we will not falter; and we will not fail. Peace and freedom will prevail."

President George W. Bush

October 7, 2001

The United States faces ruthless enemies who seek to break our will and exploit America's fundamental freedoms. Our adversaries are eager to employ violence against Americans at home. In this environment, the Department of Defense's paramount goal will continue to be the defense of the US homeland from direct attack.

A new kind of enemy requires a new concept for defending the homeland. **The terrorist enemy now considers the US homeland a preeminent part of the global theater of combat, and so must we.** We cannot depend on passive or reactive defenses but must seize the initiative from adversaries.

The active, layered defense articulated in this Strategy seamlessly integrates US capabilities in the forward regions of the world, the global commons of space and cyberspace, the geographic approaches to the US territory, and within the United States. Whether in a leading, supporting, or enabling role, the Department of Defense, guided by this Strategy and consistent with US law, will work with an intense focus to protect the US homeland and the American people.

When fully realized, this Strategy will transform the Department's homeland defense and civil support capabilities. The nation will have effective intelligence, surveillance, and reconnaissance

capabilities for homeland defense; and information will be widely shared with relevant decision-makers. The Department will have well-trained and responsive forces for homeland defense missions that will use improved technology and operational concepts to eliminate potential seams between the maritime, air, and land domains. Additionally, **the Department will achieve unity of effort with our interagency and international partners in the execution of homeland defense and civil support missions.**

In implementing the Strategy for Homeland Defense and Civil Support, the Department will carefully consider the potential implications for force structure, technology, and funding. More fundamentally, the Department must change its conceptual and cultural approach to homeland defense. The Department can no longer think in terms of the "home" game and the "away" game. There is only one game.

The effectiveness of any strategy is ultimately in the hands of those charged with its implementation. The Strategy for Homeland Defense and Civil Support is a call for fundamental transformation in military capabilities in order to counter the 21st century threat. Defending the US homeland—our people, property, and freedom—is a fundamental duty. Failure is not an option.

DRAFT

Strategy for Homeland Defense and Civil Support

DRAFT



**Department of Defense
Washington, D.C.**

March 2005



Table of Contents

Executive Summary	1
Secure the United States from Attack through an Active, Layered Defense	1
Organizing Construct—Lead, Support, and Enable	2
Key Objectives of the Strategy	2
Capability Themes for Homeland Defense and Civil Support	3
Projected Implications of the Strategy	4
I. Context	5
Key Definitions	5
Standing Guidance from National and Defense Strategies	5
Security Environment	7
Organizing for Homeland Defense and Civil Support	7
Assumptions	9
II. Active, Layered Defense	10
III. Strategic Goal and Key Objectives	14
Lead	15
Support	19
Enable	19
IV. Core Capabilities	21
Capabilities for Achieving Maximum Awareness of Threats	21
Capabilities for Deterring, Intercepting and Defeating Threats at a Safe Distance	25
Capabilities for Achieving Mission Assurance	28
Capabilities for CBRNE Consequence Management	32
Enhancing US and International Capabilities for Homeland Defense and Homeland Security	34
V. Implications of the Strategy	37
Force Structure	37
Technology	39
Funding	40
Managing Homeland Defense and Civil Support Risk	41
VI. Conclusion	43

Table of Contents



Executive Summary

"The world changed on September 11, 2001. We learned that a threat that gathers on the other side of the earth can strike our own cities and kill our own citizens. It's an important lesson, one we can never forget. Oceans no longer protect America from the dangers of this world. We're protected by daily vigilance at home. And we will be protected by resolute and decisive action against threats abroad."

President George W. Bush

September 17, 2002

Protecting the United States homeland from attack is the highest priority of the Department of Defense (DoD). On September 11, 2001, the world changed dramatically. For the first time since Pearl Harbor, we experienced catastrophic, direct attacks against our territory. This time, however, the foe was not another nation but terrorists seeking to undermine America's political will and destroy our way of life. As a result, the United States has become a nation at war, a war whose length and scope may be unprecedented.

We now confront an enemy who will attempt to engage us not only far from US shores, but also at home. Terrorists will seek to employ asymmetric means to penetrate our defenses and exploit the openness of our society to their advantage. By attacking our citizens, our economic institutions, our physical infrastructure, and our social fabric, they seek to destroy American democracy. We dare not underestimate the devastation that terrorists seek to bring to Americans at home.

To defeat 21st century threats, we must think and act innovatively. Our adversaries consider US territory an integral part of a global theater of combat. We must therefore have a strategy that applies to the domestic context the key principles that are driving the

transformation of US power projection and joint expeditionary warfare.

Secure the United States from Attack through an Active, Layered Defense

This Strategy for Homeland Defense and Civil Support focuses on achieving the Defense Department's paramount goal: securing the United States from direct attack. The strategy is rooted in the following:

- Respect for America's constitutional principles;
- Adherence to Presidential and Secretary of Defense guidance;
- Recognition of terrorist and state-based threats to the United States; and
- Commitment to continue transformation of US military capabilities.

Protecting the United States in the ten-year timeframe covered by this Strategy requires an active, layered defense. **This active, layered defense is global, seamlessly integrating US capabilities in the forward regions of the world, the global commons of space and cyberspace, in the geographic approaches to US territory, and within the United States. It is a defense in depth. To be**

effective, it requires superior intelligence collection, fusion, and analysis, calculated deterrence of enemies, a layered system of mutually supporting defensive measures that are neither passive nor ad hoc, and the capability to mass and focus sufficient warfighting assets to defeat any attack.

This active, layered defense employs tactical defenses in a strategic offense. It maximizes threat awareness and seizes the initiative from those who would harm us. In so doing, it intends to defeat potential challengers before they threaten the United States at home.

Organizing Construct—Lead, Support, and Enable

Although the active, layered defense extends across the globe, this Strategy for Homeland Defense and Civil Support focuses primarily on DoD's activities in the US homeland and the approaches to US territory. In those geographic layers, the Department undertakes a range of activities to secure the United States from direct attack. These generally divide into the following categories:

- **Lead:** At the direction of the President or the Secretary of Defense, the Department of Defense executes military missions that dissuade, deter, and defeat attacks upon the United States, our population, and our defense critical infrastructure.
- **Support:** At the direction of the President or the Secretary of Defense, the Department of Defense provides support to civil authorities. This support is part of a comprehensive national response to prevent and protect against terrorist incidents or recover from an attack or disaster. DoD provides support to a lead federal agency when directed by the President or the Secretary of Defense.
- **Enable:** The Department of Defense actively seeks to improve the homeland defense and homeland security contributions of our domestic and international partners and, in turn, to improve DoD capabilities by sharing expertise and relevant technology, as appropriate, across military and civilian boundaries.

Key Objectives of the Strategy

Within the lead, support, and enable framework for homeland defense and civil support, the Department is focused on the following paramount objectives, listed in order of priority:

- **Achieve maximum awareness of potential threats.** Together with the Intelligence Community and civil authorities, DoD works to obtain and promptly exploit all actionable information needed to protect the United States. Timely and actionable intelligence, together with early warning, is the most critical enabler to protecting the United States at a safe distance.
- **Deter, intercept and defeat threats at a safe distance.** The Department of Defense will actively work to deter adversaries from attacking the US homeland. Through our deterrent posture and capabilities, we will convince adversaries that threats to the US homeland risk unacceptable counteraction by the United States. Should deterrence fail, we will seek to intercept and defeat threats at a safe distance from the United States. When directed by the President or the Secretary of Defense, we will also defeat direct threats within US airspace and on US

territory. In all cases, the Department of Defense cooperates closely with its domestic and international partners and acts in accordance with applicable laws.

- **Achieve mission assurance.** The Department of Defense performs assigned duties even under attack or after disruption. We achieve mission assurance through force protection, ensuring the security of defense critical infrastructure, and executing defense crisis management and continuity of operations (COOP).
- **Support civil authorities in minimizing the damage and recovering from domestic chemical, biological, radiological, nuclear or high-yield explosive (CBRNE) mass casualty attacks.** The Department of Defense will be prepared to provide forces and capabilities in support of domestic CBRNE consequence management, with an emphasis on preparing for multiple, simultaneous mass casualty incidents. DoD's responses will be planned, practiced, and carefully integrated into the national response.

With the exception of a dedicated command and control element (currently the Joint Task Force-Civil Support) and the Army National Guard Weapons of Mass Destruction (WMD) Civil Support Teams, DoD will continue to rely on dual-capable forces for the domestic consequence management mission. These dual-capable forces must nevertheless be trained, equipped, and ready to provide timely assistance to civil authorities in times of domestic CBRNE catastrophes, programming for this capability when directed.

- **Improve national and international capabilities for homeland defense and**

homeland security. The Department of Defense is learning from the experiences of domestic and international partners and sharing expertise with federal, state, local, and tribal authorities, the private sector, and US allies and friends abroad. By sharing expertise, we improve the ability of the Department of Defense to carry out an active, layered defense.

Capability Themes for Homeland Defense and Civil Support

Several important themes underlie the objectives and capabilities established by this Strategy:

- **Intelligence, Surveillance, and Reconnaissance Capabilities.** The Department of Defense requires current and actionable intelligence defining potential threats to US territory. DoD must also ensure that it can identify and track suspect traffic approaching the United States, conducting reconnaissance and surveillance to examine wide areas of the maritime and air domains—and working with lead domestic partners and Canada and Mexico in the land domain—to discover potential threats before they reach the United States.
- **Information-Sharing.** Together with domestic and international partners, DoD will integrate and share information collected from a wide range of sources. The events of September 11, 2001 highlighted the need to share information across federal agencies and, increasingly, with state, local, and tribal authorities, the private sector, and international partners.

- **Joint Operational Capabilities for Homeland Defense.** DoD will continue to transform US military forces to execute homeland defense missions in the forward regions, approaches, US homeland, and global commons.
- **Interagency and Intergovernmental Coordination.** The Department of Defense and our domestic and international partners will continue to cooperate closely in the execution of homeland defense and civil support missions.

When fully realized, this Strategy for Homeland Defense and Civil Support will transform and improve DoD capabilities in each of these areas.

Projected Implications of the Strategy

In developing this Strategy, the Department took into account its likely force structure, resource, and technology implications in order to ensure the appropriate alignment of scarce Department resources with the priorities set forth in the National Defense Strategy. As DoD components implement the strategic tenets outlined in this document, a more precise accounting of the forces, technological advances, and financial resources it requires will be needed.

Because DoD's forces and resources are finite, the Strategy recognizes the need to manage risk within the homeland defense and civil support mission areas. It therefore prioritizes DoD's efforts, focusing on the requirement to fulfill DoD's lead responsibilities for homeland defense. As a second priority, we will ensure the Department's ability to support civil authorities in recovering from multiple, catastrophic mass casualty CBRNE incidents within the United States.

The Department of Defense will expeditiously implement the Strategy for Homeland Defense and Civil Support. Fundamentally, this will require the Department to integrate strategy, planning, and operational capabilities for homeland defense and civil support more fully into DoD processes. **The Strategy for Homeland Defense and Civil Support is not a static document.** Even as the Department of Defense implements this Strategy, it will continue to adapt to changes in the strategic environment, incorporate lessons learned from operational experience, and capitalize on emerging technology and operational concepts.



I. Context

"For most of the twentieth century, the world was divided by a great struggle over ideas: destructive totalitarian visions or freedom and equality. That great struggle is over. The militant visions of class, nation, and race which promised utopia have been defeated and discredited. America is now threatened less by conquering states than we are by failing ones. We are menaced less by fleets and armies than by catastrophic technologies in the hands of the embittered few. We must defeat these threats to our Nation, allies, and friends."

The National Security Strategy of the United States of America

September 2002

The Strategy for Homeland Defense and Civil Support embodies the core principles articulated in the US Constitution, the Nation's laws, and in Presidential and Secretary of Defense guidance. It also responds to the challenges posed by the security environment over the next decade.

Key Definitions

Homeland security, as defined in the National Strategy for 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 Department of Homeland Security is the lead federal agency for homeland security. In addition, its responsibilities extend beyond terrorism to preventing, preparing for, responding to, and recovering from a wide range of major domestic disasters and other emergencies.

Homeland defense is the protection of US sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression, or other threats as directed by the President. The

Department of Defense is responsible for homeland defense.¹

Defense support of civil authorities, often referred to as **civil support**, is DoD support, including Federal military forces, the Department's career civilian and contractor personnel, and DoD agency and component assets, for domestic emergencies and for designated law enforcement and other activities. The Department of Defense provides defense support of civil authorities when directed to do so by the President or Secretary of Defense.

Standing Guidance from National and Defense Strategies

The Strategy for Homeland Defense and Civil Support integrates the objectives and guidance expressed in the National Security Strategy, the National Strategy for Homeland

¹ Homeland Defense includes missions such as domestic air defense. The Department recognizes that threats planned or inspired by "external" actors may materialize internally. The reference to "external threats" does not limit where or how attacks could be planned and executed. The Department is prepared to conduct homeland defense missions whenever the President, exercising his constitutional authority as Commander in Chief, authorizes military actions.

I. Context

Security, and the National Defense Strategy to guide Department of Defense operations to protect the US homeland.

- The National Security Strategy (2002) expands the scope of US foreign and security policy to encompass forward-reaching preventive activities, including pre-emption, against hostile states and terrorist groups.
- The National Strategy for Homeland Security (2002) guides the national effort to secure the US homeland against terrorist attacks. It provides a framework for action at all levels of government that play a role in homeland security.
- The National Defense Strategy (2005) identifies as its top priority the dissuasion,

deterrence, and defeat of direct threats to the United States. The Strategy's implementation hinges on an active, layered defense that is designed to defeat the most dangerous challenges early and at a safe distance, before they are allowed to mature. It directs military leadership to properly shape, size, and globally posture to 1) defend the US homeland; 2) operate in and from the forward regions; 3) swiftly defeat adversaries in overlapping military campaigns while preserving the president's option to call for a decisive result in a single operation; and 4) conduct a limited number of lesser contingencies.

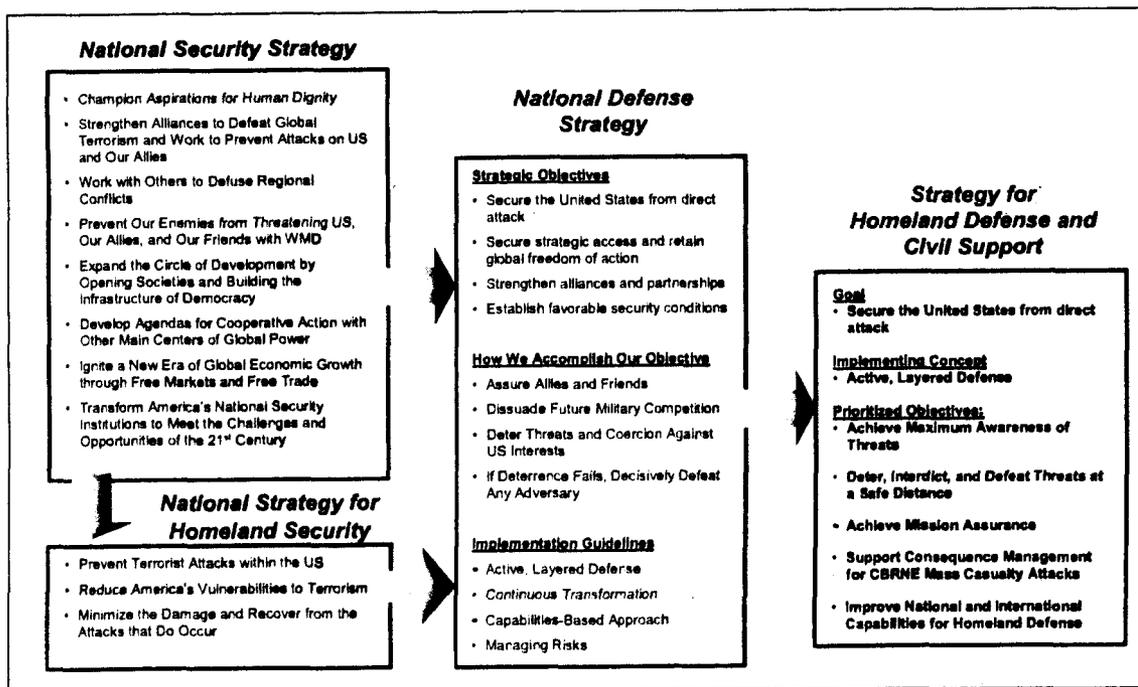


Figure 1: Strategic Underpinnings of the Homeland Defense and Civil Support Strategy

In addition to these overarching strategies, the Strategy for Homeland Defense and Civil Support is informed by, and complements, other key strategic and planning documents. These include standing National Security and

Homeland Security Presidential Directives, the National Military Strategy, the DoD Homeland Security Joint Operating Concept, and *Military Transformation: A Strategic*

Approach (Office of the Director for Force Transformation).

Security Environment

The defining characteristic of the security environment over the next ten years is the certainty of substantial diverse and asymmetric challenges to the United States, our allies, and interests. At the same time, we are faced with great *uncertainty* regarding the specific character, timing, and sources of potential attacks. The Strategy for Homeland Defense and Civil Support aims to mitigate that uncertainty, addressing the full range of challenges to the US homeland over the next decade.

Nation-state military threats to the United States will persist throughout the next decade. Rogue nations, for example, pose immediate and continuing challenges to the United States and our allies, friends, and interests. In addition, we must prepare for the potential emergence of regional peer competitors.

The United States will also face a range of asymmetric, transnational threats. Of greatest concern is the availability of weapons of mass destruction, heretofore the exclusive domain of nation-states, to terrorist groups. **In the next ten years, these terrorist groups, poised to attack the United States and actively seeking to inflict mass casualties or disrupt US military operations, represent the most immediate challenge to the nation's security.**

Transnational terrorist groups view the world as an integrated, global battlespace in which to exploit perceived US vulnerabilities, wherever they may be. This battlespace includes the US homeland. Terrorists seek to attack the United States and its centers of

gravity at home and abroad and will use asymmetric means to achieve their ends, such as simultaneous, mass casualty attacks. On September 11, 2001, terrorists demonstrated both the intent and capability to conduct complex, geographically dispersed attacks against the United States and our allies. It is foreseeable that adversaries will also develop or otherwise obtain chemical, biological, radiological, nuclear, or high-yield explosives (CBRNE) capabilities, with the intent of causing mass panic or catastrophic loss of life. Although America's allies and interests abroad will be the most likely targets of terrorism in the coming decade, we must also anticipate enemy attacks aimed at Americans at home.

Organizing for Homeland Defense and Civil Support

In light of the importance of homeland defense and DoD's contributions to homeland security, the Secretary of Defense, with the support of Congress, has improved the Department's organization and oversight structure for homeland defense and civil support.

- **The Assistant Secretary of Defense for Homeland Defense.** As stated in the 2003 National Defense Authorization Act, the Assistant Secretary of Defense for Homeland Defense provides overall supervision of DoD's homeland defense activities. The establishment of the Assistant Secretary of Defense for Homeland Defense responded to the need for improved policy guidance to DoD Components on homeland defense and civil support issues.
- **Chairman of the Joint Chiefs of Staff.** The Chairman of the Joint Chiefs of Staff

coordinates with and assists US Northern Command, US Pacific Command, the North American Aerospace Defense Command, and all other combatant commands with the strategic direction and planning for, as well as the execution of, homeland defense and civil support missions.

- **US Northern Command**, headquartered in Colorado Springs, Colorado. Established in 2002, US Northern Command (USNORTHCOM) is responsible for planning, organizing, and executing homeland defense and civil support missions within the continental United States, Alaska, and territorial waters. It also coordinates security cooperation with Canada and Mexico. In addition to the landmasses of the United States, Canada, and Mexico, US Northern Command's area of responsibility includes the coastal approaches, the Gulf of Mexico, Puerto Rico, and the US Virgin Islands.
- **US Pacific Command**, headquartered in Honolulu, Hawaii. US Pacific Command (USPACOM) has homeland defense and civil support responsibilities for Hawaii and US territories, possessions, and freely associated states in the Pacific.²

² The Pacific territories, possessions, and freely associated states that are included in the US homeland are: Guam, American Samoa, and Jarvis Island; the Commonwealth of Northern Mariana Islands; the Freely Associated States under the Compacts of Free Association, which include the Federated States of Micronesia, the Republic of the Marshall Islands, and the Republic of Palau; and the following US possessions: Wake Island, Midway Islands, Johnston Island, Baker Island, Howland Island, Palmyra Atoll, Jarvis Island, and Kingman Reef.

- **North American Aerospace Defense Command**, headquartered in Colorado Springs, Colorado. The bi-national North American Aerospace Defense Command (NORAD) is responsible for protecting the North American airspace over the United States and Canada. Aerospace warning and control are the cornerstones of the NORAD mission.

In addition to these organizations, all other regional and functional combatant commands, the Military Departments, and DoD elements contribute to the protection of the US homeland from attack.

- Other regional combatant commanders can promote international cooperation on homeland defense through exercises and military-to-military contact programs. Together with the functional combatant commanders, these regional commanders can also intercept and defeat adversaries intent on attacking US territory.

Of particular note, US Strategic Command provides significant support to USNORTHCOM, USPACOM, and NORAD. US Strategic Command is responsible for planning, integrating, and coordinating global missile defense operations and support for missile defense, including providing warning of missile attack, across all combatant commands. US Strategic Command is further charged with the global missions to undertake military space operations, to conduct information operations as well as computer network operations, and to integrate and synchronize DoD efforts in combating weapons of mass destruction.[52]

- The Military Departments organize, train, and equip US military forces across

operational domains. The Military Departments provide the bulk of the DoD capabilities likely to be requested for civil support.

- Other DoD Components contribute to homeland defense through intelligence collection, analysis, and prioritization; capability assessments; and oversight of relevant policy, acquisition, logistics, personnel, readiness, and financial matters.

The Strategy for Homeland Defense and Civil Support will guide all DoD Components across the full range of homeland defense and civil support activities.

Assumptions

This Strategy makes the following key assumptions:

- The United States will continue to face traditional military challenges emanating from hostile nation-states. Nation-state adversaries will incorporate asymmetric threats into their broader strategies of competition and confrontation with the United States.
- Terrorists will seek and likely gain surreptitious entry into the United States to conduct mass casualty attacks against Americans on US soil.
 - Terrorists will leverage vulnerabilities to create new methods of attack.
 - Terrorists and/or rogue states will attempt multiple, simultaneous mass casualty CBRNE attacks against the US homeland.
- Terrorists will try to shape and degrade American political will in order to diminish American resistance to terrorist ideologies and agendas.
- Allies and friends will cooperate with the United States in mutually beneficial security cooperation arrangements.
- US Northern Command, the North American Aerospace Defense Command, and US Pacific Command will continue to develop mature homeland defense capabilities in the air, land, and maritime domains, with appropriate support provided by other combatant commands.
- The Department of Homeland Security and other federal, state, local, and tribal authorities will continue to improve their prevention, preparedness, response, and recovery capabilities throughout the decade.
- The Department of Defense will promote the integration and sharing of applicable DoD capabilities, equipment, and technologies with federal, state, local, and tribal authorities and the private sector.
- In the event of major catastrophes, the President or the Secretary of Defense will direct DoD to provide substantial support to civil authorities. DoD's responses will be planned, practiced, and carefully integrated into the national response.
- The likelihood of US military operations overseas will be high throughout the next ten years.

II. Active, Layered Defense

"The war on terror will not be won on the defensive. We must take the battle to the enemy, disrupt his plans, and confront the worst threats before they emerge. In the world we have entered, the only path to safety is the path of action. And this nation will act."

President George W. Bush

June 1, 2002

As set forth in the National Defense Strategy (2004), the Department of Defense is transforming its approach to homeland defense just as it is transforming national defense capabilities overall. **Guiding homeland defense planning is the concept of an active, layered defense, predicated on seizing the initiative from adversaries.**

"Our most important contribution to the security of the US homeland is our capacity to disrupt and defeat threats early and at a safe distance, as far from the US and its partners as possible. Our ability to identify and defeat threats abroad—before they can strike—while making critical contributions to the direct defense of our territory and population is the sine qua non of our nation's security."

The National Defense Strategy

The case for an active, layered defense is clear. The United States has multiple points of vulnerability that adversaries seek to exploit. Significantly, these vulnerabilities exist in America's key centers of gravity. Commerce relies on the flow of goods and people across the nation's borders, through our seaports and airports, and on our streets and highways. The US free market economy requires trust in the uninterrupted electronic movement of financial data and funds through cyberspace. The symbols of American heritage—monuments and public buildings—

are a source of national pride and are open to all. Vast and potentially vulnerable natural resources provide power to our homes and food for our tables.

To safeguard the American way of life and to secure our freedom we cannot depend on passive or reactive defenses. A strictly defensive strategy is easily subject to enemy reconnaissance and inevitable defeat. By contrast, an active, layered defense relies on early warning of an emerging threat in order to quickly deploy and execute a decisive response. This active defense is a powerful deterrent, dissuading adversaries and denying them any benefit from attacking the US homeland and imposing costs on those who attempt it.

The United States must keep potential adversaries off balance by both an effective defense of US territory and, when necessary, by projecting power across the globe. **We must seize the initiative from adversaries and apply all aspects of national power to deter, intercept, and disrupt attacks against us and our allies and friends. In short, the United States must act in ways that an enemy cannot predict, circumvent, or overcome.** Multiple barriers to attack must be deployed across the globe—in the forward regions, the approaches to the United States, in the US homeland, and in the global commons—to create an unpredictable web of

II. Active, Layered Defense

land, maritime, and air assets that are arrayed to aggressively detect, deter, and defeat hostile action. When the United States identifies specific threats or vulnerabilities, it will enhance its deterrence posture through

force projection, flexible deterrent options, heightened alert status, and tailored strategic communications.

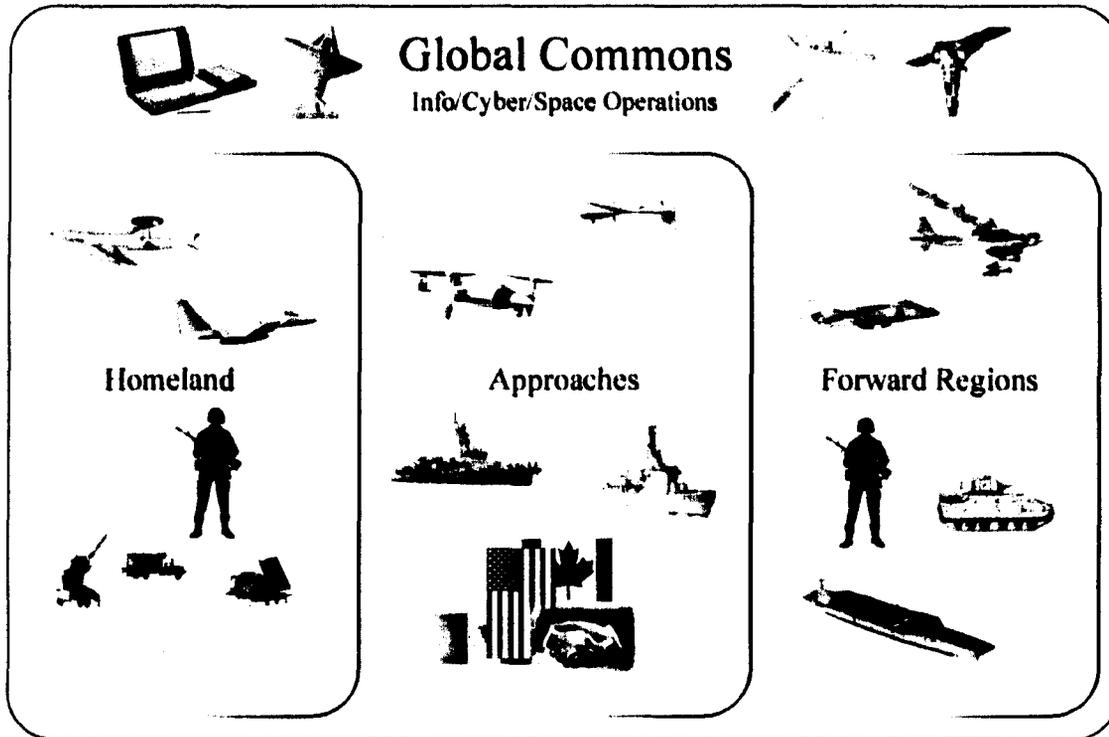


Figure 2: Active, Layered Defense Concept

The Forward Regions. The forward regions are foreign land areas, sovereign airspace, and sovereign waters outside the US homeland. The Department of Defense is a key contributor to the President's integrated national security effort abroad. To respond quickly to rising threats, the United States requires timely and actionable intelligence. Improved human intelligence (HUMINT) collection, improved intelligence integration and fusion, improved analysis of terrorist threats and targets, and improved technical collection against potential CBRNE weapons are all critical in this regard. In addition, the United States must counter and delegitimize the ideological support for

terrorist groups, disrupt their flow of funding, and create an environment that curtails recruitment. US military forces must be trained, ready, and postured to intercept potential enemies, eliminate enemy sanctuaries, and maintain regional stability, in conjunction with allies and friendly states.

The Approaches. The land approaches to the continental United States are within the sovereign territory of Canada and Mexico. These nations, in close cooperation with the United States, contribute to North American security through their law enforcement, defense, and counterterrorism capabilities.

The waters and airspace geographically contiguous to the United States are critical homeland defense battlespaces. In these approaches, US Northern Command, the North American Aerospace Defense Command, and US Pacific Command, working in concert with other combatant commands, the Intelligence Community, the US Coast Guard, and other domestic and international partners have the opportunity to detect, deter, and, if necessary, defeat threats en route—before they reach the United States.³ **This requires maximum awareness of threats in the approaches as well as the air and maritime interception capabilities necessary to maintain US freedom of action, secure the rights and obligations of the United States, and protect the nation at a safe distance.**

The US Homeland. The US homeland includes the United States, its territories and possessions, and the Commonwealths and Compact States of the Pacific. It also includes the surrounding territorial seas. Among its responsibilities within US territory, DoD focuses on the following areas:

- DoD is responsible for deterring and, when directed by the President, defeating direct attacks against the United States. NORAD is the cornerstone of our homeland air defense capability. Our air defense success rests on an integrated system for air surveillance and defense against air threats at

all altitudes. DoD also maintains land forces capable of responding rapidly, when so directed, to threats against DoD personnel, defense critical infrastructure, or other domestic targets. Finally, DoD supports the US Coast Guard in the exercise of its maritime authorities under domestic and international law.

- DoD supports civilian law enforcement and counterterrorism authorities consistent with US law. The Attorney General coordinates the activities of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States. DoD support to the Department of Justice and other domestic law enforcement authorities includes providing expertise, intelligence, equipment, and training facilities to these authorities when so directed. It can also include the use of US military forces to support civilian law enforcement in responding to civil disturbances, as provided in US law.
- DoD provides critical CBRNE consequence management capabilities in support of civil authorities. With few exceptions, DoD's consequence management capabilities are designed for the wartime protection of the Department's personnel and facilities. Nevertheless, civil authorities are likely to call upon these capabilities if a domestic CBRNE catastrophe occurs in the ten-year time frame of this strategy. **DoD must therefore equip and train these warfighting forces, as necessary, for domestic CBRNE consequence management. Beyond an already dedicated command and control element designed for this purpose,**

³ The US Coast Guard is inherently flexible, as both a military service and law enforcement agency within the Department of Homeland Security. The US Coast Guard supports DoD in its homeland defense role, while DoD supports the Coast Guard in its homeland security role, across the forward regions, the global commons, and approaches, and within the US homeland.

however, DoD will continue to rely on dual-capable forces for domestic consequence management missions.

The Global Commons. The global commons consist of international waters and airspace, space, and cyberspace. America's ability to deter threats against the global commons and to operate from them effectively is critical to the conduct of all its military missions, from the forward regions to the US homeland. Of particular note is the importance of space and cyberspace to US net-centric capabilities. **An active, layered defense requires a trustworthy information system, impervious to**

disabling digital or physical attacks.

Computer network defense must ensure that networks can self-diagnose problems and build immunity to future attacks. At the same time, networks must remain operational and consistently available for the execution of US military missions.

An active defense also requires the ability to detect and defeat threats from space.

This includes the need for capable defenses against ballistic missiles. Ground facilities that support US military space systems are potential targets of attacks, and the Department will protect them.



III. Strategic Goal and Key Objectives

"We must build and maintain our defenses beyond challenge. Our military's highest priority is to defend the United States . . . The threats and enemies we must confront have changed, and so must our forces."

The National Security Strategy of the United States of America

September 2002

The employment of an active, layered defense across the globe is fundamental to achieving the Department of Defense's strategic goal for homeland defense. That is, **we will secure the United States from direct attack.** The National Defense Strategy emphasizes the Department of Defense's role in the forward regions and the global commons and how that role is critical to the defense of US territory. **This Strategy for Homeland Defense and Civil Support therefore focuses particular attention on the US homeland and its approaches.** In these geographic layers, the Department's activities to protect the United States generally fall into one of the following categories:

- **Lead:** DoD leads military missions to deter, prevent, and defeat attacks on the United States, its population, and its defense critical infrastructure. This includes defending the maritime and air approaches to the United States and protecting US airspace, territorial seas, and territory from attacks. The Department is also responsible for protecting DoD personnel located in US territory.
- **Support:** At the direction of the President or the Secretary of Defense, the Department provides defense support of civil authorities in order to prevent terrorist incidents or manage the consequences of an attack or a disaster. Civil authorities are most likely to request DoD support

where we have unique capabilities to contribute or when civilian responders are overwhelmed. DoD's contributions to the comprehensive national response effort can be critical, particularly in the near-term, as the Department of Homeland Security and other agencies strengthen their preparedness and response capabilities.

- **Enable:** Efforts to share capabilities and expertise with domestic agencies and inter-national partners reinforce the Department's lead and support activities. At home, the Department works to improve civilian capabilities for homeland security by lending expertise and sharing relevant technology. For example, DoD is assisting the Department of Homeland Security in its efforts to develop intelligence analytical capabilities. We are also sharing training and simulation technologies, as well as unmanned aerial vehicle technologies for civilian surveillance along the Nation's borders. Abroad, the Department's security cooperation initiatives improve collective capabilities for homeland defense missions through exercises, information-sharing agreements, and formal defense agreements, such as NORAD.

To fulfill the key strategic goal of protecting the United States from attack, the Department of Defense will focus on achieving five key

III. Strategic Goal and Key Objectives

objectives directly related to the lead, support, and enable framework. In order of priority, these objectives are:

1. Achieve maximum awareness of potential threats (Lead);
2. Deter, intercept and defeat threats at a safe distance from the United States, and US territories and possessions (Lead);
3. Achieve mission assurance (Lead);
4. Ensure DoD's ability to support civil authorities in domestic CBRNE consequence management (Support); and
5. Improve domestic and international partner capabilities for homeland defense and homeland security (Enable).

ACTIVITIES	OBJECTIVES	CORE CAPABILITIES
LEAD	Achieve Maximum Awareness of Threats	<ul style="list-style-type: none"> • Maintain agile and capable defense intelligence architecture • Analyze and understand potential threats • Detect, identify, and track emerging threats in all operational domains • Ensure shared situational awareness within DoD and with domestic and foreign partners
	Deter, Intercept and Defeat Threats at a Safe Distance	<ul style="list-style-type: none"> • Deter adversaries from attacking the US homeland • Intercept and defeat national security threats in the maritime and air approaches and within US territory
	Achieve Mission Assurance	<ul style="list-style-type: none"> • Ensure force protection, to include DoD installations, especially against the threat of CBRNE attacks • Prepare and protect defense critical infrastructure • Ensure preparedness of the Defense Industrial Base • Prepare to protect designated national critical infrastructure • Ensure DoD crisis management and continuity preparedness
SUPPORT	Support Consequence Management for CBRNE Mass Casualty Attacks	<ul style="list-style-type: none"> • Manage consequences of CBRNE mass casualty attacks
ENABLE	Improve National and International Capabilities for Homeland Defense and Civil Support	<ul style="list-style-type: none"> • Effective interagency planning and interoperability • Capable federal, state, and local partners and effective domestic relationships • Capable international partners and effective defense-to-defense relationships

Figure 3: DoD Objectives and Core Capabilities for Protecting the United States from Attack

Lead

Objective 1: Achieve maximum awareness of threats

To defend the nation in the 21st century, the Department requires sufficient forewarning and immediate situational awareness of

potential attacks. No longer is it sufficient to track the movement of hostile military aircraft and warships. In the 21st century threat environment, transnational terrorists and rogue states may employ a wide range of civilian vessels and aircraft as weapons, engage in cyber attacks, or target civilian infrastructure to achieve devastating effects.

To protect the United States in this environment, the Department of Defense, in cooperation with domestic and international partners, will seek to achieve maximum awareness of threats. By so doing, the United States increases the time available for an effective operational response. **Threat awareness includes the ability to obtain comprehensive, accurate, timely, and actionable intelligence and information; exploiting relevant information; and making it available to the warfighters, policy makers, and interagency and international partners responsible for identifying and responding to threats.**

An active, layered defense requires information to flow freely regardless of operational boundaries. Relevant information may originate in one or several of the operational domains—land, maritime, air, cyberspace, or space. It may originate from an array of domestic and foreign sources. To achieve maximum awareness of threats, information will be posted to DoD's Global Information Grid, integrating operational domains and facilitating information sharing across traditional military-civilian boundaries. Using fused and shared threat awareness, our domestic and international partners and we can determine the most appropriate means to deter, intercept, or defeat threats and act accordingly.

Objective 2: Deter, intercept and defeat threats at a safe distance

During the Cold War, the United States focused on preventing Soviet submarines, ballistic missiles, and long-range bombers from attacking the American homeland. Although concerns about traditional

conventional and nuclear threats to the US homeland remain, we recognize that in the next ten years, adversaries will present a host of new challenges. They may attempt to use commercial vessels to transport terrorists or weapons to the United States. They may attempt to intrude on US airspace with low-altitude aircraft, cruise missiles, and unmanned aerial vehicles. They may attempt to convert maritime vessels, aircraft, and other modes of transportation into weapons. Through these and other means, our enemies will constantly employ asymmetric means to challenge the security of the United States.

In the maritime approaches, DoD is working with the Department of Homeland Security to integrate US maritime defense and to optimize the mutually supporting capabilities of the US Navy and the US Coast Guard. **As the Chief of Naval Operations (CNO) has stated, "forward deployed naval forces will network with other assets of the Navy and the Coast Guard, as well as the intelligence agencies to identify, track and intercept threats long before they threaten this nation."** This will require a level of situational awareness in the maritime domain similar to that in the air approaches. The goal, as the CNO explains, is to **"extend the security of the United States far seaward, taking advantage of the time and space purchased by forward deployed assets to protect the U.S. from impending threats."**

In the air domain, DoD has primary responsibility for defending US airspace and protecting the United States from ballistic missiles, cruise missiles, and other aerospace attacks. For North America, this defense is carried out in partnership with Canada, through NORAD. In addition, the

III. Strategic Goal and Key Objectives

Department of Defense relies heavily on the Federal Aviation Administration and the Department of Homeland Security (Transportation Security Administration) for early identification of air threats. As in the maritime environment, cooperation and operational coordination with our interagency partners, as well as our neighbors and other allies, is critical to protecting the United States from air threats.

Within US territory, we face the challenge of intercepting and defeating enemies determined to cause fear, death, and economic disruption. Although we must not dismiss traditional foreign military threats, in the period covered by this strategy, domestic employment of the US military in a homeland defense role will likely come in response to transnational terrorist, rogue state, or other threats that exceed the capabilities of domestic counterterrorism and law enforcement authorities.

Therefore, the Department must approach the interception and defeat of threats to US territory from a joint, interagency, and, ultimately, intergovernmental perspective. DoD must not conduct operations in separate and distinct land, maritime, and air operational domains. Over the coming decade, the Department will continue to develop joint concepts of operations, working with critical interagency and international partners as appropriate.

Objective 3: Achieve mission assurance

The Department cannot fulfill any of the Strategy's key objectives without having the core capabilities in place to assure mission success. **Mission assurance, the certainty that DoD components can perform**

assigned tasks or duties in accordance with the intended purpose or plan, is therefore itself a key objective. The Department of Defense achieves mission assurance through a range of programs and efforts that are aimed at securing DoD warfighting capabilities even when under attack or after disruption. These include force protection, the defense critical infrastructure program, and defense crisis management and continuity of operations efforts.

Force Protection. Force protection is central to achieving DoD mission assurance. It includes actions taken to prevent or mitigate hostile actions against DoD personnel (to include family members), resources, facilities, and critical information in an all hazards environment. Force protection measures can be defensive in nature, such as those used to reduce force and installation vulnerability to terrorist attacks or protect against CBRNE effects, or offensive, such as those taken to prevent, deter, and respond to terrorism. By conserving the force's fighting potential so that they can apply it at the decisive time and place, force protection ensures the effective employment of the joint force while degrading the enemy's opportunities.

An attack on DoD facilities could directly affect the Department's ability to project power overseas or carry out vital homeland defense functions. Installation commanders and facility managers have an inherent responsibility to protect the forces and installations under their command. Of particular concern is the threat to DoD personnel and installations posed by domestic CBRNE attacks.

III. Strategic Goal and Key Objectives

CBRNE Preparedness. The Department of Defense will develop and implement a comprehensive preparedness plan for CBRNE attacks. This plan will leverage capabilities and programs throughout the Department (e.g. Critical Infrastructure Protection, Antiterrorism/Force Protection, Project Guardian) including required intelligence support. In accordance with DoD responsibilities in the National Biodefense Policy, the Department is especially attentive to the unique challenges posed by biological agents.

Defense Critical Infrastructure. Related to its force protection responsibilities for DoD facilities, the Department of Defense has the responsibility to assure it has access to *defense critical infrastructure*. This is defined as DoD and non-DoD cyber and physical assets and associated infrastructure essential to project and support military forces worldwide. When these infrastructures are located on Department of Defense installations, their protection is the responsibility of the installation commander or facility manager. In some instances, however, critical defense assets are located at public or private sites beyond the direct control of DoD. In either case, the protection of designated defense critical infrastructure must be assured on a priority basis.

In some scenarios, assurance of non-DoD infrastructures might involve protection activities, in close coordination with other federal, state, local, tribal, or private sector partners. This could include elements of the Defense Industrial Base, which is a world-wide industrial complex with capabilities to perform research and development and design, produce, and maintain military weapons systems, subsystems, components, or parts to meet military requirements.

These defense-related products and services are essential to mobilize, deploy, and sustain military operations. Moreover, defense critical infrastructure could also include selected civil and commercial infrastructures that provide the power, communications, transportation, and other utilities that military forces and DoD support organizations rely on to meet their operational needs.

In addition, the President or the Secretary of Defense might direct US military forces to protect non-DoD assets of national significance. The President has designated fourteen categories of non-defense Critical Infrastructures and Key Assets. Although these facilities and assets may not be required for the support of DoD missions, they are so vital to the nation that their incapacitation, exploitation, or destruction could have a debilitating effect on the security and economic well being of the United States.

Defense Crisis Management and Continuity of Operations. During an emergency, the nation's leaders, including DoD decision-makers, must be able to carry out vital government functions. **The Department must provide the President and Secretary of Defense with survivable and enduring national command and control of DoD assets and US military forces.** DoD also plays an important supporting role in ensuring Continuity of Government and Enduring Constitutional Government in times of crisis. In the Cold War era, DoD continuity efforts focused on survival of senior leadership to prosecute war in the aftermath of a massive nuclear attack. Today, DoD's crisis management efforts are broader, responsive to the full range of potential threats to the nation.

III. Strategic Goal and Key Objectives

Meeting the Department's crisis management objectives requires ready DoD transportation assets, capable and survivable remote operation sites, and advanced communications capabilities throughout the DoD continuity architecture. DoD will continue to explore innovative concepts in communications and netcentric operations to improve national-level capabilities.

Support

Objective 4: Support consequence management for CBRNE mass-casualty attacks

The Department has traditionally supported civil authorities in a wide variety of domestic contingencies, usually natural disasters. DoD typically does so using military forces and DoD capabilities designed for use in expeditionary warfighting missions. That support continues today. For example, unique national intelligence capabilities that are located within the Defense intelligence community continuously support other US Government agencies. Although these traditional types of defense support of civil authorities are likely to continue, they are not likely to impede DoD's ability to execute other missions specified in the National Defense Strategy.

At the high end of the threat spectrum, however, the 21st century environment has fundamentally altered the terms under which Department of Defense assets and capabilities might be called upon for support. **The potential for multiple, simultaneous, CBRNE attacks on US territory is real.** It is therefore particularly imperative that the Department of Defense

be prepared to support civilian responders in responding to such mass casualty events.

Support to domestic authorities for consequence management is a core element of active, layered defense. The Department of Defense maintains considerable CBRNE recovery expertise and equipment. When directed by the President or the Secretary of Defense, DoD will employ these capabilities to assist the Secretary of Homeland Security, the principal federal official for domestic incident management, or other domestic authorities. DoD must be prepared to support its interagency partners in responding to a range of CBRNE incidents, including multiple, simultaneous mass casualty attacks within the United States.

Enable

Objective 5: Improve national and international capabilities for homeland defense and homeland security

Enabling better national capabilities for homeland security missions is an important complement to DoD's lead and support activities. The broad range of threats posed by terrorists and other transnational actors has expanded our traditional concept of national security. In the past, the Department of Defense could largely fulfill its responsibility for protecting the nation by integrating its activities with the Department of State and the Intelligence Community. Today, the expertise and corresponding responsibility for managing security challenges is much more widely shared among federal departments and agencies. State, local, and tribal authorities, the private sector, and our allies and friends

III. Strategic Goal and Key Objectives

abroad are also critical contributors to US national security.

In such an environment, DoD must unify its efforts with those of its key interagency partners and international friends and allies to ensure the nation's security. Sharing technology, capabilities, and expertise strengthens the nation's ability to respond to hostile threats and domestic emergencies. Likewise, cooperative homeland defense

education and training initiatives will foster a common understanding of shared threats and how best to address them. In turn, DoD can readily leverage the expertise of other federal, state, local, and tribal authorities and international partners to improve its own capabilities for counterterrorism, maritime interception, and other missions critical to an active, layered defense.



IV. Core Capabilities

"Some believe that, with the U.S. in the midst of a dangerous war on terrorism, now is not the time to transform our armed forces. I believe that quite the opposite is true. Now is precisely the time to make changes. The impetus and the urgency added by the events of September 11th powerfully make the case for action."

Secretary of Defense Donald Rumsfeld

January 31, 2002

The Department of Defense will provide the homeland defense and civil support capabilities necessary to support implementation of the National Security Strategy, the National Strategy for Homeland Security, and the National Defense Strategy. Over the next ten years, DoD will protect the United States from attack by focusing on the core capabilities necessary to achieve each of the key objectives detailed in Section III.

Capabilities for Achieving Maximum Awareness of Threats

Core Capability: Capable and agile defense intelligence architecture

Protecting the United States against the full-range of 21st century threats requires the US Intelligence Community to restore its human intelligence capabilities, reprioritize intelligence collection to address probable homeland defense threats, and continue to invest in intelligence, reconnaissance, and surveillance (ISR) sensor capabilities. In the Cold War, we knew both the nature of the threat to our country and the source of that threat. Today, intelligence and warning must extend beyond conventional military and strategic nuclear threats to cover a wide range of other state

and non-state challenges that may manifest themselves overseas or at home.

The Intelligence Community is adjusting to this changing strategic landscape to meet the nation's homeland security needs. The establishment of a National Intelligence Director, the National Counter-Terrorism Center (NCTC), the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate, and the DoD's Joint Intelligence Task Force for Combating Terrorism (JITF-CT) exemplify this shift. Executive Orders for strengthened management of the Intelligence Community also ensure a more collaborative, comprehensive approach to intelligence support for national security. While these changes are taking place, the Department of Defense is reorienting its intelligence capabilities in line with the full range of homeland defense priorities. Specifically, the Department will:

- Focus on integrated collection management of foreign and military information and its application to homeland defense and homeland security;
- Better utilize national intelligence assets and capabilities to increase early warning and support prevention, interception, and disruption of potential threats overseas or in the approaches to the United States;

IV. Core Capabilities

- Collect homeland defense threat information from relevant private and public sector sources, consistent with US constitutional authorities and privacy law;
- Identify capability needs for CBRNE sensors to meet homeland defense requirements; and
- Develop automated tools to improve data fusion, analysis, and management, in order to systematically track large amounts of data, and to detect, fuse, and analyze aberrant patterns of activity, consistent with US privacy protections.

Core Capability: Collect, analyze, and understand potential threats

Improving our understanding of America's foreign enemies—in advance of an attack—is at the heart of DoD's efforts to achieve maximum awareness of potential threats. In accordance with the National Strategy for Combating Terrorism (2002), we are strengthening DoD's knowledge of foreign terrorist networks and the inner workings of their operations.

Improved human intelligence, particularly in the forward regions of the world, is the single most important factor in understanding terrorist organizations. The Department of Defense is currently undertaking a focused review of DoD human intelligence capabilities, including reforms to improve HUMINT career development, policies, practices, and organizations. It is critical that DoD HUMINT operators have relevant linguistic skills and cultural understanding as well as the technical skills needed to provide high quality, insightful information to the analysts within the Intelligence Community.

In addition, we will **develop a cadre of specialized terrorism intelligence analysts within the Defense intelligence community** and deploy a number of these analysts to interagency centers for homeland defense and counterterrorism analysis and operations. The Department will continue to maintain significant counterterrorism collection and analytical capability to support military activities overseas and in the approaches to the United States.

National agencies within the Department, such as the National Security Agency and the National Geospatial-Intelligence Agency, will continue to provide their unique capabilities in support of the national homeland security mission in accordance with applicable laws and regulations. The Department will also maintain an analytical capability to identify threats to defense critical infrastructure.

Core Capability: Detection, identification, and tracking of emerging threats in all operational domains

We face challenges in our ability to detect, identify, and track objects in all operational environments. Every day, thousands of US and foreign vessels and aircraft approach and depart North American ports and airports, and many times that number of individuals and vehicles cross our borders. For the Department of Defense, these challenges are especially pertinent in the air and maritime domains, where the military plays a much more substantial role.

To detect and track anticipated air and maritime threats effectively, the United States must have capabilities to cue, surveil, identify, engage, and assess potential threats in real time. Detection and tracking capabilities must be all-weather, around-the-

clock, and effective against moving targets. The United States must also have the ability to detect CBRNE threats emanating from any operating environment. **This requires a comprehensive, all-domain CBRNE detection architecture, from collection to dissemination.**

The maritime picture is multi-jurisdictional, with various US agencies responsible for tracking vessels from their departure at foreign ports to their arrival in the United States. Recognizing the potential vulnerability this situation creates, DoD is working closely with interagency partners, especially the Department of Homeland Security, to finalize a unified concept for maritime domain awareness (MDA)—the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States.

Based on the emerging MDA concept and related plans that will result from the implementation of National Security Presidential Directive-41/Homeland Security Presidential Directive-13: National Maritime Security, the Department of Defense will work with interagency partners to develop a comprehensive capability to detect threats as far forward of the US homeland as possible, ideally before threat vessels depart foreign ports. **DoD will ensure persistent wide-area surveillance and reconnaissance of the US maritime approaches, layered and periodically varied in such a manner that an adversary cannot predict or evade observation.** The nation will benefit from the Department of Homeland Security's work to institute worldwide cargo and crew reliability mechanisms. DoD, in concert with the Department of Homeland Security, will receive and share data from improved

identification systems for small commercial and other vessels, just as it has done for maritime vessels of over 300 gross tons that are on international voyages.

Achieving threat awareness in the air operational domain presents similar challenges. Throughout the Cold War, the Department of Defense focused on maintaining awareness of external threats that entered US airspace from overseas. The attacks on September 11, 2001, however, originated in US airspace and highlighted weaknesses in domestic radar coverage and interagency air defense coordination. Adversaries might maintain low altitude flight profiles, employ stealth and other defense countermeasures, or engage in deception to challenge US air defenses.

Since the attacks of September 11, 2001, DoD has coordinated with interagency partners to significantly improve the air defense of the United States. DoD has worked with the Federal Aviation Administration (FAA) to integrate domestic radar coverage and has conducted Operation Noble Eagle air patrols to protect designated US cities and critical assets. We have placed particular emphasis on implementing a robust air defense capability for the National Capital Region, using both air and ground air defense forces. DoD has also worked closely with interagency partners to exchange a wide range of information regarding potential threats.

The Department of Defense will continue to work with domestic and international partners to develop a persistent, wide-area surveillance and reconnaissance capability for the airspace within US borders, as well as over the nation's approaches. This capability could require the development of

advanced technology sensors to detect and track low altitude air vehicles across a wide geographic area. DoD is investigating various technologies that could provide an over-the-horizon engagement capability to detect enemy threats in the approaches or over US territory, leading to their defeat. The United States and our allies must also integrate sensor and intelligence data to identify hostile air vehicles by observing their performance characteristics, suspicious activities, or other attributes. These capabilities in the air domain will provide timely threat detection, extending the depth of air defenses and the time for response, thereby providing multiple engagement opportunities to defeat identified threats.

Core Capability: Shared situational awareness within DoD and with domestic and foreign partners

Shared situational awareness is defined as a common perception of the environment and its implications. All domestic and foreign partners within the homeland defense mission space require situational awareness for three reasons: to identify threats as early and as distant from US borders as possible; to provide ample time for an optimal course of action; and to allow for a flexible operational response. From the March 2003 Homeland Security Information Sharing Memorandum of Agreement, to the aggressive and unprecedented information sharing underway at the NCTC, the US Government continues to make great strides in overcoming obstacles to shared situational awareness.

During the Cold War, the Department of Defense sought shared situational awareness with the Department of State, the Intelligence Community, and allied nations in order to deter and defeat threats posed by the Soviet

Union and other nations. At the same time, the American law enforcement community worked with its international counterparts to thwart international drug cartels and a growing number of worldwide crime syndicates.

Today, transnational terrorists have blurred the traditional distinction between national security and international law enforcement. Together with a significant proliferation in the number and type of potential foreign threats, **this expanded national security challenge necessitates an unprecedented degree of shared situational awareness among federal agencies, with state, local, tribal, and private entities, and between the United States and its key foreign partners.**

As a first step, the Department of Defense must provide seamless connectivity and timely, accurate, and trusted information to all DoD Components—any time, any place—in order to achieve maximum awareness of potential attacks against the United States. The Department will therefore ensure that DoD's information infrastructure provides an integrated, interoperable worldwide network of information technology products and management services. This will allow users across DoD to process information and move it to warfighters, policymakers, and support personnel on demand. Network connectivity must be flexible enough to support global operations while allowing for local requirements and innovation. **It must also create a real-time link among sensors, decision makers, and warfighters to facilitate the rapid engagement of enemy targets.**

Beyond building an integrated information infrastructure, DoD must also populate that network with accurate, timely, and actionable data. Today, information relevant to

protecting the United States is widely dispersed. The Department, in concert with the intelligence and law enforcement communities and foreign partners, will build on the great strides already made to diminish existing cultural, technological, and bureaucratic obstacles to information sharing. The Intelligence Community and Department of Defense will drive improved information sharing within a “need to share” context. The resulting information exchange, commonly referred to as “horizontal integration of intelligence,” will provide analysts across the US Government and partner nations with timely and accurate all-source information, vastly improving the creation of a coherent and fully integrated threat picture. Such an expansion in information sharing requires appropriate safeguards to ensure that DoD intelligence components rigorously apply laws that protect Americans’ civil liberties and privacy.

Capabilities for Deterring, Intercepting and Defeating Threats at a Safe Distance

Core Capability: Deter adversaries from attacking the US homeland.

DoD’s efforts to secure the United States from direct attack are intrinsically linked to the concept of deterrence. The objective of deterrence is to convince potential adversaries that threatening courses of action will result in outcomes decisively worse than they could achieve through other, non-threatening, means.

Just as the range of potential adversaries to the United States varies, so, too, do the most effective means of deterrence. As a general rule, however, our deterrent is enabled by

global situational awareness, effective command and control, military presence abroad, the strength and agility of US military forces, strong domestic and international cooperation and sustained global influence, and a coherent national strategic communications campaign. Information operations, influence operations, control of the operational domains—land, sea, aerospace, and cyberspace, conventional and nuclear global strike capabilities, and active and passive defense measures all contribute significantly to deterring threats to the US homeland.

Core Capability: Interception and defeat of national security threats in the maritime and air approaches and within US territory

Maritime Operational Domain. The United States must be prepared for the foreseeable threat of transnational terrorists, detected on the high seas and armed with weapons of mass destruction. Accordingly, we will fully integrate our surface, subsurface, air, and surveillance assets, focus them forward, and identify, track and intercept threats at a safe distance from the US coast. In so doing, we will work with our domestic and international partners and take action consistent with applicable law.

Enhancing our ability to intercept enemies in the maritime domain requires a seamless system of overlapping defenses—both adaptable and flexible—to frustrate enemy observation and avoid predictability. This begins in the forward regions with improved surveillance capability, increased HUMINT collection, and enhanced international partnerships through programs like the Container Security Initiative and Proliferation Security Initiative. To maximize maritime domain awareness, successive layers of

IV. Core Capabilities

surveillance must be fully coordinated with the operational activity of our forward deployed forces.

DoD has established standing orders for conducting maritime homeland defense and maritime interception operations. Given this guidance, geographic combatant commanders will include interception exercises in their theater security cooperation plans and conduct such exercises on a periodic basis. The US Navy and US Coast Guard will conduct routine and frequent maritime interception exercises to ensure a high state of training and readiness.

To intercept and defeat transnational threats, the Department of Defense and Department of Homeland Security must have a predetermined process for ensuring rapid, effective US Coast Guard support to the US Navy and vice versa. Although DoD has the lead role in defending the United States from direct maritime attack, we recognize the US Coast Guard's responsibilities for maritime law enforcement and homeland security. We will continue to support the US Coast Guard in fulfilling its homeland security responsibilities. Together with the US Coast Guard, we must build upon the security in our ports and littorals, expanding maritime defense capabilities further seaward in support of national security.

The United States must have a concept of operations for the active, layered maritime defense of the US homeland. Such a concept will require naval forces be responsive to US Northern Command, consistent with maritime mission requirements, and will require that Navy forces be placed under periodic command and control of US Northern Command as appropriate. DoD will also consider the use of US Naval

Reserve forces to undertake unique roles in maritime homeland defense. In addition, the US Navy should assess the integrated benefit of forces currently available in support of Operation Noble Eagle, available coastal patrol craft, and the utility of future Naval and Joint capabilities, such as the Navy's littoral combat ship, to execute the maritime homeland defense missions.

Air Operational Domain. The Department of Defense will defeat air threats to the United States, such as ballistic and cruise missiles and attacking military aircraft. DoD must also be prepared to intercept non-traditional air threats, even when the intent to harm the United States is more uncertain, as initially occurred on September 11, 2001. These threats could include commercial or chartered aircraft, general aviation, ultralight airplanes, unmanned aerial vehicles, radio controlled aircraft, or even balloons. Early detection and successful interception of these types of potential threats requires very close cooperation with DoD's interagency partners.

Since September 11, 2001, the Department of Defense, through Operation Noble Eagle, has conducted air patrols to protect major US population centers, critical infrastructure, and other sites. Working with our interagency partners, DoD will continue these patrols to intercept air threats to the US homeland as long as required by the projected threat.

The Department of Defense will continue to improve the air-to-air and ground-to-air capabilities and associated forces necessary to intercept and defeat all domestic air threats. For air patrol missions, DoD will use more capable aircraft as they are fielded and explore the potential for employing unmanned combat air vehicles. DoD is also

IV. Core Capabilities

upgrading ground-based air defense assets with improved detection and targeting capabilities.

The Department of Defense will devote significant attention to defending US territory against cruise missile attacks.

Defense against cruise missiles poses unique challenges, given that their low altitude and small size make them more difficult to identify and track than traditional air threats. The Department of Defense is developing integrated capabilities to defend against cruise missiles, as well as other types of unmanned aerial vehicles. As an interim step, DoD is developing a deployable air and cruise missile defense capability to protect designated areas. This capability aims to integrate Service tactical air defense assets, the NORAD air defense system, interagency information sources, and advanced technology sensors. **Future air and cruise missile defense assets will be fully interoperable, increase the size of the defended area, and engage threats at increased range.**

DoD will also continue to work with interagency partners to develop a common air surveillance picture that will enhance our ability to identify and, ultimately, defeat enemy targets. An improved capability is required to detect and track potential air threats within the United States. The current radars maintained by the Federal Aviation Administration to track air traffic within the United States are aging, with high maintenance costs, poor reliability, and reduced capability to track emerging threats. **The nation will need to develop an advanced capability to replace the current generation of radars in order to improve tracking and identification of low-altitude threats.**

Land Operational Domain. The Department of Defense will be prepared to deter and defeat direct, land-based attacks against the United States. We must work closely and cooperatively with our neighbors, establish seamless relationships and organizational structures with interagency partners, and be prepared to respond with military forces on our own soil quickly, responsively, and in a manner that is well coordinated with civilian law enforcement agencies.

Historically, the United States relied almost exclusively on forward deployed forces to confront and defeat nation-state adversaries overseas. Although military power projection remains crucial, transnational terrorism has significantly reduced the effectiveness of this singular approach. Now and in the future, we must be prepared in every part of the globe—most especially the US homeland—to deter, prevent, and defeat terrorist or other asymmetric threats.

The majority of infrastructure in the United States is privately owned. Consequently, private owners provide the first line of defense for most of the nation's assets. Should that defense prove insufficient, or public welfare is threatened, local, state, and, if necessary, federal authorities will assist in intercepting and defeating threats on US territory. By law and national policy, DoD's role on US soil is relatively circumscribed. The following three-tiered approach provides the parameters under which the military would likely operate:

Tier 1: Local and Federal law enforcement. When directed by the President or the Secretary of Defense, DoD will provide appropriate defense assets in support of domestic law enforcement authority, normally in support of a lead federal agency such as

the FBI. Under these circumstances, military forces and assets will remain under the command and control of a DoD authority.

Tier 2: National Guard forces not on Federal Active Duty. When directed by the Governor or appropriate state authority, National Guard forces and assets in state active duty status can respond quickly to perform homeland defense and homeland security activities within US territory.

Newly expanded authorities under Title 32 of US Code—and the National Guard’s on-going transformation into a truly 21st century force—provide Governors and state authorities with the authority to use flexible, responsive, multi-capable National Guard units for a limited period to perform homeland defense activities, when approved by the Secretary of Defense. For example, National Guard forces—scalable in terms of size and mix of skills—may, when the Secretary of Defense determines that doing so is both necessary and appropriate, provide security for critical infrastructure, support civilian law enforcement agencies in responding to terrorist acts, and offer their neighbors immediate assurance of safety and security.

Tier 3: US military forces responding to Presidential direction. If circumstances warrant, the President or the Secretary of Defense may direct military forces and assets to intercept and defeat threats on US territory. **When conducting land defense missions on US territory, DoD does so as a core, warfighting mission, fulfilling the Commander in Chief’s Constitutional obligation to defend the nation.** To fulfill this responsibility, DoD

will ensure the availability of appropriately sized, trained, equipped, and ready forces. Currently, this capability is provided by quick reaction forces (QRFs) and rapid reaction forces (RRFs).

Capabilities for Achieving Mission Assurance

Core Capability: Ensure Force Protection

As previously noted, force protection is that set of measures taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. The Department of Defense has institutionalized force protection across the Services as part of their core capabilities. The Department will ensure that force protection efforts fully incorporate considerations of risk management and mitigation to lessen the potentially adverse effects of incidents, whether man-made or natural, on key infrastructure within DoD installations and facilities.

CBRNE Preparedness. Although force protection is an all-hazards concept, the Department is particularly concerned about the threat that adversary use of CBRNE poses to DoD personnel and installations. Improving DoD’s capabilities for mitigating and, if necessary, operating in a CBRNE-contaminated environment will require progress in detecting and identifying threats (sense), providing early warning (shape), protecting forces and installations (shield), and ensuring the ability to operate in a contaminated environment (sustain). DoD’s Joint Chemical and Biological Defense Program is focused on developing and fielding technologies to mitigate, and if

IV. Core Capabilities

necessary, allow forces to operate in CBRNE contaminated environments.

Sense. DoD currently has a range of capabilities to detect, identify, and quantify airborne, waterborne, and other hazards. Needed improvements include advanced standoff and point detection capabilities for chemical and biological threats. DoD is also working to develop and field standoff detection capabilities for explosives. Advances in standoff detection capability will enhance the Department's ability to detect nuclear devices as well as weapons using explosives to disperse chemical, biological, and radioactive materials. Finally, the Department is improving medical surveillance capabilities both on installations and within surrounding communities to provide early detection and identification of CBRNE events in the workforce.

Shape. DoD characterizes CBRNE attacks by assimilating information drawn from sensors, hazard prediction models, and elsewhere to inform commanders of impending or approaching threats. The Department is continuing to improve on early CBRNE threat characterization by developing an integrated concept of operations for sensing, reporting, and warning of CBRNE attacks, ensuring compatibility with national-level CBRNE sensor architectures currently in operation, such as the Department of Homeland Security's BIOWATCH program, and those under development.

Shield. The Department will continue to provide force protection in advance of a potential CBRNE attack, whether overseas or at domestic installations. Already, more than 850,000 US military personnel have

been vaccinated against anthrax; more than 730,000 are vaccinated against smallpox. The Department is now focusing on the development of vaccines and other capabilities that can address new and emerging biological and chemical threats. This includes significant research on technologies for improved chemical and biological agent detection and personal and collective protection equipment. DoD is also preparing to field capabilities that protect US forces from chemical agents that can be absorbed through the skin.

Lastly, the Department is deepening and expanding collaboration on biodefense research with the Department of Homeland Security and the Department of Health and Human Services. This includes significant new investments by these civilian agencies and the creation of a new research consortium. The construction of a National Interagency Biodefense Campus, collocated with the US Army Medical Research Institute of Infectious Diseases (USAMRIID), will significantly facilitate civil-military cooperation in this area. A revitalized and recapitalized USAMRIID, along with major Department of Homeland Security and Department of Health and Human Services investments, will provide DoD and the nation with added research capacity, additional biopharmaceutical development, increased testing and evaluation of potential biodefense medical products, and large surge lab capacity for bioterrorism incident response.

Sustain. DoD must be able to sustain operations during and after a CBRNE attack in the United States. Medical therapeutics that allow DoD personnel to

continue mission-essential tasks in a CBRNE environment are of highest priority. DoD will also expand pilot programs for CBRNE installation preparedness to protect DoD personnel and facilities in the event of an attack. In addition to providing enhanced CBRNE defense capabilities at 200 critical installations in the United States and abroad through the Guardian Program, DoD will improve its capability to protect all installations through updated doctrine and guidance. The Department will examine an aggressive expansion of force protection and related programs to increase both the level of protection and the number of DoD installations it covers.

Core Capability: Preparedness and protection of defense critical infrastructure

Because resources are constrained, uniform protection of all defense critical infrastructure is not possible. **The Department must prioritize the protection of assets based on their criticality to executing the National Defense Strategy and seek to minimize the vulnerability of critical assets in accordance with integrated risk management approach.** To this end the Department will devise a strategy to:

- Identify infrastructure critical to the accomplishment of DoD missions, based on a warfighter mission area analysis.
- Assess the potential effect of a loss or degradation of critical infrastructure on DoD operations to determine specific vulnerabilities, especially from terrorist attack.
- Manage the risk of loss, degradation, or disruption of critical assets through

remediation or mitigation efforts, such as changes in tactics, techniques, and procedures; minimizing single points of service; and creating appropriate redundancies, where feasible.

- Protect infrastructure at the direction of the President or the Secretary of Defense where the nature of the threat exceeds the capabilities of an asset owner and civilian law enforcement are insufficient.
- Enable real-time incident management operations by integrating current threat data and relevant critical infrastructure requirements.

The Military Departments, Defense Agencies, and other DoD components are now implementing the Protective Risk Management Strategy through modifications to their programs and budgets.

Core Capability: Preparedness of the Defense Industrial Base

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (2003) notes that, **without the important contributions of the private sector, DoD cannot effectively execute core defense missions.** Private industry manufactures and provides the majority of the equipment, materials, services, and weapons for the US armed forces. Ensuring that military forces are properly equipped is critical to maintaining DoD power projection and homeland defense capabilities. In that regard, the President recently designated DoD as the Sector-Specific Agency for the Defense Industrial Base (DIB). **In this role, DoD is responsible for national infrastructure protection activities for critical defense industries as set forth in Homeland Security Presidential Directive-7.**

IV. Core Capabilities

To assure that mission critical supplies and services are available, DoD contracts are being modified to ensure that appropriate protective measures are in place at key facilities and appropriate information is shared with the DoD to assess the security of the DIB. In addition, the Defense Logistics Agency and other DoD contracting activities are revising the contract process to ensure that civilian defense contractors are able to operate for the duration of a national emergency. **Defense contractors must be able to maintain adequate response times, ensure supply and labor availability, and provide direct logistic support in times of crisis.** DoD program managers will be held accountable, where necessary, for ensuring the protection of supporting infrastructure, including key suppliers. DoD base and installation commanders, and those who contract for non-DoD infrastructure services and assets, will monitor assurance activities through compliance with contract language that clearly identifies reliable service availability, priority of restoration, and asset protection.

Core Capability: Preparedness to protect designated national critical infrastructure

The Department has historically focused on preventing unauthorized personnel from gaining access to DoD installations and protecting those installations from traditional military attacks. **In the post-September 11, 2001 era, DoD is expanding the traditional concept of critical asset protection to include protection from acts of transnational terrorism.** Countering terrorist reconnaissance activity is central to the successful defense of critical infrastructure.

As outlined in the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2003), DoD bears responsibility for protecting its own assets, infrastructure, and personnel. At the Department's request, domestic law enforcement may assist with protection functions at DoD facilities.

For non-DoD infrastructure, including private and public assets that are critical to the execution of the defense strategy, DoD's protection role is more limited. The initial responsibility for protection of non-DoD infrastructure rests with asset owners. Civilian law enforcement authorities augment and reinforce the efforts of asset owners, creating a second tier of protection.

Should protection requirements exceed the capabilities of asset owners and civilian law enforcement, state authorities provide an additional layer of defense. In addition to a Governor's authority to employ National Guard forces in a state active duty status, recent changes to Title 32 of the US Code may provide an additional, expeditious means to use National Guard forces under the control of the Governor, with the approval of the Secretary of Defense, using federal funding perform homeland defense activities.

To achieve critical infrastructure protection in the most serious situations, the Department of Defense maintains trained and ready combat forces for homeland defense missions.

Core Capability: Defense crisis management and DoD continuity preparedness

The Department's crisis management and continuity of operations programs are central to mission assurance. DoD must provide capabilities necessary to support senior

leadership decision-making and military command and control and to perform essential DoD functions to support national-level crisis managers. DoD is working to enhance its information management and communications capabilities to support senior leadership in crises. It is also improving the survivability and flexibility of military command and control capabilities.

A significant element of mission assurance is **continuity of operations**—maintaining the ability to carry out DoD mission essential functions in the event of a national emergency or terrorist attack. Fulfilling this objective in the current security environment necessitates new and innovative approaches. Some of these approaches include policies for personnel dispersion, leveraging advances in information technology to improve crisis coordination, and improving relocation facilities. The Department recently conducted a zero-based assessment of DoD continuity capabilities. The results of this assessment detail numerous capability improvements that the Department can pursue in order to ensure the continuity of DoD operations in times of crisis. It also provides recommendations that will transform DoD's approach to continuity operations from a Cold War-oriented operational concept to one better suited to address the current and evolving terrorist threat. The recommendations include the use of new and emerging technologies and the development of more flexible relocation options.

Capabilities for CBRNE Consequence Management

Core Capability: Consequence management assistance for domestic CBRNE mass casualty attacks

Acknowledging the challenges presented by the current security environment, the Department of Defense must be able to conduct most major combat operations in a CBRNE environment. US military forces organize, train, and equip to operate in contaminated environments, as well as manage the consequences of CBRNE incidents, on a level unmatched by any other single domestic agency or international partner. **If directed by the President or the Secretary of Defense, the Department of Defense must be prepared to use these capabilities to assist interagency partners in the aftermath of domestic CBRNE mass casualty attacks.** DoD's CBRNE capabilities include specialized agent detection, identification, and dispersion modeling systems as well as casualty extraction and mass decontamination abilities. DoD can also provide significant support to domestic consequence management by providing emergency medical support, such as equipment, mobile hospitals, aeromedical evacuation, medical personnel, engineering support, and mortuary services.

Not all domestic CBRNE incidents will necessitate a federal response; many scenarios may be well within the capabilities of state and local responders. Those incidents that do require a US Government response will be coordinated by a lead federal agency. In most catastrophic scenarios, DoD may be called upon to provide support to the Department of

IV. Core Capabilities

Homeland Security or another federal agency. **The Department will work closely with interagency partners—through the National Response Plan and the National Incident Management System—to ensure proficiency and interoperability in responding to multiple CBRNE incidents.**

The Department will ensure that dedicated CBRNE civil support capabilities are sized, trained, equipped, and ready for the domestic consequence management mission. Dedicated domestic CBRNE command and control is provided by the Joint Task Force-Civil Support. In addition, the National Guard WMD Civil Support Teams can operate under federal control in times of crisis, when directed to do so by the President or Secretary of Defense. DoD is currently examining the augmentation of WMD Civil Support Teams with National Guard and other military capabilities and forces that are task-organized for this mission.

DoD will also identify, train, and equip an additional, discrete number of military forces for the potential requirements associated with multiple, simultaneous CBRNE attacks within the United States. These forces will be dual-mission in nature—these warfighters and support elements will not be dedicated to the civil support role but they will nevertheless

be ready to perform domestic consequence management missions when required.⁴

Lastly, the Department will ensure that other elements of the Total Force—currently sized and shaped primarily for overseas missions—are identified, exercised, and ready to support CBRNE consequence management as necessary. This capability will provide added utility for overseas deployments or domestic missions. Within this Total Force context, DoD's effectiveness in responding to domestic CBRNE contingencies will be greatly improved through adjustments to Active and Reserve Component training, procedures that allow for faster mobilization of National Guard and Reserve Forces, and improved command relationships that make optimal use of the Reserve Component. This includes leveraging the National Guard's proposed Joint Force Headquarters-State organizations.

⁴ Among existing dual-use DoD assets are the US Marine Corps Chemical-Biological Incident Response Force (CBIRF); the US Army Technical Escort Unit; the US Army Chemical Biological Rapid Response Team; the Defense Threat Reduction Agency's Consequence Management Advisory Team; the US Army 52nd Ordnance Group; the US Navy Environmental and Preventive Medicine Unit; the US Naval Medical Research Center; the US Navy Defense Technical Response Group; the US Air Force Radiation Assessment Team; and the US Air Force Technical Application Center.

Enhancing US and International Capabilities for Homeland Defense and Homeland Security

Core Capability: Interagency planning and interoperability

Recognizing the critical importance of interoperability, DoD will share training, planning, and other appropriate resources with interagency partners to standardize operational concepts, develop technology requirements, and coordinate budget planning for homeland missions. Interagency efforts must focus on closing any remaining seams in air, land, maritime, cyberspace and space operational domains and must enhance national preparedness and incident management efforts. Development of a coordinated training and exercise program is an essential step toward enhanced cooperation in executing homeland defense and civil support missions.

Active DoD participation in the interagency process improves planning and interoperability and will ensure that procedures for supporting civil authorities are consistent with the framework for domestic incident response outlined in the National Response Plan and the National Incident Management System. DoD will work closely with interagency partners to identify how best to coordinate interagency civil support activities.

Core Capability: Capable federal, state, and local partners and effective domestic relationships

The Department of Defense has identified three tenets to enhance defense support of civil authorities:

- Augment civil capabilities with DoD expertise where necessary;
- Ensure the seamless operational integration of defense support capabilities with those of the civil sector;
- Assist in the civil sector's development, procurement, and sourcing of new technologies and equipment.

Within this civil support framework, the Department will actively seek to identify opportunities for cooperation with the civil sector. Several initiatives to enhance civilian capabilities are already underway. Examples include:

- DoD assistance to the Department of Homeland Security to develop CBRNE victim rescue capabilities, similar to those of the US Marine Corps' Chemical Biological Incident Response Force.
- Joint DoD and Department of Homeland Security research and development on, and civilian acquisition of unmanned aerial vehicles for law enforcement and ground surveillance systems for border security.
- DoD efforts through the Interagency Counter Man-Portable Air Defense System (MANPADS) Task Force to help develop an attack prevention and recovery plan, provide technical advice and analysis to the Department of Homeland Security regarding MANPAD countermeasures, and operational

assistance to stem the proliferation of MANPADS overseas.

In compliance with Section 1401 of the National Defense Authorization Act for FY 2003, DoD will continue to engage in efforts to transfer competencies between DoD and the civil sector—through technology transfer as well as sharing DoD's "lessons learned" from applicable exercises and program management. **Such collaborative efforts can increase the overall effectiveness of national capabilities and potentially reduce other agencies' dependencies on limited DoD assets.**

To succeed, the Department will need a systematic approach to ensure close coordination with the Department of Homeland Security and other interagency, state, and local partners, specifically:

- Facilitating the Department of Homeland Security's efforts to identify and provide appropriate and applicable defense technologies to state and local first responders;
- Nurturing new collaborative research, development, experimentation, test and acquisition opportunities with the Department of Homeland Security, while avoiding duplication of effort in these areas; and
- Ensuring the smooth transition of appropriate missions, technologies, and capabilities to the civil sector.
- Complementing these activities will be a long-term effort with our federal partners to identify specific, frequently requested DoD capabilities for possible transition to the civil sector.

Core Capability: Capable international partners and effective defense-to-defense relationships

Because it is the Department's first priority, homeland defense must be a central, carefully considered element of our defense-to-defense relationships with key allies and friends abroad. The United States fosters strong defense relationships worldwide for many reasons of national security interest. Two such reasons are to strengthen allied military contributions to collective security and to enhance US capabilities through exposure to partners' expertise. Thus, DoD has an active security cooperation program, directed through the Secretary of Defense's Security Cooperation Guidance, which encourages mutual improvements to support coalition operations and to ensure continued interoperability. Clearly, our homeland defense will be substantially strengthened through the cooperation and assistance of international allies. **We will therefore strengthen DoD's emphasis in the Security Cooperation Guidance on homeland defense and civil support issues, with particular focus on improved information sharing in defense-to-defense interactions.**

Our North American neighbors, Canada and Mexico, are particularly vital to the protection of the US homeland and the continent. The Department also places special emphasis on cooperative homeland defense efforts with friendly nations in the Pacific and the Caribbean and with our NATO allies.

The primary mechanism for US-Canadian cooperation on homeland defense is the North American Aerospace Defense Command. Dedicated to the defense of US and Canadian airspace, NORAD has evolved from a Cold War institution to an agile 21st

IV. Core Capabilities

century counterterrorism capability reflecting an integrated, flexible bi-national approach to air defense. Over the next decade, the Department of Defense, in conjunction with the Department of State and the Department of Homeland Security and working with our Canadian partners, will further refine and build on the NORAD concept. This effort will identify mechanisms for sharing information across all operational domains—air, maritime, and land, with shared awareness of the North American maritime domain as the first priority.

Given the importance of Mexico to US homeland defense, US-Mexican counterterrorism cooperation is essential. The Department will work with the Department of Homeland Security, the Department of State, and Mexico to anticipate and plan for crisis coordination and consequence management following a terrorist attack. Cooperation with Mexico on law enforcement and immigration issues is substantial, especially in counternarcotics and border control operations. Defense-to-defense cooperation requires similar emphasis and must be pursued with due respect for the Mexican government's policy goals and legal constraints. Traditional security assistance

tools are pivotal in further developing mutually beneficial defense capabilities and arrangements.

Just as defense of the US homeland begins well beyond our geographic boundaries, so too must our cooperative efforts to improve that defense. The expansion of information and intelligence sharing with foreign partners is critical to the success of this Strategy. Friendly and allied nations often possess significant information relating to terrorism, smuggling, and other US concerns. Incorporating this information into our base of knowledge could significantly improve US readiness both for homeland defense and civil support missions.

Beyond the information realm, some nations have significant expertise to share with the United States in combating terrorism and other mission areas related to homeland defense. The United States likewise has much to gain in increasing the homeland defense capabilities of friendly nations. The Department will therefore expand combined education, exercise, training, and experimentation initiatives related to homeland defense.



V. Implications of the Strategy

"The threats and enemies we must confront have changed, and so must our forces."

The National Security Strategy of the United States of America

September 2002

The Strategy for Homeland Defense and Civil Support requires adjustments in DoD forces and capabilities, resource allocation, and technology development. Given resource constraints, meeting the Strategy's homeland defense and civil support objectives will require accommodation of competing demands within the National Defense Strategy.

Force Structure

An understanding of the force structure implications of the Strategy for Homeland Defense and Civil Support is critical to the Department's ability to size and shape forces correctly for diverse military missions. **This strategy reflects a Total Force approach to homeland defense missions, incorporating the capabilities of Active Duty, National Guard, and Reserve forces that will be trained and equipped primarily for warfighting missions in the forward regions and approaches.** Identified forces must also be prepared to conduct the full spectrum of domestic civil support missions when directed by the President or the Secretary of Defense to do so. The types of forces employed for any given homeland defense mission will be situation-dependent. Additionally, the type, scope, and location of events, competing DoD missions, resident civilian capabilities, and a host of other variables will affect requests for defense support of civil authorities.

To execute this diverse range of missions effectively, DoD must ensure the Total Force, both reserve and active components, is:

- **Timely** in response and readily accessible. Homeland defense and civil support missions require a rapid response, often measured in hours, not days.
- **Trained and equipped** to achieve the highest degree of readiness in a broad array of mission sets.
- **Transformed** to meet the terrorist challenges of a post-Cold War security environment. Forces must be agile and interoperable, taking advantage of networked capabilities.

As part of the Quadrennial Defense Review, the Department of Defense will analyze force requirements for homeland defense and key civil support missions. To be most effective, this analysis must take into account the projected capabilities of civilian agencies where those capabilities may affect DoD's force requirements.

Focused Reliance upon the Reserve Component

Homeland defense and civil support are Total Force responsibilities. However, the nation needs to focus particular attention on better utilizing the competencies of the National Guard and Reserve Component

organizations. The National Guard is particularly well suited for civil support missions. As with other Reserve components, the National Guard is forward deployed in 3,200 communities through the nation. In addition, it is readily accessible in State Active Duty and Title 32 status, routinely exercised with local law enforcement, first responders, and the remainder of the Total Force, and experienced in supporting neighboring communities in times of crisis. In addition, Reserve forces currently provide many of the key capabilities needed for homeland defense and civil support, including intelligence, military policing, medical expertise, and chemical decontamination. The most promising areas for employment of the National Guard and Reserve forces include the following missions:

- ***Air and Missile Defense***, including surveillance and manning of ground-based defense systems.
- ***Maritime Security***, including Naval Reserve augmentation of active component and Coast Guard capabilities engaged in intelligence and surveillance, critical infrastructure protection, port security, and maritime intercept operations. **The Naval Reserve should continue to transform to meet 21st century transnational terrorist threats, including the maritime transportation of CBRNE to the United States.** Therefore, DoD will evaluate the operational benefit of employing Naval Reserve maritime and aviation capabilities in support of emerging homeland defense missions.
- ***Land defense***, including missions requiring Quick Reaction Forces/Rapid Reaction Forces. Reserve forces, including the National Guard, Army Reserve, and Marine Corps Reserve, are capable of serving in reaction force roles when sufficiently trained and resourced. For example, **the Army is considering whether to use existing National Guard force structure to form modular reaction forces, an initiative that could provide additional capabilities to support domestic land defense.**
- ***CBRNE response***, including specific capabilities for detection, extraction, decontamination, and medical care. Chemical companies resident in the Army Reserve can provide significant capabilities and are trained and equipped for CBRNE assessment as well as extraction and decontamination of mass casualties. **The National Guard WMD Civil Support Teams, which will be located in all states and territories and the District of Columbia, can be federalized, if required. The National Guard Chemical-Biological-Radiological-High Explosives Enhanced Force Packages (NGCERFPs) initiative—task-organized from existing force structure—has the potential for providing CBRNE response capabilities.** The Reserve Component can also offer significant assistance with security, engineering, transportation, communications, medical response, and many other homeland defense and civil support requirements related to CBRNE response. **The effective employment of National Guard forces in state, Title 32, or Title 10 status could increase the availability of other US military forces for overseas deployments.**
- ***Critical Infrastructure Protection***, including the performance of compre-

hensive assessments at critical infrastructure sites and utilization of Reserve component forces for quick reaction requirements, when sufficiently trained and resourced, and local security at key defense and non-defense critical infrastructure sites, when directed.

Technology

Implementation of the Strategy for Homeland Defense and Civil Support may require several new technological investments. Three areas of particular interest for further exploration are advanced information and communications technology, new generations of sensors, and non-lethal capabilities.

Advanced Information and Communications Technology

Technological and organizational improvements for homeland security and homeland defense will benefit from focused investment in advanced information technology especially to prevent, intercept, and respond to terrorist activity. Whether the objective is improved maritime domain awareness and operations, interception of weapons of mass destruction, response to chemical or biological attacks, or continuity of operations and government, improvement in information technology is a critical enabler to addressing current capability shortfalls. Advanced modeling and simulation techniques for threat identification, pattern analysis, risk assessment, dependency analysis, and cost/benefit calculus are critical for addressing issues of data sharing, security, and interoperability. Without these tools, the return on investments in other areas, such as improved sensors, detectors, command and control,

and human intelligence collection and analysis, will be incomplete and insufficient.

Equally pivotal are potential advances in communications technologies, particularly those supporting ground-mobile and airborne communications. DoD must also work to reduce the size and power requirements of mobile communications systems. It must also invest in technologies that shield them against electromagnetic effects.

Sensors

New generations of sensors and sensor platforms will enhance threat awareness in the air, maritime, and land domains by helping to close current gaps over much of the maritime domain and in domestic airspace, particularly at low altitudes. Shared sensor technology could also play an important role in enabling improved border surveillance by civilian agencies.

The placement of sensors on high altitude platforms, including new generations of unmanned aerial vehicles, satellites, and aerostats, could allow sustained surveillance of wide areas of the earth's surface. These sensors could also enhance defenses against low-flying cruise missiles. Some new ground sensors are expected to have an over the horizon capability with applications for homeland defense and homeland security missions.

New sensor technologies could also have utility for maritime defense, including the non-acoustic detection of underwater vehicles, objects, and swimmers. New sensor capabilities could also be useful for a wide range of other tasks, such as remote detection of concealed CBRNE weapons aboard ships and for mapping the location

and extent of contamination should adversaries use these weapons. Finally, **DoD must fully integrate its sensors as well as others on which it relies with information networks in order to coordinate their use and rapidly distribute information to operational and policy users.**

Non-Lethal Capabilities

The transnational terrorist attack of September 11, 2001, made it clear that the US homeland is now part of the enemy battle space. Therefore, we may be required to defeat attacks in close proximity to major civilian population centers. Non-lethal capabilities hold some promise as an effective alternative to deadly force. The Department will therefore examine the potential operational employment of non-lethal weapons for homeland defense missions, particularly those where civilian loss of life can be effectively minimized.

Non-lethal technologies with potential application to homeland defense missions include:

- **Counter-personnel technology**, used to deny entry into a particular area, temporarily incapacitate individuals or groups, and clear facilities, structures, and areas.
- **Counter-material technology**, to disable, neutralize, or deny an area to vehicles, vessels, and aircraft, or disable particular items of equipment.
- **Counter-capability technology**, to disable or neutralize facilities, systems, and CBRNE.

The Department will expand basic research into the physiological effects of non-lethal

weapons. The Department should also identify opportunities to share appropriate non-lethal capabilities with domestic law enforcement agencies, consistent with applicable law.

Rapid Prototyping of Emerging Capabilities

Advanced Concept Technology Demonstrations (ACTDs) are a key DoD vehicle for rapidly fielding promising technologies. The objectives of an ACTD are to conduct meaningful demonstrations of the capability, develop and test concepts of operations to optimize military effectiveness, and, if warranted, prepare to transition the capability into acquisition without loss of momentum. Currently, there are over 25 ACTDs with relevance to homeland defense and homeland security such as the Homeland Security/Homeland Defense Command and Control Advanced Concept Technology Demonstration. The Department will ensure that requirements for homeland defense and civil support are properly addressed in the ACTD process in the decade ahead. The Department will continue working with the Department of Homeland Security and other domestic and international partners to encourage their participation in ACTDs as appropriate. **DoD will also continue to leverage innovative capabilities arising from private sector initiatives, many of which are fostered through the interagency Technical Support Working Group (TSWG).**

Funding

With many important programs competing for finite resources, proper funding and budget oversight for homeland defense and

CBRNE consequence management missions is vital. Currently, the Department accounts for homeland defense activities through a variety of widely dispersed programs and funding lines. Funding for homeland defense is not accounted for consistently; it can be found in every Military Department and combatant command and numerous initiatives under the purview of the Office of the Secretary of Defense.

Funding Implications

In developing planning and programming guidance to implement the Strategy for Homeland Defense and Civil Support, DoD must thoroughly assess the fiscal implications of attaining and sustaining requisite core capabilities. Determining the relative costs and benefits of each of the following areas merit immediate attention:

- **Expanding communications infrastructure** and enhancing DoD's ability to share vital information while protecting the integrity of the Global Information Grid;
- **Improving intelligence assets** to enhance overall threat awareness throughout all domains;
- Developing and procuring **advanced technologies** to maximize awareness of potential threats;
- Ensuring the necessary capabilities, types, and number of transformational forces needed to effectively conduct an active, layered **maritime defense** against transnational threats, including CBRNE attacks;
- Implementing DoD's **Defense Critical Infrastructure Protection** responsibilities;

- Furthering investments in the research, testing, and fielding of **non-lethal weapons** capabilities;
- Providing support for DoD **continuity of operations** in the event of a national emergency or catastrophe; and
- **Transforming the Reserve component** for homeland defense and civil support missions.

In the course of implementing this strategy, the Department must not take on responsibilities and costs for homeland security missions better addressed by other federal, state, local, or tribal authorities. This will require close coordination and continuing cooperation with the Department of Homeland Security and other interagency partners, including finding efficiencies in the research, development, testing, acquisition, and deployment of capabilities that span multiple agencies.

Managing Homeland Defense and Civil Support Risk

The Department must employ a risk management strategy that appropriately acknowledges the importance of an active, layered homeland defense. **An active, layered defense integrates homeland defense and forward operations conceptually and operationally.** Therefore, the Department will assess homeland defense and civil support mission risks and resources in the context of all of the requirements outlined in the National Defense Strategy.

The Strategy places a premium on the Department's primary responsibility for protecting the US homeland from attack. A second priority is to meet DoD's most challenging civil support mission—CBRNE consequence management. Specifically, the Strategy's risk management approach is as follows:

Lead. The Department's key lead objectives are to achieve maximum awareness of threats, deter, intercept, and defeat threats at a safe distance, and achieve mission assurance. **DoD must not accept undue risk in its active defense of the US homeland from direct air, land, or maritime threats.** The capability and readiness of US forces to intercept and defeat these threats must be assured. Further, because the most critical element of successfully defeating threats to the US homeland is shared situational awareness, the Department will focus special attention in this area. DoD accepts some operational risk in achieving mission assurance.

Support. Transnational terrorists have a demonstrated intent to acquire weapons of mass destruction and exploit US vulnerabilities in order to employ such weapons against potential domestic targets. Accordingly, the Department will reduce

risk by improving its consequence management capabilities for responding to multiple, simultaneous CBRNE mass casualty attacks in the United States. **DoD will maintain a ready, capable, and agile command and control structure, along with competently trained forces, to assist civilian authorities with catastrophic incident response. However, with the exception of a dedicated command and control element (currently the Joint Task Force-Civil Support) and the National Guard's WMD Civil Support Teams, DoD will continue to rely on dual-capable forces for consequence management and other defense support of civil authorities.** The Department minimizes the risk that dual-capable forces may be assigned to other high priority missions by deconflicting overseas and domestic force requirements wherever possible.

Enable. Enabling domestic and international partner capabilities is an important priority for the Department. **The Department aims to decrease long-term risk by improving the capabilities of our interagency and international partners.** DoD accepts some risk in achieving the "Enable" objective in order to address other, more immediate, "Lead" and "Support" objectives.



VI. Conclusion

"The battle is now joined on many fronts. We will not waver, we will not tire, we will not flinch, and we will not fail. Peace and freedom will prevail."

*President George W. Bush
October 7, 2001*

The United States faces ruthless enemies who seek to break our will and exploit America's fundamental freedoms. Our adversaries are eager to employ violence against Americans at home. In this environment, the Department of Defense's paramount goal will continue to be the defense of the US homeland from direct attack.

A new kind of enemy requires a new concept for defending the US homeland. **The terrorist enemy now considers the US homeland a preeminent part of the global theater of combat, and so must we.** We cannot depend on passive or reactive defenses but must seize the initiative from adversaries.

The active, layered defense articulated in this Strategy seamlessly integrates US capabilities in the forward regions of the world, the global commons, the geographic approaches to the US territory, and within the United States. Whether in a leading, supporting, or enabling role, the Department of Defense, guided by this Strategy and consistent with US law, will work with an intense focus to protect the US homeland and the American people.

When fully realized, this Strategy will transform the Department's homeland defense and civil support capabilities. The nation will have effective intelligence, surveillance, and reconnaissance capabilities for home-

land defense; and information will be widely shared with relevant decision-makers. The Department will have well-trained and responsive forces for homeland defense missions that will use improved technology and operational concepts to eliminate potential seams between the maritime, air, and land domains. Additionally, **the Department will achieve unity of effort with our interagency and international partners in executing homeland defense and civil support missions.**

The effectiveness of any strategy is ultimately in the hands of those charged with its implementation. The Department of Defense will carefully consider the potential implications of this Strategy for force structure, technology, and funding. It will also continually reevaluate the strategy, adapting it as needed for the dynamic international environment and changing US policy and capabilities.

The Department of Defense must change its conceptual and cultural approach to homeland defense. The Department can no longer think in terms of the "home" game and the "away" game. There is only one game. The Strategy for Homeland Defense and Civil Support is a significant step toward this strategic transformation. Defending the US homeland—our people, property, and freedom—is our fundamental duty. Failure is not an option.