This chapter places the homeland security mission in the context of the Constitution, the nation’s national security, national military strategy, and the Army Strategic Planning Guidance; presents our working definition of homeland security; and describes the task areas that are the essence of the homeland security mission.

THE CONSTITUTIONAL AND LEGAL CONTEXT

The fundamental justification and broader context for homeland security activities can be found in the Preamble; Article I, Section 8; and Article IV, Section 4, of the Constitution of the United States. The Preamble includes the basic “insure domestic tranquility” and “provide for the common defense” justifications:

[In] Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity.

Article I, Section 8, elaborates on the circumstances in which the military might be domestically employed:

Congress shall have Power . . . to provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections, and repel Invasions.

And Article IV, Section 4, expands on this authority:
The United States shall guarantee to every State in this Union a Republican Form of Government, and shall protect each of them . . . against domestic Violence.

Federal laws provide the specific mechanisms for federal (including military) support to civil authorities, particularly in the context of "civil emergencies":

The modern authorization for Federal support to civil authorities is based on the Robert T. Stafford Disaster Relief and Emergency Assistance Act (P.L. 93-288) and the Economy Act. The former enables the Federal Government to "provide assistance to U.S. states, territories, and possessions to alleviate suffering and mitigate damage resulting from major disasters and civil emergencies." The latter empowers Federal agencies to provide routine support to each other under certain conditions if reimbursed. (Grange and Johnson, 1997.)

Homeland security activities are even more apparent in the warrant given the Department of Defense (DoD):

[DoD] maintains and employs the armed forces to:

- Support and defend the Constitution of the United States against all enemies, foreign and domestic.
- Ensure, by timely and effective military action, the security of the United States, its territories, and areas vital to its interests.
- Uphold and advance the national policies and interests of the United States.
- Safeguard the internal security of the United States. (DoD, 1987, pp. 17–18.)

THE STRATEGIC CONTEXT

The strategic context for homeland security is described well in the report of the National Defense Panel (NDP):

The United States enters the new millennium as the preeminent political, economic, and military power in the world. Today we are in a relatively secure interlude following an era of intense inter-
national confrontation. But we must anticipate that future adversaries will learn from the past and confront us in very different ways.

We can safely assume that future adversaries will have learned from the Gulf War. It is likely that they will find new ways to challenge our interests, our forces, and our citizens. They will seek to disable the underlying structures that enable our military operations. Forward bases and forward-deployed forces will likely be challenged and coalition partners coerced. Critical nodes that enable communications, transportation, deployment, and other means of power projection will be vulnerable.

Our domestic communities and key infrastructures may also be vulnerable. Transnational threats may increase. As recently stated by [Defense] Secretary [William S.] Cohen, the proliferation of nuclear, chemical, and biological weapons and their delivery means will pose a serious threat to our homeland and our forces overseas. Information systems, the vital arteries of the modern political, economic, and social infrastructures, will undoubtedly be targets as well. The increasing commercialization of space makes it feasible for state and nonstate actors alike to acquire reconnaissance and surveillance services.

In short, we can expect those opposed to our interests to confront us at home and abroad—possibly in both places at once—with asymmetrical responses to our traditional strengths. (National Defense Panel, 1997, p. ii.)

Importantly, the report implies that adversaries may use a range of unconventional weapons (WMD, cyber attacks, etc.) to target both theater forces and the U.S. homeland in future major theater wars (MTWs).

**National Security Strategy**

In October 1998, the White House released an updated version of the U.S. National Security Strategy (NSS) titled *A National Security Strategy for a New Century*, identified WMD and terrorism as two concerns that transcended national borders:

The possibility of terrorists and other criminals using WMD—nuclear, biological, and chemical weapons—is of special concern.
Threats to the national information infrastructure, ranging from cyber-crime to a strategic information attack on the United States via the global information network, present a dangerous new threat to our national security. We must also guard against threats to our critical national infrastructures—such as electrical power and transportation—which increasingly could take the form of a cyber-attack in addition to physical attack or sabotage, and could originate from terrorist or criminal groups as well as hostile states. (White House, 1998d, pp. 1 and 6–8.)

Potential enemies, whether nations, terrorist groups, or criminal organizations, are increasingly likely to attack U.S. territory and the American people in unconventional ways. Adversaries will be tempted to disrupt our critical infrastructures, impede continuity of government operations, use weapons of mass destruction against civilians in our cities, attack us when we gather at special events, and prey on our citizens overseas. The United States must act to deter or prevent such attacks and, if attacks occur despite those efforts, must be prepared to limit the damage they cause and respond decisively against the perpetrators. . . .

Weapons of mass destruction pose the greatest potential threat to global stability and security. Proliferation of advanced weapons and technologies threatens to provide rogue states, terrorists, and international crime organizations the means to inflict terrible damage on the United States, its allies, and U.S. citizens and troops abroad. (White House, 1998d, pp. 1 and 6–8.)

The solution, in the conception of the National Security Strategy, is a broad, national effort that relies on interagency efforts at the federal level and a program that knits these federal capabilities together with local and state capabilities:

At home, we must have effective capabilities for thwarting and responding to terrorist acts, countering international crime and foreign intelligence collection, and protecting critical national infrastructures. Our efforts to counter these threats cannot be limited exclusively to any one agency within the U.S. Government. The threats and their consequences cross agency lines, requiring close cooperation among Federal agencies, state and local governments, the industries that own and operate critical national infrastructures, nongovernmental organizations, and others in the private sector. (White House, 1998d, pp. 1 and 6–8.)
National Military Strategy

The most recent version of the National Military Strategy (NMS) was published in 1997, prior to the current version of the National Security Strategy; this may account for its relative inattention to the issue of homeland security. The 1997 NMS observes:

Our National Military Strategy depends first and foremost upon the United States remaining secure from external threats. A secure homeland is fundamental to U.S. global leadership.

The NMS nevertheless devotes scant attention to homeland security per se, although it does touch on such threats as state and nonstate actors and asymmetric warfare against the United States. For example, the NMS states:

Some state or nonstate actors may resort to asymmetric means to counter the U.S. military. Such means include unconventional or inexpensive approaches that circumvent our strengths, exploit our vulnerabilities, or confront us in ways we cannot match in kind. Of special concern are terrorism, the use or threatened use of WMD, and information warfare. These three risks in particular have the potential to threaten the U.S. homeland and population directly and to deny us access to critical overseas infrastructure. . . . We must increase our capabilities to counter these threats and adapt our military doctrine, training, and equipment to ensure a rapid and effective joint and interagency response. (Joint Chiefs of Staff, 1997.)

The Army Strategic Plan

Among the vital interests identified in the 1999 Army Strategic Planning Guidance (ASPG) is “the sovereignty of the United States, to include the safety of the population and the security of critical physical and information infrastructure.”

The ASPG envisions a threat environment that contains both transnational and asymmetric threats to the nation. Transnational

1The list of vital interests identified in the ASPG was extracted from the Defense Planning Guidance.
threats to the homeland include enemies who “use the international telecommunications system to synchronize an impressive set of capabilities to delay or disrupt our military operations or attack the U.S. homeland,” while asymmetric threats include the following:

In the near term, these threats will remain largely limited to traditional concepts and techniques but terrorism and WMD, facilitated by the spread of dangerous technologies, are issues of immediate and special concern. In the mid-term, the United States will face further proliferation of dangerous technologies and expansion of asymmetric concepts and doctrine to include the employment of techniques that exploit social, cultural, technological, and/or environmental change, such as urbanization. The proliferation of information technologies will provide the catalyst for a technologically sophisticated state, group, or individual to target, via computer network attack, the U.S. National Information Infrastructure (NII) or Defense Information Infrastructure (DII). . . . In the long term, we will see the further development of advanced asymmetrical capabilities and significantly more sophisticated capabilities to conduct information operations. (U.S. Army, 1999, p. 8.)

In light of these emerging threats, the ASPG accordingly has a revised set of mission areas that now explicitly includes support to homeland security (U.S. Army, 1999, pp. ii and 52):

[T]he Army will provide capabilities to conduct operations to support homeland defense [emphasis in original]. America’s Army must be ready to defend U.S. territory, population, and infrastructure against strategic attack and against emerging transnational threats. Pursuant to Presidential Decision Directive (PDD) 62, these responsibilities will include a growing involvement of the Army, as the Executive Agent (EA) for the Department of Defense (DoD) Domestic Preparedness Program, in supporting domestic authorities in preparation for and execution of crisis response and consequence management with regard to attacks utilizing WMD. The Army will also be involved in supporting PDD 63 to protect and reduce the vulnerability of critical infrastructure including telecommunications; energy; banking and finance; transportation; water; and emergency service facilities. The nature of the emerging threats against the homeland will place a premium on the Army’s ability to conduct operations in NBC environments and execute computer network defense while effectively working with sister Services; other federal agencies; state and local governments; and
non-governmental organizations. Finally, the Army is responsible for developing and testing a treaty-compliant, fixed, land-based National Missile Defense (NMD) system, as part of a Joint NMD program, that will provide the option to deploy initial capability in 2003, if so directed. (U.S. Army, 1999, p. 13.)

Thus, although each of the policy documents touches on many of the threats that have led to consideration of a homeland security mission, neither the National Security Strategy, the NMS, nor the Army strategic plan clearly define homeland security as a critical, separate mission consisting of specific task areas or place it in the context of the current defense planning framework of two nearly simultaneous MTWs.2

THE DOMESTIC POLITICAL CONTEXT

The response to these emerging threats was three major programs: combating terrorism, enhancing domestic preparedness against WMD, and critical infrastructure protection.

White House Actions

Within the Clinton administration, increasing concern about the proliferation of WMD led, on November 14, 1994, to Executive Order 12938, in which the president declared a national emergency:

I, William J. Clinton, President of the United States of America, find that the proliferation of nuclear, biological, and chemical weapons ("weapons of mass destruction") and of the means of delivering such weapons, constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States, and hereby declare a national emergency to deal with that threat. (Executive Order, 1994.)

The Executive Order then went on to enumerate the responsibilities of the departments and agencies in nonproliferation activities. On

---

2The NMS does discuss supporting “domestic authorities in combating direct and indirect threats to the U.S. homeland” in a subsection on multiple, concurrent smaller-scale contingency operations but does so only in passing.
November 12, 1998, the President extended the national emergency and amended the original executive order to broaden the types of proliferation activities covered (White House, 1998e).

Two PDDs provided subsequent policy guidance for combating terrorism and WMD:

- PDD 39, June 21, 1995, directed that efforts to combat terrorism include reducing vulnerabilities to terrorism, deterring and responding to terrorist acts, having capabilities to prevent and manage the consequences of terrorist use of NBC weapons, including those of mass destruction (FEMA, 1996).

- The Combating Terrorism directive, PDD 62, May 22, 1998, “highlighted the growing threat of unconventional attacks against the United States and detailed a new and more systematic approach to fighting terrorism by bringing a program management approach to U.S. counterterrorism efforts.” (White House, 1998c.)

In a similar vein, concern grew about threats to the nation’s physical and electronic critical infrastructures.

Chartered a year earlier, the President’s Commission on Critical Infrastructure Protection reported in October 1997 that:

[W]e found all our infrastructures increasingly dependent on information and communications systems that criss-cross the nation and span the globe. That dependence is the source of rising vulnerabilities and, therefore, it is where we concentrated our effort. We found no evidence of an impending cyber attack which could have a debilitating effect on the nation’s critical infrastructures. While we see no electronic disaster around the corner, this is no basis for

---

3 The directive also established the office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, which oversees policies and programs in counterterrorism, protection of critical infrastructure, and preparedness and consequence management for WMD.

4 “Critical Infrastructures” are defined as “those physical and cyber-based systems essential to the minimum operations of the economy and government. These systems are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.” (White House, 1998b; Executive Order, 1996.)
The commission accordingly called for a national effort to assure the security of the nation’s increasingly vulnerable and interconnected infrastructures. And in May 1998, PDD 63 was released, building on the Commission report, and described as:

[T]he culmination of an intense, interagency effort to evaluate the Commission’s recommendations and produce a workable and innovative framework for critical infrastructure protection . . . [PDD 63] sets a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003, and significantly increased security to government systems by the year 2000, by immediately establishing a national center to warn of and respond to attacks . . . [and] ensuring the capability to protect critical infrastructures from intentional acts by 2003. (White House, 1998b.)

The PDD also established “a National coordinator whose scope will include not only critical infrastructure but also foreign terrorism and threats of domestic mass destruction (including biological weapons) because attacks on the United States may not come labeled in neat jurisdictional boxes” (White House, 1998b), as well as a number of other organizations. These included: a National Infrastructure Protection Center (NIPC) at the FBI, a National Infrastructure Assurance Council, and a Critical Infrastructure Assurance Office (CIAO) in the Department of Commerce. Importantly, the directive required each department and agency to work to reduce its own exposure to new threats. The PDD also encouraged the private sector establishment of Information Sharing and Analysis Centers (ISACs) “modeled on the Centers for Disease Control and Prevention.”

Congressional Action

On the congressional front, on June 27, just two days after the bombing of the Al Khobar barracks in Saudi Arabia in which 19 Americans died, the Senate adopted an amendment aimed at “preventing terrorist assaults in the United States with nuclear,
chemical, or biological weapons and at helping cities deal with such attacks if they occurred” (Congressional Quarterly, 1997, p. 8-8). As described by Congressional Quarterly:

The amendment, sponsored by Nunn, Lugar, and Pete V. Domenici, R-N.M., proposed to authorize $235 million to counter terrorism, including $61 million for research on devices to detect and prevent the spread of “weapons of mass destruction.” The Defense and Energy departments would be authorized, under some circumstances, to respond to a domestic terrorist attack that employed nuclear, chemical, or biological weapons and to spend up to $80 million to help local police, fire, and emergency medical service agencies prepare for such an attack. The amendment also included $94 million to expand the scope of the Nunn-Lugar program to include activities such as disposing of spent nuclear fuel from Russian warships and rebuilding some nuclear power plants so they could not produce radioactive material for use in weapons production. (Congressional Quarterly, 1997, p. 8-8.)

In September 1996, Congress passed Public Law 104-201, the National Defense Authorization Act for Fiscal Year 1997, Title XIV of which was called the Defense Against Weapons of Mass Destruction Act, also known as the Nunn-Lugar-Domenici legislation. It required DoD to enact:

[A] program to provide civilian personnel of Federal, State, and local agencies with training and expert advice regarding emergency responses to a use or threatened use of a weapon of mass destruction or related materials.

Specific actions that were authorized included the following:

• Using the National Guard and other reserve components for carrying out the program.

• Establishing “a designated telephonic link (commonly referred to as a ‘hot line’) to a designated source of relevant data and expert advice for the use of State or local officials responding to such emergencies.”

• Loaning appropriate equipment.

• Assisting the Secretary of HHS in the “establishment of metropolitan emergency medical response teams (commonly
referred to as ‘Metropolitan Medical Strike Force Teams’) to provide medical services that are necessary or potentially necessary by reason of a use or threatened use of a weapon of mass destruction.”

- Developing and maintaining “at least one domestic terrorism rapid response team composed of members of the Armed Forces and employees of the Department of Defense who are capable of aiding Federal, State, and local officials in the detection, neutralization, containment, dismantlement, and disposal of weapons of mass destruction containing chemical, biological, or related materials.”

Taken together, the result of all of this administration and congressional activity has been a dramatic increase in funding for antiterrorism, counterterrorism, critical infrastructure protection, and programs countering WMD, across a broad array of functional areas. Federal spending for combating terrorism in Fiscal Year 2000 is expected to be approximately $10.0 billion, including:

- $8.613 billion for antiterrorism and counterterrorism programs, including $1.385 billion for combating WMD; and
- $1.464 billion for protection of critical infrastructure and computer security, including $500 thousand for R&D efforts.

To provide better oversight of this complex array of programs, Congress enacted subsequent language requiring the President to report annually on governmentwide spending by departments and agencies to combat terrorism and WMD. In 1999, the Senate Armed Services Committee set up the Emerging Threats and Capabilities Subcommittee “to provide a focus for the Department of Defense’s efforts to counter new and emerging threats to vital national security interests, . . . such as the proliferation of weapons of mass destruction, international terrorism directed at U.S. targets both at

---

5The overall program will be described in Chapter Four.

6The Fiscal Year 1998 National Defense Authorization Act (P.L. 105-85) required the President to provide an unclassified report on governmentwide spending to combat terrorism, and Section 1403 of the Fiscal Year 1999 National Defense Authorization Act (P.L. 105-261) required an annex providing information on domestic emergency preparedness programs for response to terrorist incidents involving WMD.
home and abroad, information warfare, and narco-trafficking” (U.S. Senate, 1999, p. 6).

Leadership Statements

In addition to efforts to mitigate the threats through the programs just described, U.S. policymakers have sought to balance the need to alert the public against the desire to avoid creating panic or unfounded fears. For example, in 1999 President Clinton stated:

I would say that if the issue is how probable [a biological or chemical attack] is in the very near term, an American city or community would be affected, I’d say you probably shouldn’t be too worried. But if the issue is, is it a near certainty that at some time in the future there will be some group, probably a terrorist group, that attempts to bring to bear either the use or the threat of a chemical or biological operation, I would say that is highly likely to happen sometime in the next few years. And therefore, I would say the appropriate response is not worry or panic, but taking this issue very seriously . . . and then to try to make sure we are doing everything we can to stop this. (“In the President’s Words,” 1999.)

I want to raise public awareness of this, without throwing people into an unnecessary panic . . . [Americans should] not be afraid or asleep. I think that’s the trick. (Miller and Broad, 1999.)

When he was asked which threats worried him most, the President answered:

A chemical attack would be horrible, but it would be finite. You know, it’s just like—for the people who went through Oklahoma City, nothing could be more horrible. But it didn’t spread. And the thing that bothers people about biological agents is that, unless they’re properly diagnosed, contained and treated, that it could spread. For example, we know that if all of us went to a rally on the Mall [in Washington, D.C.,] tomorrow with 10,000 people, and somebody flew a low-flying crop duster and sprayed us all with biological agents from, let’s say, 200 feet, that no matter how toxic it were, half of us would walk away for reasons no one quite understands. You know, either we wouldn’t breathe it, or we’d have some miraculous resistance to it. And the half of us, somebody would have to diagnose in a hurry and then contain and treat . . . I’m not
trying to be macabre, but you asked me what keeps me awake at night, and that bothers me. ("In the President’s Words," 1999.)

Richard Clarke, National Coordinator for Security, Infrastructure, and Counterterrorism, also stressed the administration’s desire to draw attention to the issue without alarming the public:

The message that we want to get across today is not that we know of an imminent attack—we do not know of any imminent attack being planned on the United States using chemical or biological weapons, or using cyber attack techniques. But we do want to raise consciousness, in the American people, in the scientific community, and in the Congress, that such attacks are growing increasingly likely. And as the President said, we need to be ahead of the power curve; we need to be prepared to defend ourselves against those attacks and, in so doing, perhaps prevent them; at least to be able to mitigate their effects. (White House, 1999b.)

Homeland security has not been free of debate, however. A trial balloon that floated the idea of creating a separate unified command for homeland security was met with visible concern by organizations ranging from the American Civil Liberties Union to conservative groups.7 There are also indications that the notion of a broader DoD (and Army) role in crisis management has not yet been accepted by key agencies. In short, the evolution of the homeland security problem seems likely to play out in a turbulent political atmosphere.

PUBLIC ATTITUDES

The Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction

7For example, in the words of the American Civil Liberties Union (1999):

A broad counterterrorism program being considered by the Clinton administration could include measures that severely jeopardize Americans’ liberties, the American Civil Liberties Union charged today. The measures include the creation of a domestic military “commandante” responsible for fighting domestic crimes of terrorism.

The proposal also met with criticism from the right. For more on this debate, see Graham (1999) and MSNBC (1999).
stated, “Every American should understand that . . . WMD—nuclear, biological, and chemical weapons and their means of delivery—pose a grave threat to the United States and to our military forces and our vital interests abroad” (Commission, 1999, p. v). As judged by public opinion, the American people seem to have gotten the message. Public opinion data reveal a differentiated set of attitudes that indicate a reasonable level of concern and a strong desire to see action taken against the threats but no expectation that the measures taken can ever eliminate the possibility of attacks:

- Although fewer than 1 percent of Americans think of terrorism when asked to identify the most important problem facing the country,8 more than half of those polled in September 1996 indicated that terrorism was one of the most important problems for the nation today,9 and about one in three polled in April 1997 identified terrorism as the greatest threat facing the United States in coming years, and the greatest threat to world peace.10

- Nearly three out of four believe that there is a chance that terrorists could attack with WMD, but fewer than one in six said they worried a great deal about this.11

---

9Princeton Survey Research Associates asked: “(I’d like you to think about the problems we face as a nation today. As I read you some possible problem areas, please tell me if you think each is one of the most important problems facing this country, important, but not as important, or not too important.) How important a problem for the country is . . . the threat of terrorism?” Another 33 percent said that it was an important problem, but not one of the most important problems facing the nation. PSRA, September 3–15, 1996.
10The Pew Research Center for the People and the Press asked two questions about the perceived threat in April 1997. One asked: “In coming years, which one of the following do you think will be the greatest threat to the United States . . . terrorism, international crime and drug rings, illegal immigration, China, Russia, or some other country?” Thirty-five percent identified “terrorism” as the greatest threat in coming years, while 39 percent identified “international crime and drug rings.” Each of the other responses elicited less than 10 percent. Also asked was: “Over the next century, which one of the following do you think will be the greatest threat to world peace?” and offered the same options. Thirty-two percent identified “terrorism,” while 26 percent identified “international crime and drug rings.” Pew Research Center for the People and the Press, April 3–6, 1997.
11In March 1996 and April 1997, the Pew Research Center for the People and the Press asked: “Do you think there is much of a chance that terrorists could use a nuclear, chemical, or biological weapon to attack a U.S. city, or don’t you think there is much of
• Similarly, nearly six in ten believe that a foreign country could launch a nuclear attack against the United States, although fewer than one in ten said they worried a great deal about it.\textsuperscript{12}

• When asked whether they perceive the greater threat of terrorism to come from inside or outside the country, nearly half (47 percent) indicated inside while four in ten said outside, and 11 percent volunteered “both.”\textsuperscript{13}

• There also were indications at the time of the Oklahoma City bombing in April 1995 that a slight majority of the public believed that bombings like that may become common in the future.\textsuperscript{14}

Regarding the government’s response to the emerging threat:

• In July 1996, the public was evenly split between those who believed that the U.S. government was doing enough to prevent terrorism in this country (48 percent) and those who did not think so (48 percent).\textsuperscript{15}

\textsuperscript{12}In April 1997, the Pew Center asked: “Do you think there is much of a chance that a foreign country could launch a nuclear attack against the United States, or don’t you think there is much of a chance of this?” Fifty-four percent indicated that they thought there was a chance of such an attack.

\textsuperscript{13}The question asked was “These days, do you think the greater threat to America from terrorism comes from people outside this country or from people inside this country?” “Inside” was chosen by 33 percent in April 1995 and rose to 39 percent in March 1996 and 40 percent in April 1997. “Outside” was chosen by 40 percent in April 1995 and rose to 49 percent in March 1996 and 47 percent in April 1997. The percent volunteering “both” fell from 21 percent in April 1995 to nine percent in March 1996 and 11 percent in April 1997. The polls were Los Angeles Times, April 1995; Pew Research Center for the People and the Press, March 1996 and April 1997. See http://www.people-press.org/apr97que.htm.

\textsuperscript{14}The question asked by the Los Angeles Times was: “In the future, do you expect attempts at terrorist acts like the bombing in Oklahoma City will be very common, somewhat common, not too common, or not at all common in this country?” Fifty-one percent said that they thought that it would be very (15 percent) or somewhat (36 percent) common. Los Angeles Times, April 26–27, 1995.

\textsuperscript{15}The question Gallup/CNN/USA Today asked was: “Overall, do you think the United States government is doing enough to prevent terrorism in this country or not?” Gallup/CNN/USA Today, July 29, 1996.
• More than half of those polled in April 1995 and March 1996 felt that antiterrorism laws were too weak.\textsuperscript{16}

• In August 1998, large majorities indicated they were following news reports on government activities to prevent terrorism. A total of 71 percent said that they had followed such reports very closely (33 percent) or fairly closely (38 percent).\textsuperscript{17}

• In August 1998, majorities indicated that they had a sober view of the difficulties in preventing terrorist incidents; when asked how many terrorist incidents officials would be able to prevent if they were given the tools they needed, more than half indicated that they would be able to prevent few or none, and fewer than one in 20 thought that all such attacks could be prevented.\textsuperscript{18}

• In 1999, substantial majorities indicated that reducing the threat of international terrorism should be a “top priority” of the U.S. government.\textsuperscript{19}

The impression one gets from the public opinion data is that the public are concerned about homeland security issues and expect intelligence, law enforcement, and defense officials to engage in the necessary planning and preparations, wherever possible, to prevent

\textsuperscript{16}The question asked was: “Do you think the federal antiterrorism laws currently on the books in this country are too strong, too weak, or about what they need to be?” Asked by the Los Angeles Times in April 1995 and the Pew Research Center for the People and the Press in March 1996. See http://www.people-press.org/terque.htm.

\textsuperscript{17}The question the Pew Center asked was: “(I will read a list of some stories covered by news organizations this past month. As I read each item, tell me if you happened to follow this news story very closely, fairly closely, not too closely, or not at all closely.) . . . Reports about activities to prevent terrorism both here and abroad.” Pew Research Center, August 7, 1998, to September 8, 1998.

\textsuperscript{18}The question the Los Angeles Times asked was: “If law enforcement officials were given the tools they need, do you think they would be able to prevent all future terrorist attacks here in the United States, or many of them, or only a few of them, or would they be able to prevent none of them?” In August 1998, 54 percent said few or none, while 39 percent said all or many; in April 1995, 56 percent said few or none, while 40 percent said all or many. On both occasions, only 4 percent said they thought that law enforcement officials would be able to prevent all attacks.

\textsuperscript{19}Princeton Survey Research Associates asked: “(As I read a list of specific foreign policy problems, tell me whether each one should have top priority in the U.S. (United States) government, a priority but not top priority, or no priority.) How about . . . reducing the threat of international terrorism?” Seventy-five percent accorded the problem top priority. PSRA, March 24–30, 1999.
terrorist acts against the United States. Nevertheless, majorities also have a fairly realistic appraisal of the difficulties of preventing terrorist incidents—fewer than one in 20 believe that all future terrorist attacks could be prevented if law enforcement officials (and, presumably others) were given the tools they need.

**HOMELAND SECURITY TASK AREAS**

Our work suggests that homeland security should include at least five task areas. Three of these task areas emerge from the foregoing analysis:

- WMD domestic preparedness (DP) and civil support, ranging from counterproliferation activities to consequence management of incidents involving high explosives (HE), chemical, biological, radiological, and nuclear weapons.
- Continuity of government (COG), i.e., efforts to reestablish at the earliest possible opportunity civilian political and legal authority following a catastrophic incident.
- Continuity of operations (COOP), including force protection against asymmetric homeland attacks during the fort-to-port sequence, critical infrastructure protection of mission-critical facilities and systems, and other activities.

To be complete, two additional task areas also should be included in homeland security:

- Border and coastal defense, the need for which arises from the possible threat of introduction into the United States of WMD or other weapons capable of mass casualties, and the possibility of large-scale refugee flows that could create national security problems and tax available civilian capacity.²⁰

²⁰A recent historical example of this is the flow of refugees from Haiti prior to the U.S. intervention. Possible future scenarios include refugee flows from Cuba in the event that a peaceful transition to a post-Castro Cuba doesn’t eventuate or instability at the U.S.-Mexican border.
• Although it is not addressed in the present study, national missile defense.21

While overlaps occur among these areas—WMD could be used, for example, against civilian targets, against government targets, or against military mobilization efforts—they collectively seem to capture the essence of the homeland security problem set.

Because at present no agreed-on definition for homeland security exists, the study team developed the following working definition:22

Homeland [security] consists of all military activities aimed at preparing for, protecting against, or managing the consequences of attacks on American soil, including the CONUS and U.S. territories and possessions. It includes all actions to safeguard the populace and its property, critical infrastructure, the government, and the military, its installations, and deploying forces.

While other definitions are certainly possible, the merit of the definition just presented is that it is clear about homeland security’s focus on military activities, as distinct from the activities of civilian organizations, its geographic specificity, and the potential targets it seeks to protect.

CONCLUSIONS

This chapter began with necessary background for understanding the broader context in which homeland security programs are being developed. This discussion included a survey of the constitutional, strategic, and domestic political contexts for homeland security and showed not only that homeland security has deep historical roots but also that the homeland security mission is the fundamental defense mission. All other military activities are predicated on the notion that the nation’s security will be provided for. This analysis also

21 Because this area is heavily studied, we devoted no effort to this area.

22 We recognize that other departments and agencies have important roles to play in many areas related to homeland security. For example, and most notably, the FBI and FEMA play the key roles in crisis and consequence management. However, we reserve the phrase “homeland security” for the tasks performed by the armed services and the Department of Defense.
showed that the issue of the employment of the military in domestic contingencies can be a divisive one—concerns about the role of the military in civil society greatly shapes and constrains the options. The range of threats to the United States—including actions by terrorists or adversary special operations forces, cyber and other attacks on critical infrastructure, computers and communications networks, and large-scale refugee flows—led to an enumeration of the key homeland security task areas and a definition of homeland security.

The next chapter provides an analytic framework or methodology for thinking about Army homeland security roles and responsibilities in the larger setting of local, state, and federal responders.