

DEFENDING the AMERICAN HOMELAND

A Report of The Heritage Foundation Homeland Security Task Force
Chaired by L. Paul Bremer III and Edwin Meese III



THE HERITAGE FOUNDATION
JANUARY 2002

Copyright © 2002 by The Heritage Foundation
ISBN 0-89195-258-6

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202)546-4400
www.heritage.org

Cover image copyright © 2000 by Eyewire
Cover design by Mark Hurlburt
Map and table design by Harris Byers and Dexter Ingram

TABLE OF CONTENTS

The Heritage Foundation Homeland Security Task Force.....	v
Preface.....	ix
Executive Summary	1
Chapter	
1: Top Priorities for Protecting the Nation’s Infrastructure.....	11
2: Top Priorities for Strengthening Civil Defense Against Terrorism..	31
3: Top Priorities for Improving Intelligence and Law Enforcement....	53
4: Top Priorities for Military Operations to Combat Terrorism	75
Appendix	
Table A-1: Status of Anti-Terrorism Actions by the Executive Branch..	92
Table A-2: Status of Anti-Terrorism Legislation	93
Selected Bibliography	97

THE HERITAGE FOUNDATION

HOMELAND SECURITY TASK FORCE

CHAIRMEN

Ambassador L. Paul Bremer III, Chairman and CEO, Marsh Crisis Consulting;
Chairman, National Commission on Terrorism, Reagan Administration;
former Ambassador at Large for Counterterrorism, U.S. Department of State

The Honorable Edwin Meese III, Ronald Reagan Distinguished Fellow in Public
Policy and Chairman, Center for Legal and Judicial Studies, The Heritage
Foundation; Attorney General in the Reagan Administration

PROJECT DIRECTOR

Kim R. Holmes, Ph.D., Vice President, The Heritage Foundation; Director,
The Kathryn and Shelby Cullom Davis Institute for International Studies, The
Heritage Foundation; member, Defense Policy Board, U.S. Department of Defense

WORKING GROUP ON INFRASTRUCTURE PROTECTION AND INTERNAL SECURITY

Rapporteur: Michael Scardaville, Policy Analyst in Homeland Defense,
The Kathryn and Shelby Cullom Davis Institute for International Studies,
The Heritage Foundation

The Honorable Carol Hallett, President and CEO, Air Transport Association;
former Commissioner, U.S. Customs Service

The Honorable Frank Keating, Governor of Oklahoma

Jules McNeff, Director, U.S. GPS Industry Council, with Science Applications
International Corporation (SAIC)

Colonel Joseph Muckerman, USA (Ret.); former Director of Emergency
Management, Office of the Secretary of Defense; former faculty member,
Army War College and National Defense University

Captain Bruce Stubbs, USCG (Ret.); Technical Director, Theater Air Defense, Systems Engineering Group, Anteon Corporation

Thomas L. Varney, Director of Technology Assurance and Security, McDonald's Corporation

The Honorable Pete Wilson, former Governor of California

WORKING GROUP ON CIVIL DEFENSE AGAINST WEAPONS OF MASS DESTRUCTION

Rapporteur: Jack Spencer, Policy Analyst in Defense and National Security, The Kathryn and Shelby Cullom Davis Institute for International Studies, The Heritage Foundation

Albert Ashwood, Director, Oklahoma Emergency Management

Dr. Daniel Dire, Department of Emergency Medicine, University of Alabama

Dr. Daniel Goure, Senior Fellow, Lexington Institute

Dr. Fred Iklé, Distinguished Scholar, Center for Strategic and International Studies

Colonel Joseph Muckerman, USA (Ret.); former Director of Emergency Management, Office of the Secretary of Defense; former faculty member, Army War College and National Defense University

Michelle White, Counsel, Subcommittee on Economic Development, Public Buildings, and Emergency Management, Committee on Transportation and Infrastructure, U.S. House of Representatives

WORKING GROUP ON INTELLIGENCE AND LAW ENFORCEMENT

Rapporteur: Daniel W. Fisk, Deputy Director, The Kathryn and Shelby Cullom Davis Institute for International Studies, The Heritage Foundation

Louis Dupart, Esq., partner, Fleischman & Walsh, Washington, D.C.; former Deputy Assistant Secretary of Defense, International Security Affairs, U.S. Department of Defense; former Chief Counsel, Permanent Select Committee on Intelligence, U.S. House of Representatives

Carmel Fisk, former Minority Counsel, Subcommittee on International Law, Immigration, and Refugees, Committee on the Judiciary, U.S. House of

Representatives; former Assistant District Counsel, Immigration and Naturalization Service

Thomas Frazier, President, The Frazier Group, Baltimore, Maryland; former Chief of Police, Baltimore, Maryland; former Director, Community Oriented Policing Services Program, U.S. Department of Justice

Major General Bob Harding, USA (Ret.); Executive Vice President for Operations, Innovative Logistics Techniques, Inc., McLean, Va.; former Director of Operations, Defense Intelligence Agency; former Assistant Deputy Chief of Staff of Intelligence, U.S. Army

Alvin James, Anti Money-Laundering Practice Leader, Ernst and Young; former Senior Anti Money-Laundering Policy Adviser, FinCEN, U.S. Department of the Treasury

Dr. Mark M. Lowenthal, SRA International, Inc.; former Staff Director, Permanent Select Committee on Intelligence, U.S. House of Representatives

N. John MacGaffin III, President, MacGaffin & Miller, Inc., Washington, D.C.; former Assistant Deputy Director for Operations, U.S. Central Intelligence Agency

Ambassador David C. Miller, Jr., Chairman, MacGaffin & Miller, Inc., Washington, D.C.; former Special Assistant to the President and Senior Director for International Programs, National Security Council

Dr. William J. Olson, Minority Staff Director, International Narcotics Control Caucus, U.S. Senate; former Deputy Assistant Secretary of State, International Narcotics Matters

The Honorable Robert S. Warshaw, Warshaw & Associates, Sylva, North Carolina; former Chief of Police, Rochester, New York; former Associate Director, Office of National Drug Control Policy, State and Local Affairs

WORKING GROUP ON MILITARY OPERATIONS

Rapporteur: Larry M. Wortzel, Ph.D., Director, Asian Studies Center, The Heritage Foundation

David Davis, Chief of Staff, Office of Senator Kay Bailey Hutchison

Colonel James P. Gibbons, USA (Ret.); former Commander, U.S. Army Land Information Warfare Activity

Major General David L. Grange, USA (Ret.), Executive Vice President, Robert R. McCormick Tribune Foundation; former Commander, First Infantry Division;

former Director and Deputy Director of Current Operations, U.S. Army; former Deputy Commander, Delta Force; and former Ranger Regiment Commander.

Lieutenant General Patrick M. Hughes, USA (Ret.); former Director, Defense Intelligence Agency; former Deputy Chief of Staff for Intelligence, U.S. Army

Dr. Fred Iklé, Distinguished Scholar, Center for Strategic and International Studies

General Carl E. Mundy, Jr., USMC (Ret.); former Commandant, United States Marine Corps; former member, Joint Chiefs of Staff

General John H. Tilelli, Jr., USA (Ret.); former Commander, U.S. Army Forces Command, Vice Chief of Staff, United States Army, and Commander in Chief, U.S. Forces Korea

General Charles R. Wilhelm, USMC (Ret.); former Commander, U.S. Southern Command

Members listed here have endorsed the reports of their specific working groups and have not reviewed the other reports. Other contributors to the project are noted in each chapter.

PREFACE

The terrorist attacks of September 11 struck at the very heart of the American homeland. By intentionally targeting civilians in major U.S. cities, the terrorists were sending a signal: Their war against America would no longer be confined to such overseas targets as embassies, or to U.S. servicemen on ships like the U.S.S. *Cole*. Instead, they would take their war to America's heartland, killing as many innocent civilians as they could with any means at their disposal—first to change U.S. policy, and ultimately to destroy American and Western civilization. It was a new form of total war in the age of terrorism, and it put all Americans on notice that the United States is dangerously vulnerable and that new means are urgently needed to strengthen the security of the homeland.

The Heritage Foundation Homeland Security Task Force was formed days after the September 11 attacks to meet this urgent need. Comprised of some of the best homeland security experts in the world, the Task Force was asked to make specific proposals on how best to eliminate the vulnerabilities exposed on September 11.

The Task Force was co-chaired by two veteran policymakers regarding terrorism and homeland security: former Attorney General Edwin Meese III and L. Paul Bremer, Chairman of the National Commission on Terrorism and Ambassador at Large for Counterterrorism under President Ronald Reagan. They and their fellow Task Force members have reviewed a vast number of ideas and proposals already put forth on homeland security and have developed a set of priority recommendations to prevent and respond effectively to limit the repercussions of another terrorist attack on the American homeland. The conclusions and recommendations in each chapter reflect those of these Working Group members, and not necessarily of those who also were consulted on portions of each chapter.

Ever mindful of past studies on this important issue, the Task Force members reviewed and critiqued the findings of the reports of previous commissions on which some of them had worked, such as the U.S. Commission on National Security/21st Century (the Hart–Rudman Commission) and the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (the Gilmore Commission). However, the main purpose of each Working Group was to move beyond these studies to provide new ideas and proposals that would effectively address the problems identified by the September 11 attacks.

The Working Groups determined that there was no need for a general description of the threat or a lengthy justification for the need to make homeland security a higher national priority; this has been a major purpose of several other homeland security studies, and the September attacks merely made that threat and national priority self-evident. Rather, they saw a need to develop priorities for action and how to implement and make operational the recommendations to the executive branch of the Federal government, to Congress, and to State and Local governments.

The Task Force members always remained cognizant that the Administration and Congress have worked intently on improving homeland security since September 11. Every attempt has been made to incorporate any new policies and laws implemented by the Federal government since this Task Force was convened.

With these requirements in mind, the chairmen of The Heritage Foundation Homeland Security Task Force established four Working Groups to address specific areas identified by the September 11 attacks as needing priority action. These are:

- **Infrastructure Protection and Internal Security**, to make recommendations to better coordinate planning and consequence management among Federal, State, and Local agencies; to improve airport and seaport security; to protect vital space assets for the nation's telecommunications system; to enhance the private sector's role in infrastructure protection; and to secure Federal networks and information systems.
- **Civil Defense Against Weapons of Mass Destruction**, to advise the government on how to improve the coordination of Federal agencies in planning and responding to a chemical, biological, radiologic, or nuclear (CBRN) attack on the homeland; to better plan for the early detection of such an attack; to enhance planning by Local and State authorities as the "first responders" to attacks; to facilitate the production of new vaccines and pharmaceuticals against the toxic agents sought by terrorists; to improve international cooperation for planning for and consequence management in the event of an attack; and to develop public education and public relations programs for civil defense.
- **Intelligence and Law Enforcement**, to make proposals to improve threat assessments and planning by the Office of Homeland Security; to enhance intelligence gathering, analysis, and sharing among all levels of government; to strengthen the visa approval process and border security mechanisms; to eliminate theft and fraud in state identity documents systems; and to create new mechanisms to monitor and obstruct money laundering that supports terrorist activities.

- **Military Operations to Counter Terrorism**, to advise the U.S. Department of Defense on how best to boost port security and homeland security with the National Guard and Reserves; to protect critical infrastructure with air defense and missile defense; to enhance rear-area operations to protect against terrorist attack; to provide better intelligence support for military operations; and to ensure clear command and control over overseas anti-terrorism operations.

In devising these recommendations, the Task Force focused on specific steps that could be implemented by the executive branch agencies, by Congress, or by Local and State authorities. The intention was to provide policymakers with ready-made ideas that can be acted on immediately or in short order to solve the most urgent problems facing the nation and homeland security.

Another important task was to identify key recommendations in other homeland security studies that remain unimplemented. The Task Force reviewed these recommendations and reached a consensus on the ones that deserve urgent attention by government. These are listed at the end of each chapter. Also provided in this report is an inventory of the major legislative proposals and initiatives since the September 11 attacks. Past executive orders and presidential directives relating to terrorism and homeland security are also listed in the Appendix to give the reader a fuller appreciation of what other Administrations have already done.

Defending the American Homeland: A Report of The Heritage Foundation Homeland Security Task Force is part of a series of studies and activities in The Heritage Foundation's Homeland Security Project. This project reflects the urgent priority placed on the issue of homeland defense by The Heritage Foundation, which has worked diligently on one facet of this issue—ballistic missile defense—for many years. The Homeland Security Project reflects Heritage's dedication to building an America where freedom, opportunity, prosperity, and civil society can flourish.

On behalf of my colleagues at The Heritage Foundation, I would like to thank the members of the Homeland Security Task Force for participating in this study. They volunteered their valuable time and expertise to a project that was completed in a very short period of time and under a very tight schedule. We greatly appreciate their contributions and their patience.

I would also like to thank Edwin Meese and Jerry Bremer for co-chairing the Task Force and for providing their outstanding leadership, guidance, and expertise to this project. Their steady hands and vast experience were invaluable to the quality and relevance of the report.

Thanks also go to my colleagues at The Heritage Foundation who worked on this report. Especially appreciated are the rapporteurs who managed the four Working Groups and wrote the drafts of their chapters: Michael Scardaville, Policy Analyst for

Homeland Security, and Jack Spencer, Policy Analyst for National Security Affairs, in the Kathryn and Shelby Cullom Davis Institute for International Studies; Daniel W. Fisk, Deputy Director of the Kathryn and Shelby Cullom Davis Institute for International Studies; and Larry M. Wortzel, Director of the Asian Studies Center at The Heritage Foundation.

A special word of thanks goes as well to Heritage's Managing Editor, Janice A. Smith, who tirelessly and skillfully edited the entire report. Thanks, too, to Senior Editor Richard Odermatt and Senior Copyeditor William T. Poole for their fine attention to detail. I also owe a word of appreciation to Melissa Glass, Research Assistant for the Homeland Security Project, for her help in researching and managing the project, and to Anne C. Gartland, acting Director of Publishing Services, for shepherding this project through design, layout, and printing.

Finally, I wish to acknowledge these Heritage staff members for their assistance in the production of this report: Research Assistants Carrie Satterlie and Paolo Pasicolan, and Paul Skoczylas, Assistant to the Vice President of Government Relations, and intern Galereh Karimi; Dexter Ingram, Database Editor in the Center for Data Analysis, who generated the possible effects of various CBRN attacks illustrated in the maps; Harris Byers, Graphic Design Specialist, for his work on the maps, tables, and charts; Mark Hurlburt, Design Layout Specialist, for the report's cover design and layout; and Daryl Malloy, Copyeditor, for his efforts to keep the report on schedule.

Kim R. Holmes, Ph.D.
Director
The Heritage Foundation Homeland Security Project

EXECUTIVE SUMMARY

Few events have so crystallized the threat of terrorism that America's enemies pose to its people, its international stature, and its very civilization as have the attacks of September 11. America is dangerously vulnerable to this new form of terrorism. New means are needed to rapidly strengthen the security of the American homeland—to protect critical infrastructure, boost civil defense, and increase intelligence and military structures in order to prevent future attacks and limit the effects should one occur.

Many steps already have been taken by the Administration and Congress, such as creating the Office of Homeland Security and appointing former Pennsylvania Governor Tom Ridge to direct it as Assistant to the President for Homeland Security. But much more needs to be done.

The Heritage Foundation Homeland Security Task Force, formed shortly after the September 11 attacks with some of the best homeland security experts in the world, sought to address this need by reviewing the vast number of proposals put forth by commissions and legislative initiatives. Its members agreed unanimously that there no longer was a need to describe the threat to the homeland or to justify making homeland security a higher national priority. Rather, they saw a need to develop top priorities for action at all levels of government and to devise concrete steps to implement these priorities and make them operational. Their recommendations for action are as follows.

PROTECTING THE NATION'S INFRASTRUCTURE

Most Americans recognize that protecting critical infrastructure from acts of terrorism is a responsibility that does not rest with any one level of government. Structural, cultural, institutional, and statutory changes are needed to secure the nation's critical infrastructure so that terrorists have less incentive to target them and the nation can respond quickly if they do. The success of efforts to defend and protect infrastructure will rest primarily on the ability of Federal, State, and Local governments to communicate and cooperate effectively with each other and with the private sector.

To protect America's critical infrastructure, such as communication networks, utilities and water supplies, banking and finance systems, transportation nodes, and

intelligence systems, the Working Group on Infrastructure Protection and Internal Security has established the following top priorities for Federal, State, and Local efforts.

- **Priority #1: Reorganize by presidential directive all Federal agencies involved in protecting critical infrastructure.** The President should reorganize the Federal government to enhance its ability to protect the homeland. President Bill Clinton issued an infrastructure protection directive, known as PDD-63, to assign responsibility for addressing the security of 12 specific infrastructure sectors to various Federal agencies. However, his directive failed to create a system of oversight or establish a clear chain of command to ensure that agency efforts were adequately enhancing the security of these sectors. The new presidential directive should correct this deficiency by requiring annual assessments of Federal agency efforts; clarifying the chain of command for infrastructure protection efforts that involve Congress, State and Local entities, as well as the private sector; and improving coordination and information sharing.
- **Priority #2: Designate the Global Positioning System (GPS) frequencies and network as critical national infrastructure.** The GPS satellite network is an enabling system for other infrastructure systems, such as telecommunications, that are vital to the nation's security. Disruption by terrorist groups or hostile states could jeopardize America's homeland security, but the GPS has not been designated as a vital national asset. President George W. Bush should immediately add the GPS to the current list of vital national infrastructure and assign responsibility for its security to the U.S. Department of Defense (DOD). Immediate steps should begin to make the GPS network more secure.
- **Priority #3: Facilitate communication on infrastructure issues between the new Office of Homeland Security (OHS) and State and Local officials.** State and Local governments play a vital role in protecting the infrastructure within their jurisdictions. In the event of a possible terrorist attack, however, they cannot do so effectively without communications from the Federal government. Before such communications—which could include classified information—can occur, many States will need to reform their public meeting disclosure laws so that information concerning suspected terrorist activities and vulnerable infrastructure will not be made public and compromise prevention, apprehension, and deterrence. Appropriate response exercises that include the relevant Federal, State, and Local officials should be conducted for various attack scenarios, which will enable better communications should an attack occur.
- **Priority #4: Enhance the private sector's role in infrastructure protection.** Market forces provide a strong incentive for the private sector to protect any infrastructure it owns and operates. Government should not inhibit industry

efforts to do so, and it should ensure that businesses have the tools they need to increase their ability to protect vital infrastructure, such as telecommunication networks. Congress should remove any legislative roadblocks that exist to improved communications with the private sector, and tax penalties that make it more difficult for private industry to invest in greater security should be eliminated. Moreover, new security standards for protecting each type of infrastructure and new risk assessment programs should be developed and shared with the relevant businesses.

- **Priority #5: Institute new rules to monitor more closely who or what is entering America's airports and seaports.** Since September 11, new efforts to increase security at vital transportation nodes have focused primarily on manpower, such as federalizing baggage handlers at airports. A comprehensive program to increase airport and seaport security requires tighter controls on who and what is passing through America's portals. New Federal systems should be developed to share passenger information that would help prevent a potential terrorist from even boarding a plane. A Federal interagency center also will be needed to analyze information about the people and products entering the United States by sea. The U.S. Customs Service should begin experimenting with a point-of-origin inspection program for maritime trade. The Sea Marshals program should be expanded quickly. And the Transportation Security Agency should issue a new regulation to require airports and port administrations to assure that only authorized people can enter secure areas.
- **Priority #6: Secure all Federal networks and information systems.** The U.S. General Accounting Office has reported that the information systems vital to Federal operations are not sufficiently protected. Without tighter security, continuity of operations cannot be guaranteed. Federal agency technology-purchasing guidelines should be revised to place a premium on security. The executive branch also should explore alternatives to the proposed government-only Internet system (GOVNET) before making a procurement decision.
- **Priority #7: Accelerate government compliance with the Nuclear Waste Policy Act.** Despite legislation requiring that it do so, the U.S. Department of Energy (DOE) has not uniformly secured the nation's nuclear waste, which could be used by terrorists to build radiologic weapons. According to the department, it is already running 12 years behind schedule. Congress should hold hearings to determine how DOE can bring the new storage facility at Yucca Mountain, Nevada, on-line more quickly and improve security.

STRENGTHENING CIVIL DEFENSE AGAINST TERRORISM

Unlike defending the nation from military attacks, civil defense begins with preparation and planning at the local level. The first responders to an emergency are usually local emergency workers and volunteers—a fact poignantly illustrated on September 11. Should terrorism occur again in the United States, America’s firefighters, law enforcement officials, emergency medical services personnel, health professionals, and hazardous materials crews will be the front-line fighters. However, they are not adequately prepared today to respond to or prevent a terrorist attack using weapons of mass destruction.

To assist Local, State, and Federal officials in improving their ability to detect and respond to an attack on civilians using chemical, biological, radiologic, or nuclear (CBRN) agents, the Working Group on Civil Defense Against Weapons of Mass Destruction has established the following top priorities.

- **Priority #1: Build a nationwide surveillance network for early detection of chemical, biological, or other attacks.** In order to mobilize a rapid response to such attacks, government officials must be able to recognize the initial stages of an outbreak of catastrophic illness or attacks on food and water supplies. This requires a nationwide network of locally based surveillance procedures and systems to monitor these vital sectors, and nationally developed monitoring standards and reporting guidelines so that information can be disseminated quickly. The Federal government should also take steps to foster the development of more sensitive monitoring technologies.
- **Priority #2: Develop a terrorism response checklist and a manual of civil defense exercises to guide officials in assessing preparedness.** Local and State authorities must prioritize the elements of any effort to improve the ability to respond to a CBRN event. The Federal government should assist the states by developing national standards of preparedness and by designing new evaluation tools to help them assess their own weaknesses and to determine how best to proceed. The guides, developed by a task force under the direction of the OHS, should be completed within the next six months and made available on the Web site of the Centers for Disease Control and Prevention (CDC). In addition, the Federal government should conduct CBRN response exercises, first with states most at risk of terrorism and building gradually to multi-state exercises over time.
- **Priority #3: Accelerate the development of pharmaceuticals that prevent or limit the spread of toxic agents by terrorists.** Given the urgency of protecting Americans from biological terrorism, which followed the recent anthrax deaths, the Federal government should facilitate more rapid development and supply of new and safer vaccines, drugs, and other medicines that would

provide immunity to such diseases as smallpox or that would limit the effects of an outbreak after a terrorist incident. This will involve establishing reasonable requests for proposals for developing CBRN-related pharmaceuticals; guaranteeing patent protection for products related to terrorism; improving the fast-track approval process for these products; and stimulating the development of generic drugs after patents have expired.

- **Priority #4: Create a national web of CBRN experts who will train first-response teams for an outbreak or terrorist attack.** A program that can identify these experts and deploy them in teams to share their expertise and train local first responders would be an affordable and effective way to prepare for a CBRN attack. Congress should provide adequate funding for expanding the Train-the-Trainer programs in the Office for Domestic Preparedness.
- **Priority #5: Simplify the process of obtaining Federal assistance for civil defense initiatives.** An OHS block grant program should be established so that State and Local authorities can target federal funding to their unique civil defense needs. Current agency grant programs should be streamlined into a single grant application process administered by the OHS. To ensure that federal funds get to the localities that need them the most to boost preparedness, a new homeland security block grant program also should be established under the Federal Emergency Management Agency (FEMA). All grants should be conditional, non-transferable, and made accountable through new reporting requirements.
- **Priority #6: Sign mutual support agreements with Canada and Mexico on responses to terrorist acts in border communities.** The possibility exists that a terrorist could release a biological or radiologic attack on the United States without ever crossing the border, with serious consequences for people in both countries. The United States should sign mutual terrorism support agreements with Canada and Mexico on preventing such attacks and managing their consequences should they occur.
- **Priority #7: Develop a nationwide education and public relations program.** In a democracy, governments at all levels must mitigate fears of attack while building support for their efforts to protect the public. Public relations campaigns can be vital to preventing panic, improving civil defense preparedness and responses, and maximizing all efforts to prevent terrorism. Successful campaigns will require a terrorism-related public relations strategy for improving cooperation with local media to enhance the dissemination of information to the public.

IMPROVING INTELLIGENCE AND LAW ENFORCEMENT CAPABILITIES

Since September 11, many are questioning the ability of government agencies to gather and communicate actionable intelligence to enable them to apprehend terrorists before they strike and to deter them in the future. Federal, State, and Local officials recognize that more resources must be focused on improving intelligence so that government agencies, emergency personnel, and first responders can more effectively respond to those who would harm American civilians.

The capabilities of and relationships between law enforcement agencies (LEAs) at the Federal, State, and Local levels and the Intelligence Community have received comprehensive reviews, such as in hearings before the House Permanent Select Committee on Intelligence and in its 1995 report, *Intelligence Community in the 21st Century*; by the 1996 Brown–Rudman Commission; and in more recent reviews by the Hart–Rudman, Bremer, and Gilmore Commissions. Many of the excellent recommendations made by these commissions and studies have yet to be fully implemented.

September 11 sent a powerful message to decision-makers that much more needs to be done to protect the homeland, and quickly. The Administration and Congress have sought to address some of the bureaucratic problems exposed by the attacks by passing the USA PATRIOT Act (P.L. 107–56) and the FY 2002 Intelligence Authorization Act (H.R. 2883). They recognize that no single action, law, or institution—no one-step remedy—will combat all of the threats the United States and its citizens face.

A multifaceted approach to homeland security is necessary. Building on the recommendations of earlier commissions and post-September 11 legislative efforts, the Working Group on Intelligence and Law Enforcement has identified the following top priorities for improving the ability of law enforcement agencies and the Intelligence Community to protect the homeland.

- **Priority #1: Require the Office of Homeland Security to direct the assessment of threats to critical assets nationwide.** The first important step in homeland defense is providing appropriate information to government officials to help them determine what assets, critical to the nation's economy and security, remain vulnerable to terrorist attack and whether the responsible agencies and institutions are organized and equipped sufficiently to protect them. A first step in this process must be the development by the OHS of a uniform methodology for assessing the risk to possible targets and the level of threat to those targets, and establishing the methods for sharing the findings. Based on the compiled assessments, the OHS Director should establish a

national strategy for protecting the homeland and direct his office to develop a national alert and warning system.

- **Priority #2: Rapidly improve information-gathering capabilities at all levels of government.** For Federal, State, and Local law enforcement officials, a first line of defense against terrorism and other threats to the homeland is access to timely, reliable, and actionable information from both foreign and domestic sources. Rapidly enhancing government's ability to acquire and analyze this information is vital to homeland security. The President should direct the Director of OHS to establish a national intelligence coordinating group whose task is to develop a national strategy for gathering and sharing intelligence. More federal resources should be targeted to strengthening foreign intelligence-collection capabilities, as well as domestic sources of information critical to homeland defense. This includes strengthening the measurement and signature intelligence (MASINT) capabilities of the Intelligence Community and maximizing current agency capabilities to cross-cue intelligence and increase human intelligence (HUMINT).
- **Priority #3: Improve intelligence and information sharing among all levels of government with homeland security responsibilities.** The need for better sharing and dissemination of acquired information to all levels of government became clearer in the days following September 11, but improving LEA–Intelligence Community cooperation will have far more to do with changing bureaucratic cultures that resist change than with revising current statutes or regulations. The President should direct the appropriate Cabinet Secretaries and officials to work together to create an all-source Federal-level information fusion center, to which all intelligence information goes and from which it is disseminated on a need-to-know basis. The OHS Director should develop a cooperative structure for the sharing and disseminating of this information, which will include classified information. Federal funding and training should be targeted to assist State and Local LEA information-gathering efforts.
- **Priority #4: Strengthen the visa approval and border security mechanisms.** Legally entering the United States was remarkably easy for the September 11 terrorists. America's visa approval and entry–exit processes, and the ability of LEAs to enforce existing immigration laws against aliens who are in violation of those or other laws, should be strengthened. Consular officers need more information upon which to make their decision about granting each visa. A Federal-level lookout database should be created and made accessible to officials involved in border security. The “45-minute” rule that requires Immigration and Naturalization Service (INS) inspectors to clear all passengers on international flights into the United States within that time period should be repealed. The Visa Waiver Program law should be amended to allow the

Secretary of State to use it to encourage countries to institute greater anti-terrorism border control mechanisms. The U.S. government should expedite the development of tamper-proof travel documents, explore the development of an exit monitoring mechanism, strengthen INS's ability to enforce the law against aliens who violate their visas, institute comprehensive procedures for handling immigration cases that involve classified documents, and help State and Local LEAs develop a standard format for "rap sheets."

- **Priority #5: Eliminate the opportunities for identity theft and fraud in state identity document systems.** False identity documents are a major problem, and the terrorists involved in the September 11 attacks exploited the States that have the systems most liable to fraud. Any State that continues to run a document system subject to fraud and abuse must recognize that it is placing the lives of Americans in jeopardy. Current procedures for the issuance and recording of identity documents, such as driver's licenses and birth and death certificates, must be tightened and a mechanism developed to deter and prevent identity theft. Development of tamper-proof documents should be a priority.
- **Priority #6: Create a mechanism to monitor recent anti-money-laundering initiatives to obstruct the financing of terrorism.** Many of the deficiencies of efforts before September 11 to obstruct the financing of terrorist activities were addressed in the USA PATRIOT Act, but the financial services area is dynamic, and those who seek to harm the United States will continue to attempt to circumvent the current regulatory structures. To better anticipate how existing anti-money-laundering restrictions can be circumvented, the Secretary of the Treasury should create a mechanism to evaluate the current laws.

MILITARY OPERATIONS TO COMBAT TERRORISM

The 1997 National Defense Panel (NDP) report is but one of many that gave clear warnings to the people and policymakers that the United States homeland was at risk of terrorist attack. Other studies made it clear that the U.S. armed forces must be prepared not only to identify impending catastrophic terrorist attacks, but also to preempt or respond to them rapidly, working with the Intelligence Community and Federal, State, and Local officials.

In any restructuring of the forces to meet a rising threat, care must be taken to ensure a continued balance between unconventional and conventional force capabilities. A number of studies have suggested how to accomplish these objectives, but their recommendations have not been systematically implemented.

The Heritage Foundation Working Group on Military Operations has attempted to address this problem by identifying the following top priorities for improving military anti-terrorism operations to defend the homeland.

- **Priority #1: Free the National Guard and Reserves for homeland security and boost port security quickly.** Homeland security will require enhancing the capabilities of National Guard and Reserve units to respond to terrorist events. This means freeing some of these units from having to provide combat support and combat service support for the active forces by adding more active duty personnel to current force levels. It means ensuring that the National Guard has standing emergency plans to train and work with Local authorities on homeland defense and consequence management. It will require the development of coordinated public information campaigns. It also will require reinstating a U.S. Navy–U.S. Coast Guard coordinated port security program to check all incoming ships and containers to prevent weapons of mass destruction from entering the United States.
- **Priority #2: Protect U.S. borders, coasts, and critical national infrastructure with air defense and missile defense.** The threat of attack by aircraft, cruise missiles, and ballistic missiles requires that the United States establish a robust air and cruise missile defense system and begin testing ballistic missile defenses on land and at sea at full design capability. Congress should provide additional funding for the deployment of a cruise missile defense system as a component of homeland defense. And the Pentagon should deploy air defense and cruise missile defense systems to defend major U.S. cities and critical infrastructure.
- **Priority #3: Enhance rear-area military operations to protect the homeland and prepare for terrorist attacks.** The U.S. military can assist Local, State, and Federal authorities in counterterrorism efforts by identifying critical infrastructure nodes; assessing their security levels; providing protection for them as needed as well as redundant communications, command, and control systems; and procuring and maintaining equipment to assist in the local responses to terrorist attacks. To achieve this goal, the commander in chief (CINC) for homeland defense should be the Joint Forces Command CINC. The Secretary of Defense should develop a refined list of military responses to domestic terrorist attacks and a network of interactive command-and-control centers and service mobilization directorates to enable better coordination with Federal and State agencies. The service branches should provide training to the National Guard, FEMA, and other appropriate Federal and State agencies on incident response and mitigation. And all components of the Joint Forces Command should be enabled to task units to respond to incidents around the entire country.

- **Priority #4: Provide intelligence support for military operations.** Effective military operations depend on timely and accurate intelligence about enemy forces, movements, capabilities, and intentions. Real-time, all-source intelligence fusion centers are required for effective counterterrorism military operations and homeland defense. Several of the September 11 terrorists were on different government watch lists, but these databases were not linked for common retrieval of information. To protect the homeland, the U.S. Department of Defense should institute local, low-level counterintelligence source operations for force protection near military installations. To give DOD access to cross-referenced strategic and critical databases, which are currently housed in various Federal agencies, will require establishing fusion centers at the Federal, State, and Local levels (where necessary) and staffing them with personnel who have appropriate clearances for classified information.
- **Priority #5: Ensure clear command and control of overseas anti-terrorism operations.** Regardless of whether military operations are of an offensive or defensive nature, the geographic Unified Command (such as PACOM, or CENTCOM, which is directing the war in Afghanistan) must be the command-and-control headquarters for overseas military operations. In military parlance, this means that the geographic Unified Command will be the supported command and the war fighter. The United States Special Operations Command (SOCOM) should be the primary force provider (supporting commander in chief or CINC), not the major war fighter, and the specified supporting command for managing counterterrorism operations. The Secretary of Defense should ensure that SOCOM has the authority and resources it needs to carry out this mission. The CINC for homeland defense should prepare pre-planned force packages for initiating rapid responses to terrorism contingencies.

TOP PRIORITIES FOR PROTECTING THE NATION'S INFRASTRUCTURE

A Report of the Working Group on Infrastructure Protection and Internal Security¹

Michael Scardaville, Working Group Rapporteur

The aftermath of the September 11, 2001, attacks on the Pentagon and the World Trade Center illustrates the high vulnerability of America's infrastructure to terrorist attacks and the massive consequences of not protecting it. While the terrorists were able to utilize deficiencies in America's overall approach to intelligence sharing and aviation security, similar vulnerabilities exist in every infrastructure vital to the security, economy, and survival of the nation, such as computer networks, energy supplies, transportation, and the global positioning satellite system.

Today, most Americans recognize that responsibility for protecting critical infrastructure from terrorism does not rest with any one level of government. Structural, cultural, institutional, and statutory changes are needed to secure the nation's infrastructure so that terrorists have less incentive to attack them and the nation can respond quickly if they do. Primarily, the success of efforts to defend and protect

-
1. The members of the Working Group on Infrastructure Protection and Internal Security are The Honorable Carol Hallett, President and CEO of the Air Transport Association; The Honorable Frank Keating, Governor of Oklahoma; Jules McNeff, Director, U.S. GPS Industry Council, with SAIC; Col. Joseph Muckerman, USA (Ret.), former Director of Emergency Management, Office of the Secretary of Defense; Captain Bruce Stubbs, USCG (Ret.), Technical Director, Theater Air Defense, Systems Engineering Group, Anteon Corporation; Thomas L. Varney, Director of Technology Assurance and Security, McDonald's Corporation; and The Honorable Pete Wilson, former Governor of California. The following individuals contributed to this report in an advisory capacity: Dr. Billy Cook, MTS Technologies, Inc.; Richard J. Doubrava, Managing Director, Security, Air Transport Association; Rob Houseman, Counsel, Bracewell and Patterson; John M. Meenan, Senior Vice President, Industry Policy, Air Transport Association; Edward A. Merlis, Senior Vice President, Legislative and International Affairs, Air Transport Association; Robert W. Poole, Jr., Director of Transportation Studies, Reason Public Policy Institute; John Powers, Executive Director, President's Commission on Critical Infrastructure Protection; Kenneth P. Quinn, Partner, Pillsbury Winthrop LLP; Scott Rayder, Director of Government Relations, Consortium for Ocean Research; Maureen Sirhal, reporter, *Technology Daily*; and Gary Tyler, Director, Matcom Corporation.

infrastructure will rest on the ability of Federal, State, and Local governments to cooperate with each other and the private sector.

In this regard, the Working Group on Infrastructure Protection and Internal Security reviewed various commission reports and government studies² and developed a list of top new priorities for protecting America's critical infrastructure in the near term. The following priorities (1) represent new approaches to protecting the nation's infrastructure and (2), if implemented, will enhance Federal, State, and Local efforts.

- **Priority #1: Reorganize by presidential directive all Federal agencies involved in protecting infrastructure.** The President should issue a new directive to reorganize the federal government to enhance its effectiveness in protecting the American homeland. The new National Security Presidential Directive (NSPD) should correct the failure of President Bill Clinton's directive, PDD-63, to create a system of oversight and establish a clear chain of command for protecting infrastructure. PDD-63 merely assigned responsibilities for addressing the security of 12 nationally important infrastructure sectors to various Federal agencies.
- **Priority #2: Designate the Global Positioning System (GPS) frequencies and network as critical national infrastructure.** The GPS satellite network is now an enabling system for other vital infrastructure, such as telecommunications, yet it has not been designated as a vital asset. It should be added to the current list of vital national infrastructure, and responsibility for ensuring its security should reside with the U.S. Department of Defense.
- **Priority #3: Facilitate communication on infrastructure issues between the new Office of Homeland Security (OHS) and State and Local officials.** State and Local governments play a vital role in protecting infrastructure within their jurisdictions, but they cannot do so without effective communication with the Federal government.
- **Priority #4: Enhance the private sector's role in infrastructure protection.** Market forces provide a strong incentive for the private sector to protect infrastructure that it owns and operates; government should ensure both that it does not inhibit an industry's efforts to do so and that business has the tools it needs for that protection.
- **Priority #5: Institute new rules to monitor more closely who or what is entering America's airports and seaports.** Since September 11, new efforts to increase security at these vital transportation nodes have focused largely on

2. For a summary of recommendations from prior commissions and studies that remain unimplemented, see the table at the end of this chapter. The status of post-September 11 legislative efforts may be found in the Appendix.

manpower concerns, such as federalizing baggage handlers. However, a comprehensive program for airport and seaport security requires that tighter controls must be implemented to monitor who and what passes through them.

- **Priority #6: Secure all Federal networks and information systems.** The U.S. General Accounting Office has reported that information systems vital to Federal operations are not being sufficiently protected. Without tighter security, Federal networks cannot guarantee continuity of operations. Federal agencies' technology purchasing guidelines must be revised to place a premium on security. The Administration should also explore how to make Internet-based networks more secure, in addition to solutions that would rely on a federal government intranet separate from the Internet (GOVNET).
- **Priority #7: Accelerate government compliance with the Nuclear Waste Policy Act.** Despite legislation requiring it to do so, the U.S. Department of Energy has not uniformly secured the nation's nuclear waste, which could be used by terrorists to build radiologic weapons.

PRIORITY #1: REORGANIZE BY PRESIDENTIAL DIRECTIVE ALL FEDERAL AGENCIES INVOLVED IN PROTECTING INFRASTRUCTURE.

Planning for infrastructure protection should cover all facilities and utilities that are vital to the nation's security and economic well-being. President George W. Bush, as Chief Executive of the Federal government, should reorganize the agencies involved in infrastructure protection to enhance coordination and implementation of Federal

Table 1

**Lead Agencies Assigned to Vital Infrastructure
by President Clinton in PDD-63**

Department / Lead Agency	Infrastructure Sector/Function
Commerce	Information and Communications
Defense	Defense
Director of Central Intelligence	Intelligence
Energy	Electric Power, Gas, and Oil
Environmental Protection Agency	Water
Federal Emergency Management Agency	Emergency Fire Service
Health and Human Services	Emergency Medicine
Justice	Emergency Law Enforcement
Justice	Law Enforcement and International Security
State	Foreign Affairs
Transportation	Transportation
Treasury	Banking and Finance

efforts to protect that infrastructure from terrorist attack and to establish oversight and accountability.

PDD-63. Many of the problems the Federal government currently faces in protecting critical infrastructure stem from a May 1998 Presidential Decision Directive issued by President Clinton titled “Critical Infrastructure Protection” (PDD-63). This presidential directive attempted to address the problem of information warfare and cyberterrorism. It tasked specific agencies with responsibility for a particular infrastructure. (See Table 1.)

PDD-63 was based on recommendations from the President’s Commission on Critical Infrastructure Protection in 1997. However, it has three major flaws that inhibit the development of an effective infrastructure protection policy:

1. Lack of accountability and oversight. PDD-63 tasked specific agencies with responsibility for infrastructure protection. But it did not establish an oversight mechanism to ensure that these departments or agencies would give sufficient attention to this mission. It did not, for example, mandate sufficient reporting requirements or timetables.
2. No clear chain of command. PDD-63 did not establish a clear chain of command for decision-making within the Federal government. Though it designated the lead agencies for each infrastructure it considered essential to the nation’s operations and made a National Coordinator responsible for synchronizing Federal efforts, it failed to explain how the relationship between the National Coordinator and the lead agencies would work.
3. Misdirected responsibilities. PDD-63 also gave responsibility for some functions to the wrong agency, such as placing the National Information Protection Center (NIPC) under the Federal Bureau of Investigation (FBI) and gave it the often conflicting missions of information sharing and law enforcement. In addition, it ignored the advantages that the Coast Guard could offer maritime security.³

Time for a New Presidential Directive. President Bush recently took a good first step to correct these deficiencies. On October 9, 2001, he appointed former National Coordinator for Security, Infrastructure Protection and Counter-Terrorism Richard A. Clarke as Special Adviser to the President for Cyber Space Security. The following week, the President issued Executive Order 13231 on “Critical Infrastructure Protection in the Information Age”⁴ to create the President’s Critical Infrastructure Protection Board, with the Special Adviser to the President for Cyber Space Security as its chairman. It also created the National Infrastructure Advisory

3. See also chapter on Military Operations.

4. See *Federal Register*, Vol. 66, No. 202, October 18, 2001, pp. 53063–53071.

Council, which includes private-sector and State and Local representatives and reports to the Critical Infrastructure Protection Board.

The purpose of the new board is to “recommend policies and coordinate programs for protecting information systems.” In this capacity, it is responsible for coordinating actions of Sector Liaison Officials in most of the Federal lead agencies. While this will improve oversight of cyber security efforts, clear and regular reporting requirements are still needed. The Board also is directed to make recommendations to the Office of Management and Budget (OMB) on Federal agency budgets dealing with cyber security in coordination with the Office of Homeland Security. This directive will improve both oversight and the budgetary chain of command for cyber security efforts.

While the President’s recent actions are a good first step, further actions need to be taken to address a broader spectrum of infrastructure that is vital to national operations beyond information systems. To correct PDD–63’s remaining deficiencies, President Bush should issue a National Security Presidential Directive (NSPD) that involves the following key steps:

Key Step #1. The President should require the Office of Homeland Security to provide annual assessments of Federal efforts on protecting vital infrastructure. Though PDD–63 designated lead agencies to be held responsible for protecting vital infrastructure, it failed to implement effective oversight. As a first step in remedying this deficiency, President Bush established the OHS to “develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks.”

Further steps are needed. For example, the NSPD should mandate that Sector Liaison Officials report as soon as possible, and thereafter annually, to the Director of OHS, the Assistant to the President for Homeland Security, on the status of security for infrastructure under their jurisdiction. These reports should include an assessment of infrastructure vulnerability (further discussed in the chapter on Intelligence and Law Enforcement), initiatives to promote security (including cross-agency efforts), progress on implementing current protection programs, private-sector cooperation, research and development on infrastructure security, and a list of priority actions for the next budget year. Such information would enable the Federal government to develop a more realistic national plan on infrastructure protection and facilitate White House oversight of infrastructure protection efforts.

The OHS Director should compile the Sector Liaisons’ reports into one assessment of Federal infrastructure protection programs to give to the President and Congress. Portions of the report dealing with cyber security should also be delivered to the President’s Critical Infrastructure Protection Board. Such oversight will ensure

that Federal agencies are focusing on this mission and are not compromising infrastructure protection to pursue other bureaucratic interests.

Key Step #2. The President's NSPD should establish a chain of command for Federal planning in core homeland defense areas. The President should task the Director of OHS with developing a plan for federal infrastructure protection efforts that establishes a clear chain of command.

Working with the States and Private Sector. The Director of OHS should consult with the heads of Federal agencies with infrastructure protection missions and Sector Liaison Officials to ascertain the critical weaknesses in infrastructure. Sector Liaison Officials, sector coordinators or Information Sharing and Analysis Centers (ISACs) when available, and the National Infrastructure Advisory Council (NIAC) should monitor and communicate private sector concerns.

The OHS should appoint a staff member or person from an appropriate lead agency to work with the states to develop their individual inventories of infrastructure at risk.⁵ The Federal government and State and Local agencies all have a stake in compiling an accurate inventory of vulnerable assets. It would be extremely difficult to coordinate Federal, State, and Local planning without one common vulnerability assessment to use as a model. By determining which areas need to be improved immediately and which could be addressed at a later date, such an inventory could assist governments in developing more effective infrastructure protection programs.

Federal agencies should continue to manage relations with private-sector industry through the Sector Liaison Officials. The OHS should hold these officials accountable by establishing clear reporting requirements.

Working with Congress. The OHS has been criticized as weak because it lacks the authority to formally approve budget requests and agency legislative proposals, as well as government-wide policy on homeland security. Granting the OHS such authority would require a statutory change, but the President can increase the OHS's voice in this process informally through presidential directions.

President Bush should create a Cabinet Council for homeland defense policy modeled after those used by President Ronald Reagan for various issues. All federal homeland defense policy should be discussed in this forum. The Cabinet Council should be chaired by the President. When the President is not in attendance, the Vice President should preside as chairman. The Assistant to the President for Homeland Security should function as executive officer, carrying out communica-

5. See discussion on national threat assessment in chapter on Intelligence and Law Enforcement.

tions and acting as the key contact point between the Cabinet Council members and the White House.

At the first meeting of this Cabinet Council, President Bush should make clear that the Director of OHS speaks for him in his absence.⁶ While not as formal and direct as statutory authority, this forum would increase the OHS Director's role in policymaking in accord with his mandate to coordinate Federal policy. By having a greater say in agency homeland security policy, the Director would indirectly influence budget requests and legislative proposals associated with those policies.

Key Step #3. The President should move the position of National Coordinator for Security, Infrastructure Protection and Counter-Terrorism into the OHS.

PDD-63 created the position of National Coordinator for Security, Infrastructure Protection and Counter-Terrorism in the National Security Council (NSC), under the National Security Adviser. The National Coordinator, a now-vacant position, is tasked with coordinating Federal efforts for infrastructure protection, a role similar to that of the new Assistant to the President for Homeland Security. The Office of Homeland Security is responsible for coordinating national policy on homeland security, of which infrastructure protection is one part. In order to avoid creating redundant structures in both the OHS and the NSC, the National Coordinator position should be moved to OHS and report to the OHS Director, the Assistant to the President for Homeland Security. The staff office created to support the National Coordinator, the Critical Infrastructure Assurance Office (CIAO), should also be moved to the OHS from the Department of Commerce. This office was created as a policy coordinating body, not a policy implementation office, and thus belongs in the new OHS.

Key Step #4. The President should move the National Information Protection Center (NIPC) out of the FBI. PDD-63 authorized the FBI to expand its warning and information-sharing efforts by creating the NIPC as a “national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity.”

This dual-track mission undermines cooperation with the private sector on information sharing. Though the NIPC's information-sharing mechanisms work rather well, many in the private sector remain cautious in sharing such information as network intrusions with the Center because of its concurrent law enforcement role. Businesses have no way of knowing whether the information they share about network security could be used to build a criminal case against them. Further, the

6. For a more in-depth discussion of the Cabinet Council, see Alvin S. Felzenberg, *The Keys to a Successful Presidency* (Washington, D.C.: The Heritage Foundation, 2000), Chapter 4.

FBI's operational guidelines encumber the work of the NIPC—for example, by restricting access to foreign intelligence.

Protection of computer infrastructure would be facilitated more through cooperation with the private sector than through investigations. Moving the NIPC out of the FBI would increase the industry's willingness to cooperate. The NIPC should, for the time being, be placed in the Department of Commerce. PDD-63 designated the Commerce Department as lead agency for information technology and the communication industry, and moving the NIPC to Commerce will complement this mission. Further, the Commerce Department has significant experience working with the hi-tech industry and implementing policy, both through the National Telecommunications and Information Agency (NTIA), which administers the department's responsibilities under PDD-63, and the Technology Administration.

If Congress passes legislation creating a permanent Federal agency for homeland security, as suggested by the Hart-Rudman Commission and proposed by Representative William (Mac) Thornberry (R-TX) and Senator Joseph Lieberman (D-CT), consideration should be given to moving the NIPC to this agency to highlight the vital nature of secure information systems.

The relocated Center also should forge a consultative and information-sharing relationship with the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University in Pittsburgh. This federally funded program operates as a private-sector clearinghouse for network security and provides services similar to those of the NIPC. Once the NIPC is removed from the law enforcement purview, it will be easier to forge a cooperative relationship with CERT and other private-sector counterparts.

Key Step #5. The President should assign the Coast Guard as lead agency for maritime homeland security. PDD-63 designated the Department of Transportation (DOT) as the lead agency for all transportation infrastructure. Within the DOT, the Coast Guard should have responsibility for protecting coastal transportation. The Coast Guard is well equipped to develop and execute a national strategy for maritime security in cooperation with the OHS. It maintains unique defense, law enforcement, intelligence, and port management authorities and capabilities.

The Commandant of the Coast Guard should work with State and Local port authorities, as well as the Immigration and Naturalization Service and the U.S. Customs Service, to develop Port Security Task Forces in every U.S. port.⁷ Each task force should be responsible for developing each port's own security plan and conducting threat and vulnerability assessments. Members of these groups should

7. For more on the role of INS and Customs, see chapter on Intelligence and Law Enforcement.

include representatives from Federal, State, and Local agencies as well as representatives of private-sector participants in that port.

Key Step #6. The President should create a Center for Interagency Maritime Intelligence and Communications. The Intelligence Community, law enforcement agencies (LEAs), and the private sector regularly obtain information vital to port security. However, no uniform mechanism exists for coordinating this information and delivering it to the owners and operators of U.S. ports. A system should be implemented through a new Center for Interagency Maritime Intelligence and Communications (CIMIC) to ensure that intelligence is delivered to the owners/operators in a way that allows them to respond with appropriate security measures. The Center should be located in the Coast Guard Intelligence Coordination Center (CGICC) in Suitland, Maryland, which manages the collection and distribution of intelligence from all Federal sources for the Coast Guard and represents it in inter-agency intelligence functions.

CGICC's information-sharing and cooperative culture makes it the appropriate place to build the new interagency center. CIMIC should be staffed with representatives of the intelligence and law enforcement communities that are active in maritime security. Current databases should be networked so that decision-makers and operational commanders can respond quickly to an emerging threat.⁸

PRIORITY #2: DESIGNATE THE GPS FREQUENCIES AND NETWORK AS CRITICAL NATIONAL INFRASTRUCTURE.

PDD-63 did not include the Global Positioning System (GPS) in the list of critical infrastructure. GPS is a space-based positioning, navigation, and timing system developed by the Department of Defense for both defense and civilian applications. Like computer networks, GPS is now integrated into the operations of other forms of telecommunications and electronic infrastructure, and public and private-sector operations critical to national security and economic stability increasingly rely on it. The telecommunications industry relies on GPS for time and frequency synchronization. The national electric grid relies on GPS to ensure line stability and find disruptions. The financial sector employs GPS timing to synchronize its encrypted computer networks. The transportation industry relies increasingly on GPS for navigational purposes.

GPS is vulnerable because it uses a very low-power signal that can be corrupted or interrupted, causing loss of information. Access to the GPS network can be disrupted in a number of ways. Russia is actively marketing handheld GPS jamming

8. For additional discussion, see chapter on Intelligence and Law Enforcement and chapter on Military Operations.

equipment that can block receiving equipment for up to 120 miles.⁹ The proliferation of ballistic missile technology presents a similar threat to the GPS satellite system. State sponsors of terrorism such as Iraq, Iran, and North Korea already possess the missile technology to mount an attack on the system, and could do so with either conventional or nuclear weapons. Because GPS networks, as well as the commercial satellite assets on which GPS relies, are critical to homeland security, the President should take the following steps:

- Key Step #1. The President should include the GPS as infrastructure critical to homeland security in the NSPD and create a national program office to manage it.** The program office should be modeled loosely after the early Atomic Energy Commission and consist of a council of members appointed by the President and a small staff of senior government personnel who coordinate GPS policy between Federal agencies, Congress, State and Local agencies, and the private sector.
- Key Step #2. The President should assign the Department of Defense as the lead agency for GPS.** The Department of Defense developed GPS, and the system serves vital national security purposes. The civil and economic value it provides are products of the Pentagon's decision to make the system publicly available. As a result, the Defense Department should be made responsible for coordinating GPS security with private-sector stakeholders and other federal agencies.
- Key Step #3. The President should issue new directives to amend existing ones on critical infrastructure to include GPS.** A number of existing directives on infrastructure protection, including Executive Order 13231, "Critical Infrastructure in the Information Age," issued by President Bush on October 18, 2001, do not include GPS in the list of programs they cover. In order for infrastructure protection to apply also to GPS, the President should issue new directives amending the earlier orders' lists of critical infrastructure to include GPS.
- Key Step #4. The Department of Defense should deploy a more secure GPS network.** The President should direct the Department of Defense—with support from the Office of Science and Technology Policy, the National Security Council, and the Office of Management and Budget—to accelerate modification of GPS satellites currently in production to include more robust signals. It should begin launching these satellites at an increased rate to augment the fragile constellation currently in operation and to establish a larger constellation over time (some 30 to 36 satellites).

9. The availability of this jamming equipment was highlighted in the Report of the Commission to Assess United States National Security Space Management and Organization (Rumsfeld Commission), released on January 11, 2001.

Additional satellites with stronger, better designed signals would increase availability and ensure operations by providing a more robust signal structure that is considerably less vulnerable to jamming. Consideration should be given to flying a mixed constellation of commodity service and specialized satellites to improve system affordability, operability, and robustness. Immediate planning is necessary to begin acquiring additional satellites to sustain a larger constellation. In the interim, the Office of Science and Technology Policy and Coordination, with the National Security Council, should place greater emphasis on developing means to protect satellite assets, particularly the GPS network.

PRIORITY #3: FACILITATE COMMUNICATION ON INFRASTRUCTURE ISSUES BETWEEN OHS AND STATE AND LOCAL OFFICIALS.

Recent events illustrate that, faced with a potential threat to infrastructure, accurate communication between State and Federal officials is critical. In November 2001, for example, the FBI warned California Governor Gray Davis that it had “uncorroborated information” that a number of the state’s bridges could come under attack. Governor Davis then issued a warning to Californians that there was “credible evidence” specific bridges might be attacked. The public announcement made an attack on specific infrastructure seem imminent. Clear communication between Federal, State, and Local officials about threats to critical infrastructure is vital.

Greater intelligence sharing also is hampered by public meeting laws in many localities. Such laws require State or Local governing bodies to make the proceedings of their meetings public. This transparency means that such venues are not conducive to discussions of classified information about risks to infrastructure; vital intelligence sources could be put at risk.

While the Office of Homeland Security is responsible for coordinating with State and Local agencies on detection, preparedness, prevention, and protection missions, action will be required at all levels of government to enhance cooperation. In addition to the national alert and warning system discussed in the chapter on Intelligence and Law Enforcement, the following actions should be taken:

Key Step #1. States should review their public meeting and disclosure laws to guarantee that classified information will not be compromised in such forums. While Federal agencies will need to share more information with State and Local agencies on suspected terrorists, potential attacks, and vulnerabilities, State and Local legislatures must make sure this information does not fall into the wrong hands. Maximum transparency should be encouraged, but current laws allow the public to attend meetings at which classified information would be exchanged, or require govern-

ment to make the proceedings of those meetings public. Where such potential exists, Local and State laws should be amended to protect secret information regarding infrastructure.

Key Step #2. The Office of Homeland Security should conduct government-wide response exercises for infrastructure attack scenarios. The response exercises should include all levels of government, from Washington to local town offices. Such exercises would allow the OHS to determine other areas where communications may be deficient, testing the nation's ability to respond to an attack. Such exercises have proven valuable for national security planning in the past and could offer similar value for homeland security. The 1978 "Nifty Nugget" exercise identified numerous communications and other gaps in American mobilization planning, resulting in a restructuring of Department of Defense transportation commands. This restructuring proved successful in 1991 when the U.S. Transportation Command (USTRANSCOM) mobilized for Operation Desert Storm. OHS should learn from DOD's experience in conducting such large-scale exercises and make plans to simulate a simultaneous attack on different infrastructures.

PRIORITY #4: ENHANCE THE PRIVATE SECTOR'S ROLE IN INFRASTRUCTURE PROTECTION.

Most of America's critical infrastructure is owned or operated by the private sector. The White House strives to include the private sector in its policymaking decisions through the National Infrastructure Advisory Council (NIAC). OHS also has hired a number of workers from industry, on a temporary basis, to help develop new policies. The private sector is a vital and reliable partner, because bottom lines and consumer and shareholder confidence are strong incentives to take steps to protect their infrastructure. Yet legal concerns and a lack of detailed information can limit the extent to which the private sector can be involved in the Federal government's efforts.

In addition to moving the National Information Protection Center out of the FBI, the Federal government should take the following actions:

Key Step #1. Congress should remove legislative roadblocks to closer communications with industry.

Freedom of Information Act (FOIA) exemptions. The Administration should work with Congress to include FOIA exemptions in authorization legislation for Federal agencies that deal with information on infrastructure from the private sector. Many private firms are reluctant to provide extensive information on vulnerability or intrusion because they fear that this information could become

public. Release of such information could adversely affect public or shareholder confidence. Similarly, competitors could use FOIA requests to gain information on company practices or systems. These fears are a major roadblock to a dialogue with the private sector. Enabling legislation for each lead agency should include FOIA exemptions for businesses that cooperate in efforts to assess threats to infrastructure.

Narrow antitrust exemptions. Congress should provide narrow antitrust exemptions for companies that share information on infrastructure protection. When corporations work together, concerns inevitably arise that they are trying to subvert the market. Antitrust laws, which try to prevent such practices as price fixing and market division, also inhibit companies from sharing information on the vulnerability of their infrastructure or the means to protect it. Cooperation on protecting critical infrastructure should be exempt from antitrust laws to protect companies that share information from unjust lawsuits. Similarly, independent private-sector mechanisms for sharing information, known as Information Sharing and Analysis Centers (ISACs), should be exempt from antitrust laws in this area.

It should be noted that the 105th Congress adopted similar legislation in the Information Readiness Disclosure Act (P.L. 105–271), signed into law on October 19, 1998, to exempt from antitrust laws any information-sharing on Y2K preparedness. In adopting the Act, Congress recognized the need to provide antitrust exemptions in areas in which public safety and national civil and government operations are concerned. This precedent should be applied to homeland security applications.

Addressing liability concerns. Legislative action should be taken to reduce liability for operators who adopt best-practices security. Such legislation should resemble the protective structure provided to consumers in the Electronic Funds Transfer Act (15 U.S.C. Sec. 1693). Congress should hear testimony on this from operators, insurance companies, and Sector Liaison Officials to establish a framework for infrastructure protection. Reducing the liability of service providers that adopt strict security measures in the event of a terrorist attack would add another incentive for businesses to adopt new standards of security and to share intrusion information.

Key Step #2. Lead Federal agencies should develop new security standards for industry.

Although security standards in the aviation industry received the most attention after September 11, a similar lack of standards exists in most infrastructure sectors. The President should direct the lead agency heads and Sector Liaison Officials for each vital infrastructure to work with the private sector to develop security standards and to determine how best to enforce them. Federal agencies should support voluntary standards that industry will be willing to adopt with federal oversight. Sector Liaison Officials should report annually to Congress and the President through the Assistant to the President for Homeland Security on the status of voluntary implementation of these standards.

Each lead agency also should publish a biannual “Honor Roll” of the top 100 operators that implement the new security standards to highlight their efforts. This program would create a competitive atmosphere in industry to adopt the most comprehensive security systems; potential customers, investors, and insurers would likely utilize such a list when deciding whether to do business with a prospective provider. A flexible free market, as opposed to a rigid bureaucracy, would serve to regulate the industry. However, if a standard vital to national homeland security proves unpopular, direct regulation with penalties for failing to comply may be necessary.

Key Step #3. Lead Federal agencies should create risk assessment programs for the private sector. Federal agencies also should assist each infrastructure sector in developing its own risk, vulnerability, and survivability assessment programs. Though the government can advise owners and operators of infrastructure of a suspected threat, it cannot assess the risk, vulnerability, or survivability of each asset. Lead agencies should develop a best-practices model for the private sector that enables them to conduct more accurate risk, vulnerability, and survivability assessments. This model would allow industry to address security necessities by meeting a set of performance standards instead of firm government specifications. In developing these models, the head of each lead agency should use the Defense Department’s internal assessment program as a guide.

Key Step #4. Congress should remove tax penalties that make it more difficult for the private sector to invest in security. Congress should revise the tax code to allow infrastructure owners to deduct the full cost of security-related spending in the year such expenses are incurred. At present, industry is only allowed to depreciate its spending for security-related purchases, often over an extended period. As a result, this creates a tax on investment spending, increasing the effective cost. Since private industry must keep the bottom line in mind, increased costs create a hurdle to private-sector spending on security. Allowing infrastructure industries to write off security spending all at once will reduce these costs, thereby improving the bottom line for companies investing in security.

PRIORITY #5: INSTITUTE NEW RULES TO MONITOR MORE CLOSELY WHO OR WHAT IS ENTERING AMERICA’S AIRPORTS AND SEAPORTS.

According to the Department of Transportation, 211,000 ships entered U.S. waters in 2000. Air traffic between the United States and the rest of the world in any one month can exceed 11 million passengers and over 700,000 tons of freight. Yet beyond the consular visa application process, there are few government programs to

monitor foreign passenger traffic for potential terrorists. And only 3 percent of shipping containers that enter the United States are inspected after they enter a port. Clearly, a more robust means for monitoring such traffic without interfering with international commerce or travel is key to protecting the nation's infrastructure.

To further protect the nation's airports and seaports:

Key Step #1. The FAA should issue new regulations and develop a system to assure that airlines are preventing terrorists from boarding an aircraft. An interagency office, under the Department of Transportation with oversight from OHS, should be responsible for developing a system to cross-check airline reservations with government-wide databases of known and suspected terrorists.¹⁰ This should be done in real time using advanced virtual technology that can collate data from a number of databases into one source.

After this technology is in place, the FAA should require airlines to use this system, which would alert ticket counter or gate employees that a suspected terrorist may be planning to board a flight. The new technology would then inform law enforcement officials and airport security, and action could be taken before the suspect boards the aircraft and the flight is cleared for takeoff. In practice, this program should function similarly to that of the Advanced Passenger Information System (APIS), which is administered by Customs, the Immigration and Naturalization Service (INS), and the Animal Plant Health Inspection Service (APHIS). Under the APIS program, which all airlines are now required to use, passenger manifests for all flights originating outside the United States must be provided before the flights arrive, to be checked for any illicit activity or suspected terrorists.

The new system of cross-checking airline reservations with government-wide databases would accomplish a similar function for all aircraft regardless of point of departure, and in real time. In order to protect Americans' freedoms, the system should not collect information on passengers' travel habits and should share only limited information (such as a warning to put a hold on a ticket) with airlines.

Key Step #2. The Administration should create an interagency center to analyze data on people and products entering the United States by sea. This interagency center, which should be managed by the new Center for Interagency Maritime Intelligence and Communications (CIMIC),¹¹ would cross-check passenger, crew, and cargo manifests of all vessels entering American territorial waters with all Federal watch lists of suspected and known terrorists before a ship is allowed to enter port.¹²

10. For a discussion on how federal agencies can better share database information, see chapter on Intelligence and Law Enforcement.

11. As discussed in Priority #1.

12. See chapter on Military Operations.

Like the system discussed above, the new center would have to use virtual office technology to check manifests against the numerous federal databases. However, it would not have to operate under the strict time and operational constraints that the airline system faces. Suspected terrorists attempting to enter the United States on an airline or to ship weapons by air would have to be intercepted before departure for two reasons: the relatively short amount of time it takes for a modern airliner to reach its destination and the limited number of options available in intercepting a passenger during the flight. Traveling by ship takes significantly longer and increases interception options.

Ships wishing to enter American ports are already required to give advance notice of this intention. Before September 11, ships were required to give 24 hours notice. Since September 11, the Coast Guard has increased that requirement to 96 hours. When a ship gives the Coast Guard notice of its wish to enter an American port, it should be required to provide the CIMIC a complete manifest of passengers and cargo. This would give the Center ample time to review these documents and deploy Coast Guard or Navy assets to intercept and investigate any ship suspected of transporting terrorists or their weapons.

Key Step #3. The U.S. Customs Service should experiment with a point-of-origin inspections program for maritime trade. Numerous measures should be developed to protect Americans from terrorism, but the most effective means remains preventing terrorists and their weapons from even entering the United States. Inspecting vessels before they leave their points of origin would make it more difficult for potentially deadly weapons and people to enter U.S. territorial waters.

To this end, the Administration should direct the U.S. Customs Service to create a pilot point-of-origin inspection program in order to determine whether such inspections can be done in a cost-efficient manner. The pilot program should include three countries to start. Initially, the Administration should negotiate with one significant trade partner each in Europe, Asia, and the Third World to implement the pilot program. This geographic diversity will allow the Administration to determine the potential success of a general program across different political systems, cultures, and levels of economic development. The pilot program also should experiment with different ways of cooperating with the government of origin, and with outsourcing functions to private industry to keep costs down.

If the pilot program proves successful and cost-efficient, the Administration should include point-of-origin inspection agreements in international trade agreements. Provisions should be included to prevent the use of a point-of-origin inspection program as a non-tariff barrier to trade. Nations that want to trade freely with the United States should also want to trade securely. The U.S. Ambassador to the United Nations should propose a treaty on point-of-origin inspections while

assuring potential trade partners that bilateral programs would not be held hostage to any multilateral efforts in this area.

Key Step #4. Congress should authorize a nationwide Sea Marshals Program. Sea Marshals should be organized into two-, four-, and six-person teams based on lessons learned from the pilot program in California. The teams must be capable of boarding deep-draft vessels to inspect their cargo and passenger manifests. Team members may include representatives of the military, Federal law enforcement, and the private sector, and must meet federally established and certifiable standards. The program should include Special Maritime Security Strike Teams within the Coast Guard—rapid response teams that are specially trained and equipped to take control of a facility or vessel that is a potential threat to security.

Key Step #5. The Transportation Security Agency should require airport administrators and port authorities to employ systems that prevent unauthorized people from gaining access to secure areas. Both airports and seaports should, at a minimum, be required to screen employees seeking access to secure areas before permitting them to enter. The Secretary of Transportation should direct the Transportation Security Agency (TSA) to issue new regulations to ensure that only those who need access are able to enter the secure areas of airports. Similarly, local port authorities, in cooperation with the Coast Guard and Federal, State, and Local law enforcement agencies, should adopt new programs to improve security for port employees and users. Advanced biometrical technologies, smart cards, and background checks for employees may also be employed to ensure greater safety.¹³

PRIORITY #6: SECURE ALL FEDERAL NETWORKS AND INFORMATION SYSTEMS.

All federal agencies rely on computers and information networks for day-to-day operations. The U.S. General Accounting Office, in a recent report titled *Computer Security: Improvements Needed to Reduce the Risk to Critical Federal Operations and Assets*,¹⁴ found that “federal systems were not being adequately protected from computer based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations.” Poor purchasing decisions caused some of these problems.

13. For further discussion of the use of biometric technologies for homeland security, see chapter on Civil Defense and chapter on Intelligence and Law Enforcement.

14. GAO-02-231T, November 9, 2001.

Key Step #1. All Federal agencies should focus network purchasing decisions more on security than on cost. The Office of Management and Budget, in Circular A-76, “Performance of Commercial Activities,” directs Federal agencies to make many purchasing decisions on a lowest bid basis. OMB Circular A-76, which was last revised in October 1998 to conform with the Federal Activities Reform Act of 1998 (P.L. 105-270), calls for basing agency decisions on contracting out commercial activities solely on cost estimates. This may be the best way to make procurement decisions for food services and other non-security-related services, but outsourcing vital Federal information systems should not be conducted on a lowest price basis.

Priority must be placed on ensuring the security of Federal information systems. OMB Circular A-76 should be amended to make security the key consideration—at least as important as keeping costs in line—when outsourcing information technology services. In addition, the revised reporting requirements should include an analysis of how procurement decisions on information technology systems will affect network security.

Key Step #2. The executive branch should explore alternatives to the proposed government-only Internet system (GOVNET) before making procurement decisions.

The Special Adviser to the President for Cyber Space Security has proposed creating a government-only intranet that would rely on routers and servers separate from those of the regular Internet. The General Services Administration (GSA) has begun consulting with the computer industry for recommendations on implementation.

The idea behind this proposal is to increase security of unclassified government networks by “running them on fiber [optic cable] that doesn’t touch the Internet routers,” according to the Special Adviser in a recent interview with the *National Journal’s Technology Daily*.¹⁵ It would operate similarly to the independent network already operated by the Defense Department for classified information.

Many experts, however, including former Director of Central Intelligence James Woolsey and former National Security Adviser Sandy Berger, argue that GOVNET would improve security only marginally at best. GOVNET would not be secure from operator error, hacking, or even e-mail viruses such as the “I Love You Bug” that hit Pentagon computers in 2001. Moreover, purchasing or leasing an entirely separate network could be very expensive. Security must be placed at a premium, of course, but GSA must ensure that the security provided justifies the expenditures. The President should direct GSA to consult with industry about achieving the same or greater level of security through the use of intranets that rely on the Internet. GSA and OMB should evaluate both the GOVNET and standard Internet options in consultation with OHS, the Office of Science and Technology Policy (OSTP),

15. Bara Vaida, “Transcript: Clarke Talks Cyber Security,” *Technology Daily*, November 27, 2001.

and the Special Adviser to the President for Cyber Space Security to determine which one would provide better security for the dollar.

PRIORITY #7: ACCELERATE GOVERNMENT COMPLIANCE WITH THE NUCLEAR WASTE POLICY ACT.

The Nuclear Waste Policy Act of 1982 (P.L. 100–207) requires the Department of Energy (DOE) to build a secure underground repository for high-level nuclear waste. Currently, spent nuclear fuel is stored in numerous facilities around the country with varying levels of security. The Act mandated that DOE begin transferring waste to the new facility at Yucca Mountain, Nevada, in 1998. DOE, on its Web site, now estimates that it cannot begin transferring any nuclear waste to this site until 2010. If that is the case, DOE is already running 12 years behind schedule.

Spent nuclear fuel, if acquired by enemies of the United States, could be used to build a “dirty bomb” that could be exploded to spread radiation across a designated area. The destruction of infrastructure caused by such a bomb would be much less than the human toll, but it would still be immense. Providing greater security for this waste material must be a priority, and DOE must be held to its statutory obligations.

Key Step #1. Congress should hold hearings to determine how DOE can bring the Yucca Mountain facility on-line more quickly and improve security. Once operational, the Yucca Mountain, Nevada, facility should provide the appropriate level of security for nuclear waste. A top priority should be given to accelerating implementation of DOE’s legal responsibility. In the meantime, Congress should explore how the private sector and government can work together to ensure that nuclear material is secure.

CONCLUSION

Critical infrastructure protection is vital for the nation’s economic, physical, and social well-being. Some actions need to occur immediately to increase near-term security and create a more open atmosphere for cooperation and coordination among government agencies and with the private sector. President Bush should issue a presidential directive on infrastructure protection to reflect the realities of the post-September 11 world.

Federal agencies must work together and with their counterparts at the State and Local levels to create security standards for infrastructure protection. To improve security, Federal action must be taken in key infrastructure areas, including the Global Positioning System, airport and seaport security, Federal network security,

Table 2

A Key Unimplemented Commission Recommendation for Infrastructure Protection

Recommendation	Name of Commission	Status
The Coast Guard and U.S. Department of Transportation, in cooperation with State and Local agencies and the private sector, should develop and institute “Model Port Standards” for ports’ physical security.	Seaports Commission, <i>Report of the Interagency Commission on Crime and Security in U.S. Seaports</i> (Fall 2000)	Currently, no Federal program available to oversee the implementation of standards or to advise owners and operators on how to implement them.

and nuclear waste security. Roadblocks that currently hinder information sharing with the private sector must also be eliminated. Over the long term, an effective infrastructure protection policy will require restructuring the government agencies involved and how they interact and operate as well as addressing security shortcomings in specific industries.

TOP PRIORITIES FOR STRENGTHENING CIVIL DEFENSE AGAINST TERRORISM

*A Report of the Working Group on Civil Defense Against
Weapons of Mass Destruction¹*

Jack Spencer, Working Group Rapporteur

Assuring adequate civil defense against terrorist attacks has become a national priority since September 11, 2001. Unlike defending the nation from military attacks, civil defense begins with preparation and planning at the local level. The first responders to an emergency almost always are local emergency workers and volunteers, a fact poignantly illustrated in New York and Virginia. In the war on terrorism at home, it is the firefighters, law enforcement officials, emergency medical services, health professionals, and hazardous materials crews that become America's front-line fighters. They are ill-prepared, however, to respond to or prevent a terrorist attack using weapons of mass destruction—a fact made clear by a host of commissions and studies prior to September 11.²

The threat of a new terrorist attack on civilians is real. To assist Local, State, and Federal officials in improving their ability to detect and respond to attacks on civilians using chemical, biological, radiologic, or nuclear (CBRN) agents, the

-
1. The members of the Working Group on Civil Defense Against Weapons of Mass Destruction include Albert Ashwood, Director, Oklahoma Emergency Management; Dr. Daniel Dire, Department of Emergency Medicine, University of Alabama; Dr. Daniel Goure, Senior Fellow, Lexington Institute; Dr. Fred Iklé, Distinguished Scholar, Center for Strategic and International Studies; Col. Joseph Muckerman, USA (Ret.), former Director of Emergency Management, Office of the Secretary of Defense; and Michelle White, Counsel, Subcommittee on Economic Development, Public Buildings, and Emergency Management, Committee on Transportation and Infrastructure, U.S. House of Representatives. The following individuals contributed to this report in an advisory capacity: Michael J. Merchlinsky, Ph.D., Microbiologist, Office of Vaccine Research and Review, Center for Biologics Evaluation and Research, U.S. Food and Drug Administration; Phoebe Mounts, Ph.D., Esq., Adjunct Faculty, Johns Hopkins University School of Public Health; Grace-Marie Turner, President, The Galen Institute; and the staff of The Honorable Martin O'Malley, Mayor of Baltimore, Maryland.
 2. For a summary of recommendations from prior commissions and studies that have not been implemented, see the table at the end of this chapter. The status of post-September 11 legislative efforts may be found in the Appendix.

Working Group on Civil Defense Against Weapons of Mass Destruction has prepared a list of top priorities. The following priorities were selected because (1) they represent new approaches not previously proposed, and (2) if implemented, they will strengthen government's efforts to deter and respond to terrorism.

- **Priority #1: Build a nationwide surveillance network for early detection of chemical, biological, or other attacks.** After September 11, concerns about the ability of terrorists to harm large numbers of civilians with a CBRN agent led to calls for increased surveillance. In order to mobilize a rapid response to such an attack, government leaders must be able to recognize the outbreak of a catastrophic illness or an attack on food and water supplies. This requires setting up a nationwide network of local surveillance systems to monitor and disseminate the information collected. Such information would increase government's ability to recognize an attack in the earliest stages and limit its effects.
- **Priority #2: Develop a terrorism response checklist and a manual of civil defense exercises to guide officials in assessing preparedness.** Local and State authorities need to prioritize their efforts to improve their capabilities to respond to CBRN events. These new tools should be designed to give them guidance on where their weaknesses are and how best to proceed based on national standards. They should help improve coordination between Local, State, and Federal civil defense authorities and responders, and give guidance on how to obtain Federal assistance.
- **Priority #3: Accelerate the development of pharmaceuticals to prevent and limit the spread of toxic agents by terrorists.** Given the urgency of protecting Americans from biological terrorism that followed the recent anthrax deaths, the Federal government should facilitate the rapid development and supply of new and safer vaccines and antitoxins, drugs, and medicines that provide immunity to such diseases as smallpox or that limit their effects.
- **Priority #4: Create a national web of CBRN experts who will train first-response teams for an outbreak or terrorist attack.** A program that identifies these experts and deploys them in teams to share their expertise with local first responders is an affordable and effective way to prepare for CBRN attacks.
- **Priority #5: Simplify the process of obtaining Federal assistance for civil defense initiatives.** A civil defense block-grant program under the Federal Emergency Management Agency (FEMA) should be established to enable State and Local authorities to target funding to address their unique civil defense needs.

- **Priority #6: Sign mutual support agreements with Canada and Mexico on responding to terrorist acts in border communities.** A biological or radiologic attack on Detroit, for example, could have serious consequences for people in Ontario. The United States should sign agreements with Canada and Mexico to cooperate not only on preventing such attacks, but also on managing the consequences should one occur.
- **Priority #7: Develop a nationwide education and public relations program.** Governments at every level should have programs in place to inform the public about terrorist threats and civil defense plans in order to mitigate fear and build support for their efforts.

PRIORITY #1: BUILD A NATIONWIDE SURVEILLANCE NETWORK FOR EARLY DETECTION OF CHEMICAL, BIOLOGICAL, OR OTHER ATTACKS.

Terrorists who seek mass casualties using a chemical, biological, or radiologic agent are unlikely to announce that event. The key to preventing the spread of deadly diseases and to timely consequence management is early detection. Government officials must be able to anticipate when an outbreak of certain illnesses means an attack has occurred. Yet no comprehensive national surveillance network exists to assist Local, State, and Federal officials in detecting a CBRN attack in the earliest stages.

Even though effective nationwide surveillance requires improving or developing technology to detect CBRN events, the United States does not need to remain highly vulnerable until those technologies become available. Monitoring and reporting systems can be established today to help local governments ascertain that a CBRN event is occurring. Local governments maintain a constant watch over America's cities and local jurisdictions, and their emergency and public safety personnel are usually the first to respond to an outbreak or health crisis.

Thus, any national surveillance network must operate from the ground up.³ Local surveillance networks should provide data regularly to the State on health or other vulnerable sectors; the State should compile and channel these data to Federal authorities. In this way, alerts about a possible CBRN event unfolding could be sent out nationwide to alert communities to step up their detection efforts and response preparations.⁴

3. See also discussions in chapter on Infrastructure and chapter on Intelligence and Law Enforcement.

4. For a discussion of a CBRN alert system, see chapter on Intelligence and Law Enforcement.

For such a system to be effective, mayors must take the lead in establishing a surveillance network for their metropolitan areas, and governors should establish a surveillance network covering the rural areas of their States. The Federal government should provide guidance, information-sharing, and other support services as needed.

Key Step #1. The President should direct the Office of Homeland Security, in association with the Centers for Disease Control and Prevention (CDC) and the Federal Emergency Management Agency (FEMA), to develop monitoring standards and guidelines for reporting likely CBRN events. State and Local agencies, health services, and certain industries are likely to be the first to observe symptoms of CBRN attacks. To assure the creation of an effective national surveillance system, these entities need guidance on what criteria to measure and how to report their findings. These monitoring and reporting standards should be developed by the Federal government by involving individuals with expertise on the effects of chemical, biological, and radiological agents on humans, animals, and the environment. The criteria could include such symptoms as increases in hospital or veterinary clinic admissions, appearance of chemical or biologic substances in water supplies, and sharp increases in consumer purchases of over-the-counter medicines to treat flu-like symptoms. The Federal guidelines should be established within three months and made available on the FEMA and CDC Web sites.

Key Step #2. Governors and mayors of major cities should each designate a top public health official to establish and oversee a CBRN-related surveillance network in each jurisdiction. These designees should oversee their respective Local or State surveillance networks, including collecting and distributing the data. These data should be made available to the Centers for Disease Control and Prevention for analyzing the information collected on a national scale.

Key Step #3. Local and State public health officials should implement monitoring and reporting requirements according to the Federal guidelines. State and Local public health officials must be trained to recognize the symptoms of a CBRN attack and identify where these symptoms are likely to emerge in their jurisdictions. They should require specific agencies, health services, and business sectors that are likely to see or treat the casualties to give real-time data to the public health departments.

For example, each mayor and governor should contact every hospital chief in their jurisdiction and ask them to submit regular reports to the health department. These reports would consist of a one- or two-page form to be transmitted via fax or e-mail, adding little cost to the daily operations of these institutions. These reports should be submitted daily, since the initial hours following a CBRN attack are the most critical and the most deadly. They should include information on increases in

admissions, cases that exhibit specific symptoms, and ambulance activity. Other public institutions should submit similar information, such as a sudden increase in the number of students or employees who are absent.

Private organizations and businesses that handle data critical to the veracity of this effort should be asked to submit similar reports. Such data include prescription and over-the-counter drug purchases, veterinary hospital activity, and agricultural yields.

Anomalies in these public and private-sector reports could indicate that a CBRN event had occurred. Local health departments should channel these data to the State health departments, which would forward the information to the CDC. The CDC would decide whether a nationwide alert should be released.

Key Step #4. The President should direct the CDC to establish a national system to collect and analyze relevant data from Local and State governments. The CDC, in collaboration with the Office of Homeland Security and the Federal Bureau of Investigation (FBI), should establish a national CBRN surveillance system for collecting, analyzing, and distributing data reported by the State surveillance networks. This system should be developed as part of the existing National Health Alert Network, a dynamic information database operated by the CDC that will enable officials to detect anomalies in public health that indicate a terrorist attack.

Key Step #5. The President should direct the Department of Health and Human Services (HHS) to foster the development of sensitive technologies that detect the presence of CBRN agents. HHS should issue a new request for proposal (RFP) for the development of more sophisticated detection systems. Though other commissions and reports also have recommended that more research be done to develop technologies that detect the presence of CBRN agents, not enough has been done to date to produce and field such technologies.

HHS should design the RFP with support from the new Committee on Science and Technology for Countering Terrorism under the National Academies of Science,⁵ and the Technical Support Working Group (TSWG), a cross-agency group coordinated by the U.S. Department of State.⁶ The RFP should require that proposals include (1) a biosurveillance system architecture for integrating independent sources of data, such as biosensor and health surveillance data, and a protocol for monitoring the system; (2) an autonomous detection algorithm (a software program) that accepts data from multiple surveillance nodes (e.g., emergency room admissions) on selected patient types or drug prescriptions suggestive of a

5. The committee was established to bring together the nation's top scientists and laboratories to establish a long-term CBRN counterterrorism research and development effort. See <http://national-academies.org/counterterrorism>.

CBRN attack; and (3) disease models for autonomous detection of real-time data using high-precision models of dynamic epidemiology. HHS should design the RFP to stimulate a collaborative effort between industry and major universities with biodefense research labs.

This project should complement the CDC's National Health Alert Network initiative, a nationwide integrated information and communications system intended to facilitate the dissemination of health alerts, prevention guidelines, and other information.

PRIORITY #2: DEVELOP A TERRORISM RESPONSE CHECKLIST AND A MANUAL OF CIVIL DEFENSE EXERCISES TO GUIDE OFFICIALS IN ASSESSING PREPAREDNESS.

State and Local authorities do not now receive adequate guidance or support from the Federal government about how to prevent a terrorist attack and how to respond should deterrence fail.⁷ No national standards have been compiled for assessing the extent to which a State or Local government is prepared for a CBRN event or how they should respond to one. The result: Local and State authorities are unsure about how to mobilize their resources to prepare for terrorist attacks and how to prevent them.

The Federal government should assist the states by developing evaluation tools that enable them to assess their levels of preparedness.

Key Step #1. The President should mandate the creation of an OHS-led task force to recommend national standards for CBRN preparedness at the State and Local levels. The President should direct the Assistant to the President for Homeland Security (the Director of OHS) to establish a task force with representatives from OHS, the U.S. Departments of Justice and Defense, FEMA, the CDC, and other relevant federal agencies. The task force also should include representatives from Local and State governments that have dealt with CBRN-type events, such as in

-
6. The TSWG describes itself as “the U.S. national forum that identifies, prioritizes, and coordinates interagency and international research and development (R&D) requirements for combating terrorism. The TSWG rapidly develops technologies and equipment to meet the high-priority needs of the combating terrorism community, and addresses joint international operational requirements through cooperative R&D with major allies.” It includes representatives from the U.S. Departments of State, Defense, and Justice (including the FBI), and FEMA. Participation is open to all agencies. See <http://www.tswg.gov>.
 7. President Bush recently created an Office of Public Health Preparedness to assist in coordinating a national response to public health emergencies.

Oklahoma City, Baltimore, and New York. The goal of this task force should be to establish national standards for what constitutes “preparedness” for responding to a CBRN event and to help Local and State governments identify what they need to do to be prepared.

Key Step #2. The Director of OHS should require the task force to develop printed guides by mid-2002 that will help State and Local officials assess preparedness before mid-2003. The first tool the task force distributes should be a short checklist that Local and State officials use to assess their vulnerabilities and what they need to do to prepare for CBRN events. For example, the checklist could ask whether systems are in place to identify open hospital beds, recognize the symptoms of CBRN attacks, provide back-up communications in emergencies, provide adequate medical supplies, and other prevention and precautionary measures.

The second guide, a manual of civil defense exercises, should help Local, State, and Federal officials set up “war-game” exercises that walk them through different scenarios of attack. These exercises, whether simulated in a classroom or real, would highlight key weaknesses in their civil defense and response systems and provide guidance on what to do to improve.

These guides should offer guidance on requesting Federal funds to address specific weaknesses. Together, they would act as a measurement tool for OHS to gauge the effectiveness of the State and Local initiatives. The task force should develop these documents within the next six months and make the approved documents available to State and Local governments on CDC’s Web site.

Key Step #3. The President should direct the OHS Director to initiate CBRN response exercises with each State. States deemed most at risk should be among the first to undergo the exercises; all states should have participated in these exercises within the first five years. Over time, multi-state preparedness exercises could be held. The point of contact between OHS and each State should be the governor’s office, which would be responsible for bringing State and Local officials and any private-sector or volunteer participants into these exercises. States should be required to submit evaluation reports to OHS after each exercise, along with requests for Federal homeland security preparedness aid to address any weaknesses exposed by the exercises.⁸

8. For the role of the National Guard and Reserves in homeland defense, see chapter on Military Operations.

Table 3

Characteristics of Terrorist-Related Biological Agents

Agent	Availability	Lethality	Vaccine/ IND*
BACTERIAL AGENTS			
Inhalation anthrax	Difficult to obtain virulent seed stock; difficult to process and disseminate with great success	Very high	Yes, primate tested. Some view efficacy for inhalation anthrax as questionable
Plague	Very difficult to acquire seed stock and to successfully process and disseminate	Very high	No
Glanders	Difficult to acquire seed stock; moderately difficult to process	Moderate to high	No
Tularemia	Difficult to acquire correct strain; moderately difficult to process	Moderate if untreated, low if treated	IND
Brucellosis	Difficult to acquire seed stock; moderately difficult to produce	Very low	No
Q Fever (rickettsial organism)	Difficult to acquire seed stock; moderately difficult to process and weaponize	Very low if treated	IND; tested in guinea pigs; produces adverse reactions
VIRAL AGENTS			
Hemorrhagic fevers (e.g., Ebola)	Very difficult to obtain and process. Unsafe to handle	Very high, depending on strain	No
Smallpox	Difficult to obtain seed stock and difficult to process. Only confirmed sources in the United States and Russia.	Moderate to high	Yes
Venezuelan Equine Encephalitis	Difficult to obtain seed stock. Easy to process and weaponize	Low	IND
TOXINS			
Ricin	Readily available and moderately easy to process; but tons would be required for mass casualties	Very high	No, but candidate vaccines under development
Botulinum (Types A-G)	Widely available but high toxin producers not readily available; not easy to process or weaponize	High without respiratory support	IND; tested in primates. Toxid vaccine against some types (A-E)
Staphylococcl Enterotoxin	Difficult to acquire high yielding seed stock; moderately to difficult to process	Low	No

Note: *Investigative New Drug
Source: Based on U.S. General Accounting Office, *The Department of Health Combating Terrorism: Need for a Comprehensive Threat and Risk Assessments of Chemical and Biological Attack*, GAO/NSIAD-99-163, September 1999, p. 30.

PRIORITY #3: ACCELERATE THE DEVELOPMENT OF PHARMACEUTICALS TO PREVENT AND LIMIT THE SPREAD OF TOXIC AGENTS BY TERRORISTS.

As the recent terrorist attacks demonstrate, the U.S. government must approach the research and development of new antibiotics, therapeutic drugs, and vaccines against diseases caused by CBRN agents as a national priority and put adequate resources behind these efforts. Table 3 lists the biological agents that terrorists could employ against Americans, according to one government study. A recent war-game scenario by the Center for Strategic and International Studies predicted, for example, that a coordinated terrorist attack using the smallpox virus could cause up to 6,000 American casualties within just two weeks.⁹ The last Americans immunized against smallpox were vaccinated in 1972, and it is not known whether they are still immune, or how they will respond to another vaccination.

The urgency of developing adequate vaccines, however, is only one factor in the equation. Research should also include the development of pharmaceuticals that are effective against mutated or manipulated bioagents, medicines that are effective against more than one agent, and methods of extending the shelf-life of medicines. Antitoxins also should be developed to treat late-diagnosed anthrax cases.

Development of pharmaceuticals is extremely costly. According to a recent study by the Tufts Center for the Study of Drug Development, it costs an average of over \$800 million to develop each new prescription drug.¹⁰ Currently, the U.S. Department of Health and Human Services offers grants for the development of new medicines. Because there is little demand today for terrorism-related vaccines, grants are needed to stimulate R&D. But the money HHS offers in its RFPs often is not sufficient to make developing a vaccine or medicine worthwhile for a pharmaceutical company. Thus, even the existing fast-track provisions are not being fully utilized. Moreover, communication between private industry and the Food and Drug Administration (FDA) is tortuously slow. Much can be done to improve this process to ensure that adequate supplies of safe and effective vaccines and medicines are available, including a mechanism for approving generic vaccines, which would help lower prices over time.

The Secretary of Health and Human Services recently proposed a plan to accelerate bioterrorism research. For the most part, these proposals go to support initial research, which is needed. However, there also need to be changes that allow the initial research to generate the development of products that can be made available to the public quickly.¹¹

By instituting a few policy changes, the United States could greatly reduce the time it takes to bring vaccines and medicines from the lab to pharmacy and clinic shelves.

Key Step #1. The Secretary of HHS should establish reasonable requests for proposals for the development of new pharmaceuticals associated with CBRN terrorism.

Congress should allocate adequate funds to HHS to use in the competitive bid process for anti-terrorism drugs. Manufacturers need a respectable return on their new products to stay in business. But HHS too often puts forth RFPs that offer too

9. See ANSER Institute for Homeland Security, "Dark Winter," at <http://www.homelandsecurity.org/darkwinter/index.cfm>. The CDC estimates the number to be far lower. See Steve Milloy, "Exaggerated Threat of Smallpox Terrorism," *The Washington Times*, October 7, 2001, p. B3.

10. Press release, "Tufts Center for the Study of Drug Development Pegs Cost of a New Prescription Medicine at \$802 Million," Tufts University, November 30, 2001.

11. See U.S. Department of Health and Human Services, "HHS Accelerates Bioterrorism Research," NIAID Press Office, December 6, 2001, at <http://www.hhs.gov/news/press/2001pres/20011206a.html>.

little money for the expensive R&D required. One side effect is that the smaller companies with less expertise and resources will put in bids, hoping to use the new drug to establish themselves, while larger companies will choose to participate only if the return on investment is expected to be substantial. In the war on terrorism, Americans need all companies to be motivated to do research and development on pharmaceuticals that will prevent or limit the illnesses and death that the agents favored by terrorists might cause.

Key Step #2. The President should guarantee patent protection on pharmaceuticals related to terrorism. The President must issue a statement making clear that his Administration will uphold patent protection laws for new pharmaceuticals that help protect Americans against the toxic agents sought by terrorists. American ingenuity is born out of the incentive to succeed. Pharmaceutical companies may be deterred from making the significant investments necessary to develop new medicines if they fear that HHS will override their patents to allow other manufacturers to produce generic versions of their product. This point was driven home in the recent debate over expediting production of CIPRO or its generic version to treat anthrax.

Key Step #3. The FDA should prioritize applications for fast-track approval of pharmaceuticals. Developing pharmaceuticals to protect Americans from terrorist attack is a national priority. Therefore, FDA's fast-track regulatory process should be clarified to reflect that priority.

Provisions such as “Drugs Intended to Treat Life-Threatening and Severely-Debilitating Illnesses”¹² and “Accelerated Approval of Biological Products for Serious or Life-Threatening Illnesses”¹³ establish procedures to expedite the development, evaluation, and marketing of new therapies for life-threatening and severely debilitating illnesses. To take advantage of these provisions, pharmaceutical companies must go through an extensive application process. The provisions do not prioritize applications based on product; thus, all applications from drug and biologic manufacturers go through the same lengthy application process, regardless of the product to be produced. Manufacturers trying to get into fast-track programs to develop pharmaceuticals associated with homeland security should be given higher priority, at least until the threat is determined to be reduced. The FDA also should not delay in approving life-saving drugs already in the pipeline.

To speed up the process further, upon acceptance of an application for fast-track development, the FDA should offer manufacturers a blueprint for obtaining approval of vaccines or medication for anti-terrorism agents. This would lay out

12. 21 C.F.R. Section 312.80 Subpart E.

13. 21 C.F.R. Section 601.40 Subpart E.

exactly what it is that FDA will be looking for throughout the approval process. By setting up a blueprint beforehand, the sponsor could tailor its efforts to meet regulatory requirements.

These new procedures will likely lead to more applicants, increasing FDA's work and oversight responsibilities accordingly. Therefore, FDA should reassign current staff to facilitate the effort to develop new anti-terror-related pharmaceuticals. There should be no need to expand the staff of the FDA, because staff assignments should reflect the priorities of the nation. However, if more staff are required to maintain adequate safety standards and oversight, HHS should be prepared to provide those staff.

Key Step #4. Congress should authorize the approval of generic vaccines by the Center for Biologics Evaluation and Research (CBER) after the relevant patents have expired. To encourage reductions in pharmaceutical prices, Congress should amend the Public Health Service Act (P.L. 78–410), which established and governs the CBER, to allow marketing approval of generic versions of “biologics” relevant to terrorism, which include vaccines, after their relevant patents have expired.

The Center for Drug Evaluation and Research (CDER) oversees the development of drug manufacturing and approval. In that capacity, it has the authority to approve new drugs as well as generic ones under the Federal Food, Drug, and Cosmetic Act (P.L. 75–717). The addition of generic drugs to the market would bring down the price of drugs over time. There is no similar mechanism for biologics (vaccines).

Authorizing the CBER to approve generic brands must be done in conjunction with providing additional funds for the initial development of a vaccine, in order to assure developers of a vaccine that their hefty investments will be rewarded.

PRIORITY #4: CREATE A NATIONAL WEB OF CBRN EXPERTS TO TRAIN FIRST-RESPONSE TEAMS FOR OUTBREAKS OR ATTACKS.

No Federal agency or program can train hundreds of thousands of police officers, emergency medical technicians, firefighters, and other local first responders to be ready for a terrorist attack. At full capacity, the Center for Domestic Preparedness (CDP)—America's premier CBRN first-response training facility—can train only about 10,000 people each year. Instead of attempting to train everyone at one of the National Domestic Preparedness Consortium sites, the President should expand the CDP's Train-the-Trainer programs so that graduates can return home to train local first responders.

Key Step #1. Congress should provide adequate funding for CBRN training. Congress should include an additional \$1 billion each year in the Commerce, Justice, and State appropriations bill to expand CDP's capability to create a web of CBRN experts who train the first responders.

Key Step #2. The President should direct the Attorney General to expand Train-the-Trainer programs in the Office of Domestic Preparedness. A significant portion of its CDP resources should go to each National Domestic Preparedness Consortium site to create new groups of mobile CBRN first-response trainers. These trainers should conduct on-site exercises with Local officials. After these lessons, the newly trained Local first responders can train volunteer and rural first responders. Such a change should be implemented as soon as possible to initiate a nationwide system of complementary training even before an actual web of CBRN trainers is complete.

PRIORITY #5: SIMPLIFY THE PROCESS FOR OBTAINING FEDERAL ASSISTANCE FOR CIVIL DEFENSE INITIATIVES.

Many Federal agencies now offer funding to State and Local organizations to prepare for catastrophic events such as a massive terrorist attack. Each has its own application process. Funding often has to funnel through the State before it reaches the Local jurisdictions, and there is no coherent strategy for determining how the money is used. This inefficient and confusing system facilitates the misspending of funds.

Other Federal assistance programs use "block grants" to give State and Local governments an opportunity to target the funds they receive to their unique needs. This system is a good model for providing direct funding to civil defense initiatives at the Local level.

Key Step #1. The President should direct Federal agencies to streamline the current grant process that supports State and Local terrorism response and prevention activities. The President should direct each Federal agency that gives funds to State or Local domestic preparedness programs to submit a description of those programs to the Office of Homeland Security. He should direct the OHS Director to develop a single grant application process that State and Local authorities would use to apply for the funds. And he should charge OHS to provide guidance on improving the current grant process.

By simplifying the application process, the Federal government could reduce the red tape that accompanies Federal funding. Congress can assist by including in program authorization bills a description of who is eligible for funds and how the funding should generally be used.

Key Step #2. Congress should authorize the establishment of a homeland security block grant program in the Federal Emergency Management Agency. Currently, no funding stream exists to get Federal funds directly to the Local governments. Congress should provide authorization for a Federal block grant program that distributes funds to localities to help them prepare for terrorism according to their own unique prevention and response priorities. If OHS is established as a separate Federal agency by an act of Congress, it could take over the administration of these block grants. The overarching mission of OHS—homeland security—would make it well-suited to this task.

Cities with more than 100,000 residents should be eligible for the grants. States should be eligible for the grants provided they use the money to support rural and volunteer first-response units that would not otherwise be eligible.

Key Step #3. Congress should require that block grant funding be conditional, non-transferable, and accountable. One of the problems with other Federal block grant programs is that adequate accountability measures are lacking. Measures should be included in the homeland security block grant program to ensure they are used appropriately. For example, the grants could be used to supply Local first-response teams with the equipment they need to conduct CBRN missions and training exercises, to bring their preparedness levels up to national standards (as established in the checklist and exercise guide), and to improve consequence management.

The authorization legislation must make clear that the funds are non-transferable. Further, it should require grant recipients to submit after-action reports to FEMA to establish that the funds were used appropriately. This program should coincide with the distribution of the civil defense preparedness checklist and the exercise guide described above.

PRIORITY #6: SIGN MUTUAL SUPPORT AGREEMENTS WITH CANADA AND MEXICO FOR RESPONDING TO TERRORISM IN BORDER COMMUNITIES.

It is important that the United States and its neighbors cooperate to prevent terrorism with weapons of mass destruction. But they also will need to cooperate to manage the consequences should a chemical, biological, radiologic, or nuclear attack occur. None of the reports or commissions on civil defense thus far have adequately addressed cooperative responses to near-border attacks.

There is a high likelihood at this time that a terrorist trying to smuggle a CBRN weapon into the United States would do so by crossing America's porous borders. But a terrorist could release a toxic agent into the air in Mexico or Canada that

would flow into communities in the United States. The opposite is true as well: An attack on the United States could have devastating effects on Mexico or Canada. A terrorist attack in any American, Canadian, or Mexican border community could quickly overwhelm local capabilities and systems on both sides of the border, requiring immediate support from officials in both countries. Local first response teams on both sides of the border should be prepared to work together.

Although the United States continues to increase cooperation with other nations to prevent terrorist activity, it must do more to develop plans for responding to WMD events in border regions. Prevention and response, though related, are separate functions carried out on a local level largely by separate agencies.

Key Step #1. The President should direct his Administration to develop mutual terrorism response plans with Mexico and Canada. The President should first initiate discussions with Mexico and Canada to secure a commitment about cooperation on this issue. Discussions about the specific elements of cooperation should be conducted by representatives from OHS, the Departments of State, Justice, and Health and Human Services, and their counterparts from Canada or Mexico. Once an agreement in principle is established, State and Local first responders in border communities should be brought into the discussion to work through jurisdictional issues, to establish standards for responding to attacks, and to identify any interoperability problems that may arise.

Key Step #2. The Office of Homeland Security should establish and coordinate international, cross-border first-responder exercises. Once the agreements are in place, the North American neighbors should establish cooperative first-responder training exercises that allow hazardous materials crews, health professionals, firefighters, and law enforcement agencies from the border locales and states to prepare together. The exercises should help officials identify problems with interoperability of equipment, jurisdictional authority, or responses to CBRN events. The exercises should be conducted once a year.

PRIORITY #7: DEVELOP A NATIONWIDE EDUCATION AND PUBLIC RELATIONS PROGRAM.

Government at all levels should place a priority on effective public relations. The central theme of public relations strategy regarding civil defense should be that peace, security, and prosperity depend not on the few policies implemented after the September 11 attacks, but on long-term vigilance and a commitment to security. State and Local governments are primarily responsible for informing citizens about how they will respond to terrorism, how to prevent terrorism, how to respond

should prevention fail, and what the government is doing to protect citizens. They should inform the public truthfully but carefully to avoid causing paranoia. Citizens who understand that states are interdependent—a tragedy in one could become a tragedy for the entire region or nation—will undoubtedly support cooperation at all levels.

Disseminating information is central to being able to assure citizens that they are secure, especially during times of attack or increasing threats. Americans must be certain that their civil leaders and institutions are prepared to respond to CBRN attacks. Yet most State and Local governments do not have a comprehensive public relations strategy in place. A strategy to distribute information would help reassure the public that government is working to ensure public safety and educate them on how to improve their own safety.

Key Step #1. State and Local leaders should develop a CBRN public relations strategy.

Each governor should initiate an effort to establish a statewide public information effort on civil defense. He should call a meeting with the mayors from the largest cities to identify effective communications options and to consider developing additional capabilities. Participants also should determine the best way to distribute the information to the public, given the characteristics of their state. Efforts to educate the public about civil defense preparedness must be consistent, closely coordinated, and continually updated to reflect what the Local, State, and Federal governments are doing to achieve greater security.

Key Step #2. Governors should facilitate a cooperative relationship between local

governments and the media regarding an emergency response plan. The governor should request that each mayor meet with local news directors to develop a plan for television, radio, and newspaper cooperation with government during an emergency. Plans that are already in place should be reviewed and updated. Additionally, cable television distributors should be asked to establish and advertise a channel for disseminating public civil defense information, as needed.¹⁴

Key Step #3. Local leaders should use community newsletters to distribute information on CBRN preparedness and response plans.

Mayors should post on their city's Web sites, as well as in community newsletters, a column on security issues. The column should include information on what the government is doing to prepare for attacks as well as what citizens can do to protect themselves. The newsletter should be distributed door-to-door via flyer, e-mail, and regular mail. This redundancy is vital to ensure that all citizens see the information. Pamphlets and information cards updating what is being done should be distributed annually.

14. See chapter on Infrastructure.

CONCLUSION

The key to effective civil defense is preparation on the Local level. Local first responders will be called upon to deal with the consequences of terrorism using chemical, biological, radiologic, or nuclear weapons in the moments and hours after an attack. For that reason, Federal support for these first responders is vital.

The first priority for achieving a higher state of preparedness for civil defense is to build a nationwide surveillance network for early detection of a CBRN attack. The Federal government should appoint a task force charged with developing tools that help Local and State officials to prepare for an attack. These tools should include a checklist for terrorism response preparedness and a “war-game” exercise guide. These tools should enable authorities to identify where they are not adequately prepared. The Federal government also must accelerate the development of drugs to prevent or limit the spread of deadly diseases by terrorists.

A Train-the-Trainer program should be started to assemble a web of experts who can train others at the Local level to prepare for civil defense. This is the only way to affordably train the hundreds of thousands of first responders around the nation. The Federal government should simplify the process of obtaining assistance for State and Local civil defense initiatives. The United States should sign agreements with Canada and Mexico for mutual support in case of attacks in border communities. Finally, all levels of government must involve the public in preparing for a possible CBRN event.

These measures are simple solutions to very complicated problems. They build on existing capabilities but recognize that achieving true civil defense must be an ongoing process. These steps will create structures at the Local, State, and Federal levels for identifying current capabilities and weakness and help officials to prioritize spending. Most important, these priorities reflect the understanding that, although civil defense begins on the Local level, to protect the most Americans it must be guided and supported by the Federal government.

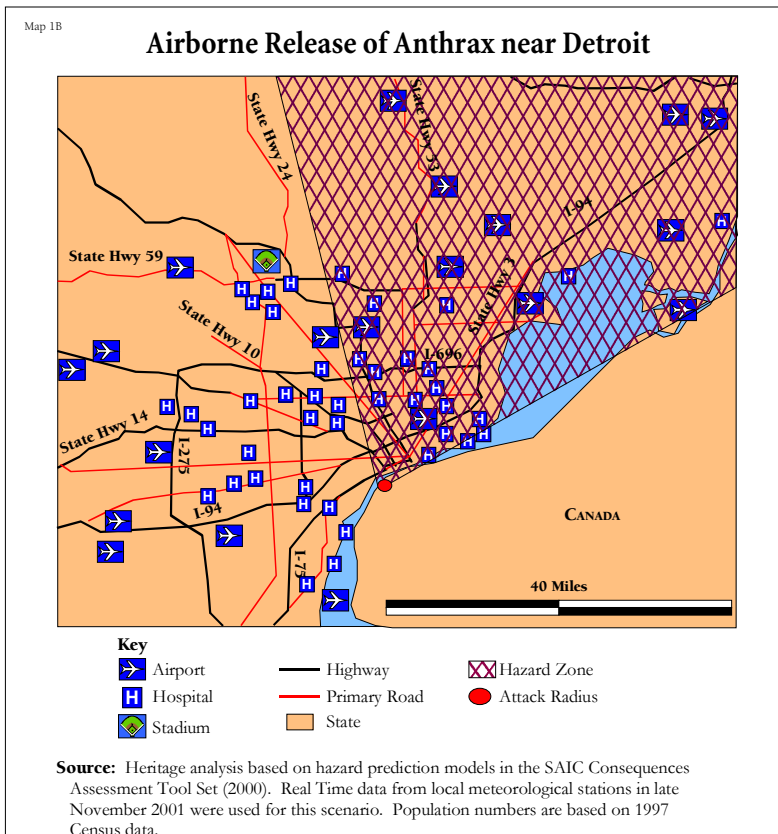
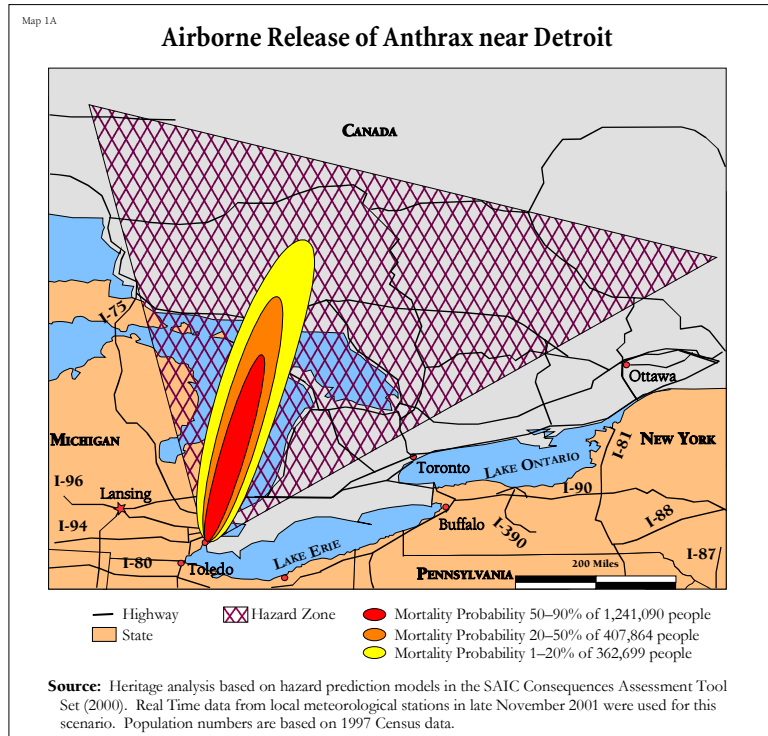
Table 4

Status of Key Unimplemented Prior Commission Recommendations for Civil Defense Against Weapons of Mass Destruction

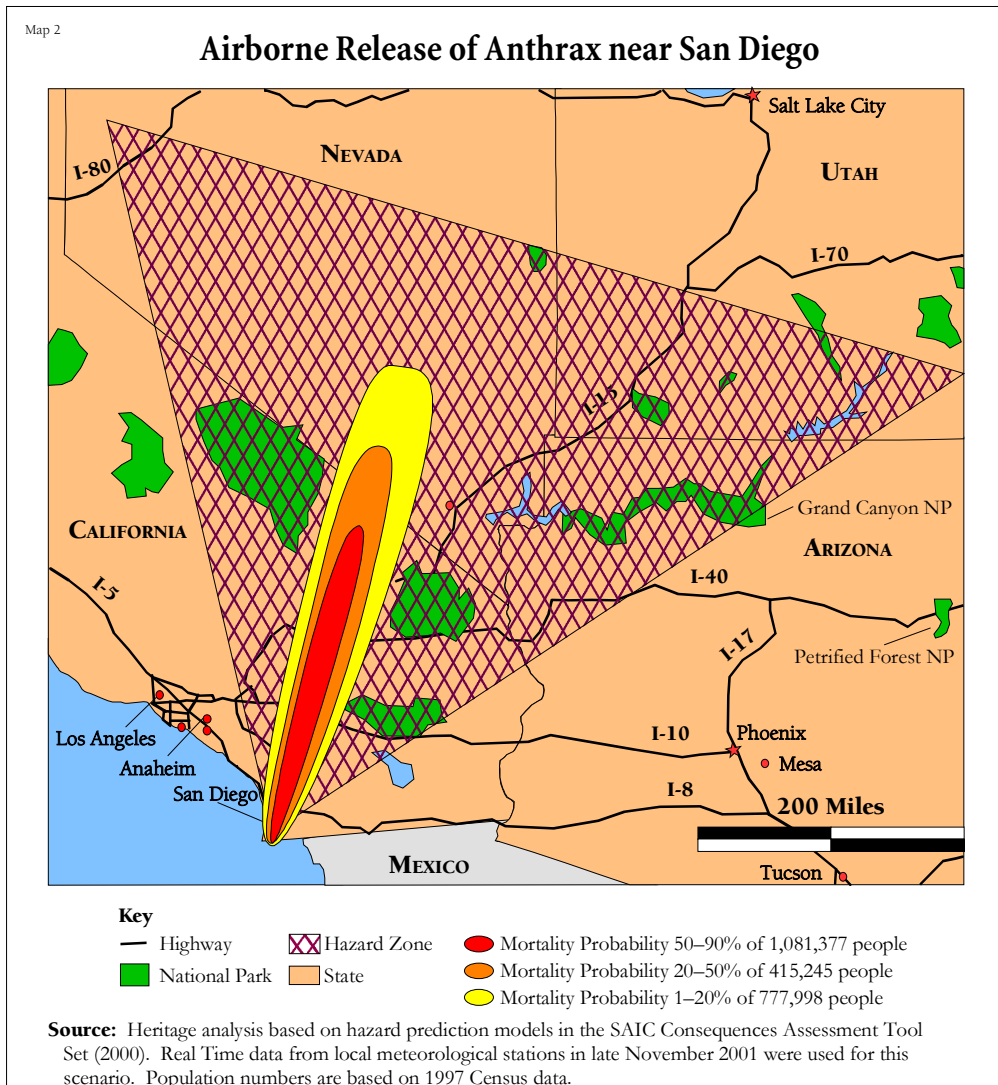
Recommendation	Commission/Report	Status of Implementation
Medicines and Vaccines. Increase funding for R&D and stockpiling of medicines and vaccines.	Bremer Commission Gilmore Commission Defense Science Board CSIS Reports	On October 17, 2001, HHS requested \$1.5 billion more in funding for pharmaceutical stockpiles, rapid response systems, additional expert epidemiology teams, medical emergency bioterrorism responses, and early detection surveillance. Although authorizing legislation has not been passed, HHS has issued contracts to produce 209 million doses of smallpox vaccine. Additionally, on December 10, 2001, the FDA issued new guidelines for a drug called potassium iodide, which counters the effect of radioactive fallout.
Training. Enhance training, exercise opportunities, and equipment for state and local first responders.	Bremer Commission Gilmore Commission Defense Science Board CSIS Reports	HHS requested \$88 million to expand its capacity to respond to bioterrorist attacks, which includes \$20 million for CDC's Rapid Response and Advance Technology labs; \$20 million for mobile epidemiology teams; \$50 million for the Metropolitan Medical Response System; and \$50 million for hospitals and emergency departments to prepare for mass immunizations, which includes \$10 million to augment state and local training. Authorizing legislation has not been passed.
Surveillance. Create a national CBRN surveillance and emergency communications capacity.	Defense Science Board CSIS Reports Bremer Commission	HHS proposal also includes \$40 million to support early detection surveillance, including Web-based notification of the national health community. Authorizing legislation has not been passed.
Cooperation. Facilitate Local, State, and Federal planning, training, and response.	Bremer Commission Gilmore Commission CSIS Reports	HHS proposal includes \$50 million to strengthen the Metropolitan Medical Response System and \$10 million to augment state and local preparedness through extensive training. Authorizing legislation has not been passed.
National Guard. Change the focus of the National Guard.	Bremer Commission Hart–Rudman Comm. CSIS Reports	The Quadrennial Defense Review recommended putting more emphasis on the role of the National Guard in homeland defense. Not yet implemented by the Department of Defense.
Guidelines and Standards. Create national guidelines and standards for prevention, preparedness, and response	Bremer Commission Gilmore Commission CSIS Reports	No standards or uniform national guidelines for bioterrorism preparedness and response are in place at this time. No vehicle recommends establishing specific guidelines.
Threat Assessment. Establish an ongoing threat and vulnerability assessment for homeland security.	Bremer Commission Defense Science Board CSIS Reports	No action has yet been taken to establish a system for ongoing threat assessment.

Note: For information on these reports, see the bibliography.

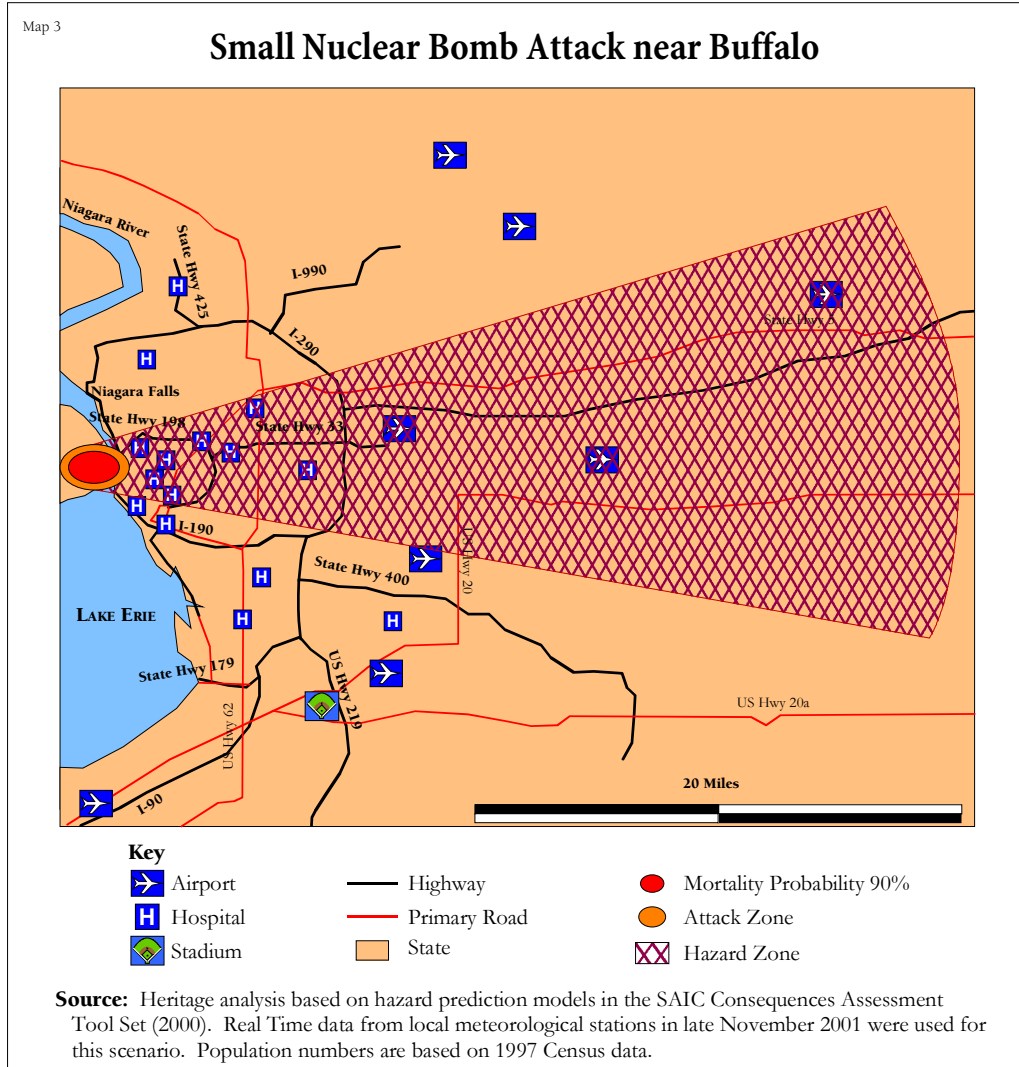
Scenario #1— Airborne Release of Anthrax near Detroit. Rather than risk being caught smuggling anthrax over the border, three al-Qaeda operatives in Canada, across the river from Detroit, decide to release some highly refined, weapons-grade anthrax that they obtained while in Iraq. With the United States on high alert, they find a Canadian agency



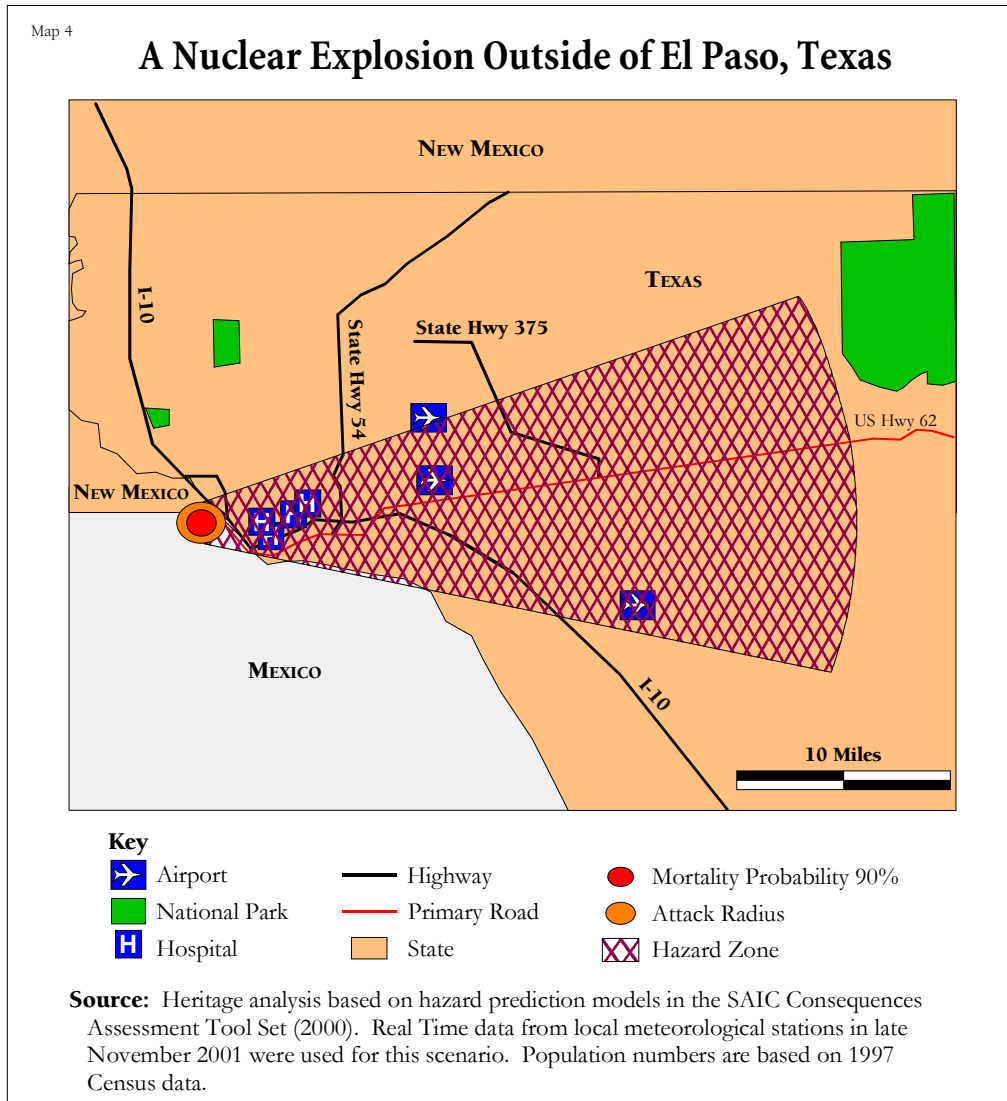
that gives helicopter tours over the Great Lakes region. As the helicopter passes its nearest point to Detroit, the terrorists subdue the pilot, open the door, and release 250 pounds of finely milled anthrax spores, which they had concealed under their clothes in bags taped to their bodies, at around 1,000 feet altitude. They crash the helicopter; no one is aware that the anthrax had been released. Maps 1A and 1B shows the devastating results after just 24 hours, with prevailing wind conditions.



Scenario #2—Airborne Release of Anthrax near San Diego. A group of terrorists in Mexico with ties to international drug smugglers in Colombia decides to use anthrax to disrupt U.S. counternarcotics operations along the border. By cover of night, the group sails a vessel off the coast of San Diego, from which it launches a radio-operated plane scaled to one-third the size of a small propeller plane, and fly it to an altitude of 1,000 feet. Because of its small frame and low altitude, the plane does not appear on radar. Within minutes, the group sets off a series of small detonators that break up the plane, deploying 250 pounds of weapons-grade anthrax spores. The terrorists, undetected, sail back to Mexico. A Southwest wind scatters the anthrax over San Diego and on to Las Vegas. Within two days, hundreds of people with flu-like symptoms crowd hospitals around San Diego. Cases appear in Las Vegas. Panic ensues as experts admit they cannot determine the origin or the scale of the attack. Map 2 shows the effects after just 24 hours, with prevailing winds.



Scenario #3—Small Nuclear Bomb Attack near Buffalo. After successfully obtaining an old Soviet suitcase nuclear weapon on the black market, a terrorist smuggles it into Canada. He secures a job as a mechanic for a local tourist company that offers day bus tours from Toronto to Buffalo. He rigs the small 3 kiloton nuclear bomb underneath a bus, but neglects to consider that one of the roads it will travel is being repaved. The bomb, as powerful as 3,000 tons of dynamite, detonates prematurely. Everything at the epicenter is vaporized by temperatures reaching millions of degrees Fahrenheit. Outside the center, casualties result from severe burns, radiation, and flying debris caused by collapsed buildings. Northeast winds spread the radiation rapidly. Americans for hundreds of miles try to flee, causing mass panic. Looters raid grocery stores and gun shops. Air traffic control systems are severely degraded. Officials cannot ascertain whether this was a single attack or a precursor to multiple attacks. The National Guard is called in. Map 3 shows the effects after 24 hours.



Scenario #4—A Nuclear Explosion Outside of El Paso, Texas. After purchasing an old Soviet suitcase nuclear weapon in Central Asia, a terrorist smuggles it into Mexico to detonate it near the U.S. border. Traveling by car, the suicide bomber makes his way to El Paso. Ten miles outside the Eagle Pass port of entry, he pulls into the vehicle inspection line and detonates a 3 kiloton nuclear bomb, equivalent to 3,000 tons of dynamite. El Paso is devastated, even though the bomb exploded on the other side of the border. At the center of the blast, everything is vaporized by temperatures reaching millions of degrees Fahrenheit. Casualties outside the center include severe burns, radiation, and multiple injuries from the flying debris of collapsed buildings. Prevailing winds from the Southwest send the radiation up to San Antonio. Authorities do not know whether this was a single attack or the precursor to other attacks. All major cities are evacuated and air traffic control systems are severely degraded. Mass hysteria and looting forces the Federal government to activate the National Guard and establish martial law. Map 4 shows the effects after 24 hours.

TOP PRIORITIES FOR IMPROVING INTELLIGENCE AND LAW ENFORCEMENT CAPABILITIES

A Report of the Working Group on Intelligence and Law Enforcement¹

Daniel W. Fisk, Working Group Rapporteur

Since the deadly terrorist attacks on America on September 11, questions have intensified about the ability of government agencies to gather and communicate actionable intelligence. Federal, State, and Local officials widely recognize that more resources must be focused on improving intelligence so that all levels of government, including emergency and first responders, can more effectively deter, stop, apprehend, and respond to those who would harm Americans.

-
1. The Working Group on Intelligence and Law Enforcement includes Louis Dupart, Esq., Partner, Fleischman & Walsh, Washington, D.C.; Carmel Fisk, former Minority Counsel, Subcommittee on International Law, Immigration, and Refugees, Committee on the Judiciary, U.S. House of Representatives; Thomas Frazier, President, The Frazier Group, Baltimore, Md., former Chief of Police, Baltimore, Md.; Major General Bob Harding, USA (Ret.), Executive Vice President for Operations, Innovative Logistics Techniques, Inc., McLean, Va.; Alvin James, Anti-Money-Laundering Practice Leader, Ernest & Young; Dr. Mark M. Lowenthal, SRA International, Inc., Fairfax, Va.; N. John MacGaffin III, President, MacGaffin & Miller, Inc., Washington, D.C.; Ambassador David C. Miller, Jr., Chairman, MacGaffin & Miller, Inc., Washington, D.C.; Dr. William J. Olson, Minority Staff Director, International Narcotics Control Caucus, U.S. Senate; and The Honorable Robert S. Warshaw, Warshaw & Associates, Inc., Sylva, N.C., former Chief of Police, Rochester, N.Y. The following individuals also contributed to elements of this report in an advisory capacity: Christopher Barton, Chief Counsel, Permanent Select Committee on Intelligence, U.S. House of Representatives; the Honorable Edward J. Derwinski, former senior member of the House Committee on Foreign Affairs; Robert Filippone, Deputy Chief of Staff, Select Committee on Intelligence, U.S. Senate; John Mackey, Investigative Counsel, Committee on International Relations, U.S. House of Representatives; David A. Martin, Doherty Professor of Law, University of Virginia, and former General Counsel, Immigration and Naturalization Service; David Muhlhausen, Policy Analyst, Center for Data Analysis, The Heritage Foundation; and Robert Rector, Senior Research Fellow, The Heritage Foundation.

The capabilities of and relationships between law enforcement agencies (LEAs) and the Intelligence Community have received sustained attention over the past few years, including a comprehensive review in 1995 by the House Permanent Select Committee on Intelligence and its report, *Intelligence Community in the 21st Century*; the 1996 Brown–Rudman Commission; and more recent reviews by the Hart–Rudman, Bremer, and Gilmore Commissions.² Many of the excellent recommendations made by these commissions and studies have yet to be fully implemented, though after September 11, the Administration and Congress sought to address some of the bureaucratic problems exposed by the attacks in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (P.L. 107–56) and the FY 2002 Intelligence Authorization Act (P.L. 107–108).

Indeed, September 11 sent a powerful message to decision-makers that much more needs to be done to protect the homeland, and quickly. They now recognize that no single action, law, or institution—no one-step remedy—can possibly combat all of the threats facing the United States and its citizens. A multifaceted approach to homeland security is necessary. Building on the recommendations of earlier commissions and post-September 11 legislative efforts, the Working Group on Intelligence and Law Enforcement has identified the top priorities for improving the ability of both law enforcement agencies across America and the Intelligence Community to protect the American people from terrorist attacks.

- **Priority #1: Require the Office of Homeland Security to direct the assessment of threats to critical assets nationwide.** Since September 11, a number of State and Local governments, along with various Federal government agencies, have begun to develop their own vulnerability assessments. This is an important step in helping government officials determine what homeland assets critical to the nation's economy and security are vulnerable and whether the responsible agencies and institutions are organized and equipped to protect them. A first step in this process should be the development of a uniform methodology for assessing the risk and the threat to vulnerable targets.
- **Priority #2: Rapidly improve information-gathering capabilities at all levels of government.** For Federal, State, and Local LEAs, a first line of defense against terrorism and other threats to the homeland is access to timely, reliable, and actionable information from both foreign and domestic sources. Rapidly enhancing government's ability to acquire and analyze this information is vital to homeland security.

2. The status of recommendations made by previous commissions and studies that remain unimplemented may be found in the table at the end of this chapter. The status of post-September 11 legislative efforts may be found in the Appendix.

- **Priority #3: Improve intelligence and information sharing among all levels of government with homeland security responsibilities.** The need for better sharing and dissemination of information to all levels of government was starkly evident in the aftermath of September 11. Improved LEA–Intelligence Community cooperation has far more to do with changing bureaucratic cultures than revising statutes or regulations. Creating an all-source information fusion center and a cooperative structure for the sharing of information collected is critical to an effective homeland security policy.
- **Priority #4: Strengthen the visa approval and border security mechanisms.** The first line of defense against terrorists today often involves a determination by a consular officer or Immigration and Naturalization Service (INS) inspector that an alien should or should not be allowed to enter the United States. Legally entering the United States was remarkably easy for the September 11 terrorists. The visa approval and entry–exit processes must be strengthened, as should the ability of LEAs to enforce existing immigration laws against aliens who are in violation of those and other laws. Consular officers must have more information upon which to make a visa decision. At the same time, the Secretary of State should leverage the approval of a waiver as permitted by the Visa Waiver Program to enhance the anti-terrorism cooperation of other countries. Mechanisms to enforce immigration laws against aliens who violate the terms of their visas or who enter the country without inspection also should be strengthened.
- **Priority #5: Reduce the opportunities for identity theft and fraud in state identity document systems.** False documents continue to be a major problem, and the terrorists involved in the September 11 attacks showed that they will exploit those States with systems most liable to fraud. Any State that continues to run a document system subject to fraud and abuse places the lives of all Americans in jeopardy. Current procedures for the issuance of identity documents, including driver’s licenses, birth certificates, and death certificates, must be tightened and a mechanism developed to deter and prevent identity theft.
- **Priority #6: Create a mechanism to monitor recent anti–money-laundering initiatives to obstruct the financing of terrorism.** Many of the deficiencies in pre-September 11 efforts to obstruct the financing of terrorist activities were addressed in the PATRIOT Act. But the financial services area is dynamic, and those who seek to harm the United States will continue to attempt to circumvent the regulatory structures currently established. To anticipate how those who would threaten the United States could skirt the existing anti–money-laundering restrictions, the Secretary of the Treasury should create a mechanism to evaluate how current laws could be circumvented.

PRIORITY #1: REQUIRE THE OFFICE OF HOMELAND SECURITY TO DIRECT AN ASSESSMENT OF THREATS TO CRITICAL ASSETS NATIONWIDE.

Since September 11, Federal, State, and Local governments have intensified efforts to identify vulnerable assets within their respective jurisdictions. These useful exercises will not necessarily be uniform in their methodology or compiled in one accessible database so that jurisdictions with overlapping responsibilities could coordinate their homeland security policies. Recognizing that not all potential targets can be protected at all times, a nationwide threat assessment of potential critical targets would provide a database to policymakers, first responders, and other agencies and officials with responsibility for homeland defense to facilitate protection and early warning by prioritizing what needs to be protected, under what circumstances, and by whom. This assessment should be matched with intelligence on the capabilities of those who would seek to harm the United States.

Key Step #1. The Director of the Office of Homeland Security (OHS) should establish the methodology for conducting Federal, State, and Local threat assessments to ensure general uniformity of findings. The Director of the OHS should establish the methodology that government entities will follow in assessing risks to people and infrastructure in their jurisdictions to ensure the compatibility of the information transmitted to OHS. To avoid compounding an already complicated coordination system, the basic format of these assessments should have the following elements:

Identify the Critical Targets. To be able to respond appropriately when a national alert about terrorism is announced, government officials with homeland security responsibilities, working with other relevant agencies and private entities, must first identify the critical targets within their jurisdictions that are or could be at risk, such as communication, utility, and transportation nodes and facilities; emergency-response facilities, bridges, and tunnels; and targets with significant political or symbolic value, such as national monuments and certain government buildings.

Assess the Threat. Next, relevant government entities should assess the threat to each critical target that has been identified. This assessment should include:

1. The type of threat or threats to each critical infrastructure (for example, explosives, cyberterrorism, biological or chemical attack, or a combination of these types). Since the nature of the threat is dynamic, the process of threat assessment must be continuous. In addition to actual targets, the assessment should include an inventory of facilities that could be used to develop chemical and biological agents and the sources of supply for such facilities, existing as well as potential.

2. The level of threat or the probability of attack on each target. Some facilities are likely targets at all times; others are at variable risk depending on the circumstances.
3. Potential threats from people or groups in a given area, including changes in demographics or patterns of behavior of groups that may threaten homeland security (such as an increase in activity by gangs with state or national reach). This assessment should identify which assets these individuals or groups are likely to target and whether agencies in the area have the ability to identify those groups.

Track the Materials Sought by Terrorists. Finally, a system should be developed to track the flow and supply of sensitive materials critical to the development and manufacture of chemical or biological agents and radioactive devices.³

Key Step #2. The OHS Director should establish a national strategy to protect the homeland based on the national assessments. A national strategy for homeland defense must include prevention (requiring both detection and deterrence); preparedness; crisis management; and consequence management. Before a national strategy can be finalized and resources allocated effectively, however, critical assets identified in the national assessments must be prioritized according to three fundamental characteristics: the potential for loss of life if attacked, the impact an attack would have on the economy, and the ability of the nation to function both domestically and internationally. Additional elements of the strategy should include how agencies should respond and who should be designated as points of contact should an emergency occur.

Recent legislation requires the President to designate a senior Department of Justice (DOJ) official as the coordinator for all Justice Department activities to combat domestic terrorism, including State and Local grant programs.⁴ It is expected that this position will be the Deputy Attorney General for Combating Terrorism. This statutory requirement effectively makes the DOJ the most significant agency for Federal homeland security efforts within the United States and will necessitate that the OHS Director coordinate the development of the national strategy with the Department of Justice.

Key Step #3. The Office of Homeland Security should develop a national alert and warning system. The President should direct the OHS Director, working with Federal agencies and State and Local governments, to develop a warning system for threats to the homeland. Such a system should specify the methods of communica-

3. For a discussion of the development of an early warning system to detect chemical, biological, or other attacks, see Priority #1 in the chapter on Civil Defense.

4. As required by Section 612 of Public Law No. 107-77.

tion and provide a threat assessment based on a grading system similar to the Defense Readiness Conditions (DEFCON) system used by the U.S. Department of Defense (DOD). The DEFCON system ranks threats based on the severity of the situation at hand (DEFCON 1 to DEFCON 5). Military commanders are required to take certain actions with each DEFCON warning level.

A similar system for homeland defense would help avoid miscommunications about threats. Threat levels should be assigned by determining, at a minimum, the apparent imminence of the threat and the credibility of the source. Other factors should be considered as deemed necessary by the OHS Director.

Warnings should be disseminated geographically. Only States or regions in danger should be warned of an impending attack. There is no reason to have the entire country at a high state of alert if information narrows the geographic scope of where an attack could occur. Nationwide warnings should be issued only when intelligence is credible that an attack is imminent but the potential targets are numerous or non-specific. For example, the threat may be to a nuclear power plant, but the intelligence does not specify which one.

The program should be managed by the OHS through an interagency command-and-control center similar to the one created to handle the “Year 2000” (Y2K) threat to computers and computerized systems. The OHS Director should be responsible for determining the threat level and communicating it to lead agencies and governors. Governors should be responsible for sharing that information, not only with the Commander of the State’s National Guard and the emergency services department head, but also with Local officials, the public, and private industry, as appropriate. Lead agencies should be responsible for communicating the threat level to the private sector when conditions warrant.

PRIORITY #2: RAPIDLY IMPROVE INFORMATION-GATHERING CAPABILITIES AT ALL LEVELS OF GOVERNMENT.

The Second Gilmore Commission report, issued in December 2000, noted that “‘foreign’ terrorism and ‘domestic’ terrorism may not be easily distinguished.” This conclusion was dramatically and tragically proved accurate on September 11. Acquiring reliable, timely, and actionable intelligence is the first line of defense against future acts of terrorism.

Key Step #1. The President should direct the OHS Director to establish a national intelligence coordinating group to develop a national intelligence strategy, including the establishment of resource allocation and targeting priorities. The OHS Director should establish a Homeland Security Intelligence Coordinating

Group (HSICG) at the Assistant Secretary level for this purpose. Disputes about policy or operations should be referred to a Deputy-level committee, a procedure currently used for the resolution of interagency disputes on other national security issues. The HSICG should be chaired by OHS and include representatives from the U.S. Departments of State, Defense, Justice, Treasury, and Transportation, and the Intelligence Community. The OHS Director should work with the Director of Central Intelligence (DCI) to ensure that a strategy exists to integrate homeland security intelligence into the work of the existing interagency mechanisms to determine targeting priorities.

In addition, to ensure adequate input from State and Local agencies, designees with security clearances from the following groups should be invited to participate on a regular basis: the International Association of Chiefs of Police, the National Sheriffs Association, and, as appropriate, other police executive organizations. On a case-by-case basis, designees with security clearance should also be invited to participate from the National Governors' Association, the U.S. Conference of Mayors, the National League of Cities, the National Association of Counties, and the International City Managers Association. The initial intelligence-sharing strategy should be finalized within 90 days of the first HSICG meeting.

Key Step #2. The Administration should strengthen foreign intelligence–collection capabilities. Recent legislation requires the DCI to lift the guidelines which hinder the recruitment of foreign agents (Section 403 of the Intelligence Authorization Act for Fiscal Year 2002). While this reform is an essential step to increasing foreign intelligence, other steps need to be taken:

Recruitment of More Officers with Non-Official Cover. To re-energize the Central Intelligence Agency's Non-Official Cover (NOC) program, the DCI should direct the recruitment of officials willing to operate under non-official cover, a group that offers the CIA a unique capability for gathering intelligence. This program has suffered from bias from full-time Directorate of Operations (DO) officers and from a lack of sustained funding. More officers who are willing to pursue this career path should be recruited, and the resources needed to sustain a vigorous NOC program should be provided.

Recruitment of Officers for the Directorate of Operations. The DCI should accelerate the recruitment of CIA DO officers who have diverse, multiethnic, multilingual backgrounds. The primary threat to the American people today is from more diverse peoples and groups from more regions than during the Cold War struggle against the Soviet Union.

Development of Foreign Liaison Relationships. The development of liaison relationships between U.S. and foreign LEAs should be enhanced through the International Law Enforcement Academy (ILEA) program. ILEAs now exist in

Thailand, for Southeast Asia, and Hungary for training for law enforcement officials from Eastern and Central Europe. An ILEA will open shortly in the United Arab Emirates (UAE) to train law enforcement officials from the Middle East.

Key Step #3. The Administration should increase the sources of domestic information available to Federal agencies with homeland defense responsibilities. Cabinet Secretaries with law enforcement responsibilities should hold LEA officials accountable for both the quality of their intelligence collection and their ability to collect evidence to develop a case for prosecution. The Attorney General should direct the Director of the Federal Bureau of Investigation (FBI) and the Administrator of the Drug Enforcement Administration (DEA) to measure and rate their Special Agents in Charge (SACs), and make promotion decisions, based on the SACs' ability to collect intelligence equal to making cases. The Secretary of the Treasury should do the same for law enforcement entities under his control, and the Secretary of Transportation should do the same for the U.S. Coast Guard.

Key Step #4. State and Local LEAs should enhance information-collection efforts. An effective homeland security structure must capitalize on the presence and potential of State and Local law enforcement agencies and personnel. The involvement of approximately 17,000 state and local police departments⁵ is critical to a comprehensive homeland defense effort. "Community policing" offers a valuable potential for citizen involvement in homeland defense and for information gathering.

Re-establish State and Local LEA intelligence units. State and Local governments should re-establish LEA intelligence units, many of which were abolished in the 1970s following allegations of police harassment of certain groups. The U.S. Attorney General and State Attorneys General should establish frameworks for dealing with documented sustained abuses.

Enhance Citizen Cooperation in Local Efforts. Local police departments should include citizens' assessments of local threats and vulnerabilities through the Police–Citizen Interaction Committee (PCIC) mechanism—a formal platform for regular precinct-level meetings with citizens to discuss problems and solutions of interest to the community. Implementing community policing tactics, like PCICs, should not require federal funding.

Regular Assessments of Local Threat Sources. The Attorney General—through the FBI Director and the relevant SAC or U.S. Attorney—should request State and Local LEAs to submit annual assessments of the events, activities, or changes in demographics or patterns of behavior of groups in their jurisdiction (for example,

5. U.S. Department of Justice, Federal Bureau of Investigation, *Crime in the United States 2000: Uniform Crime Reports*, p. 1.

an increase in activity by gangs with state or national reach) that may threaten homeland security.

Key Step #5. The DCI and Secretary of Defense should direct the strengthening of measurement and signature intelligence (MASINT) capabilities. MASINT (and biometrics) by nature is a security discipline. It detects, identifies, and—most important—can be used to verify data from other intelligence sources. Its systems, for example, detect disturbances of earth (tunnels) and differences in gradient and ambient temperatures (spotting people and things, differentiating between “real” and “fake,” etc.). MASINT is perfectly designed to assist against any number of asymmetric threats; it is already in use for many important conventional aspects of the war against terrorism.

MASINT must be integrated into intelligence systems to alert or trigger intelligence-collection platforms or sensors (known as “cueing” and “cross-cueing”) for the targeting of other intelligence platforms and assets. Although this process has started at the Defense Intelligence Agency (DIA), it is in its infancy and is not getting the attention it deserves from DOD. The Defense Department is primarily treating MASINT and biometrics as an “information-automation-technology” discipline, having assigned as executive agent for MASINT the U.S. Army under the Director for Information, Systems, Command, Control, Communications, and Computers (DISC4).

Key Step #6. The DCI and Secretary of Defense should maximize the capabilities of DOD’s Information Dominance Center (IDC) for the near term, and explore merging it into the CIA Counter Terrorism Center (CTC) in the long term. The IDC (formerly called the Land Information Warfare Activity) at Fort Belvoir, Virginia, already performs the automated data-mining and cross-cueing of intelligence from the CIA, the National Security Agency (NSA), the Defense HUMINT Service (DHS), the National Imagery and Mapping Agency (NIMA), and the Counter-Intelligence Analysis Center. The Counter Terrorism Center (CTC), based in the CIA Directorate of Operations, focuses primarily on analyzing CIA DO–collected HUMINT. In the near term, retraining CTC analysts or reorienting the CTC mission to handle the work of the IDC is unnecessary. Under present circumstances, the IDC and the CTC should continue their operations and do what they do best. Over the longer term, the DCI and Secretary of Defense, working with the relevant congressional committees, should review the possible folding of the IDC into the CTC to form an all-source Intelligence Community intelligence center.

PRIORITY #3: IMPROVE INTELLIGENCE AND INFORMATION-SHARING AMONG ALL LEVELS OF GOVERNMENT WITH HOMELAND SECURITY RESPONSIBILITIES.

The Second Gilmore Commission report emphasized that “more can and must be done to provide timely information—up, down, and laterally, at all levels of government—to those who need the information to provide effective deterrence, interdiction, protection, or response to potential threats.” The critical element of improved law enforcement–Intelligence Community cooperation has more to do with changing bureaucratic cultures than revising statutes or regulations.

Key Step #1. The OHS Director, working with relevant Cabinet officials, should create a Federal-level fusion center for collecting intelligence and law enforcement information. The President should direct the OHS Director, working with the Attorney General, the Secretary of the Treasury, the Secretary of Transportation, and the DCI, to create an all-source Federal-level information fusion center to which all information relevant to homeland defense is sent and from which information can be accessed by Federal agencies, and State and Local LEAs with homeland defense responsibilities, as required on a need-to-know basis.

Key Step #2. The OHS Director should create a structure for sharing and disseminating information among Federal, State, and Local agencies. The OHS Director, through the new Homeland Security Intelligence Coordinating Group, should develop a mechanism for sharing and disseminating information among government agencies.

Cooperative Structure. The OHS Director and HSICG should review the structure developed for Federal-State-Local cooperation in counternarcotics efforts. Both the High-Intensity Drug Trafficking Area (HIDTA) Program and the Justice Department’s Organized Crime Drug Enforcement Task Force (OCDETF) provide models for cross-government information sharing regarding terrorism-related threats to the homeland. The HSICG should explore the reconfiguration and expansion of the HIDTA Program into a “Drugs and Domestic Preparedness” structure, while remaining sensitive to the efficacy of this program in addressing the illegal drug problem and without deflecting the focus of the HIDTA program and the OCDETF mechanism away from combating the illegal drug trade.

As currently implemented, the HIDTA provides enhanced coordination and joint efforts among Federal, State and Local LEAs in order to reduce drug trafficking in critical regions of the United States. HIDTA provides a coordination umbrella for Federal, State, and Local law enforcement anti-drug efforts through an

outcome-focused, strategy-driven approach developed collectively by LEAs in the HIDTA region.

Background Checks. Each State and Territorial governor (56 jurisdictions) should designate the senior official responsible for homeland security within that specific jurisdiction to be cleared for security information on a need-to-know basis. This official should be cleared by the FBI Director and DCI for access, as required or needed, to national security information and as the principal point of contact between State and Local LEAs and Federal agencies. Under current law, both the CIA and FBI Directors have the authority to grant a security clearance for access to classified information based on national security needs. In some circumstances, the Director of the CIA or FBI, respectively, in coordination with the governor and mayor, may determine that a senior city official should also be granted a security clearance. Determinations of the need and extent of security clearances for State, Local, and Territorial officials should be reviewed on a routine basis.

Federal Liaison. The Director of OHS and the Attorney General each should appoint a senior official with both Federal and State or Local LEA experience as liaison and point of contact for State and Local officials and Federal agencies involved in homeland security. The Justice Department's Office of Domestic Policy (in the Office of Justice Programs) provides funding to State and Local agencies for training, equipment, and exercises. This office provides a basis for a liaison mechanism within the Department of Justice; however, there remains value in designating a senior Justice official who has direct communication with the Attorney General as a liaison for State and Local agencies. Further, the State and Local Advisory Group (SLAG) that had been established to advise the Attorney General should be resurrected to advise both the Attorney General and the OHS Director on how the Federal government can be more responsive to State and Local first-response agencies. The SLAG could be an important basis for creating grassroots support for homeland defense initiatives.

Handling National Security Information. To further facilitate the sharing of information, in selected instances, the Attorney General or Secretary of the Treasury, as required, should delegate authority to the SAC of the relevant Federal agency to deputize State and/or Local law enforcement officials as Special U.S. Marshals to handle classified information. The designation of these officers or units should be done in consultation, as required, with the appropriate governor, mayor, and state or metropolitan police chief. The FBI uses this arrangement in conducting investigations under its Violent Crime Task Force structure.

Key Step #3. Federal officials should increase support for State and Local LEA information efforts. An essential objective of any homeland defense strategy must include initiatives to bolster the preparedness of State and Local governments, especially

LEAs and other first responders, and to reassure the public that State and Local authorities can function separate and apart from the federal umbrella, even as they horizontally cooperate with their federal colleagues.

Funding Support. Congress, in recently enacted appropriations, has bolstered funding for the Justice Department's Office of Domestic Preparedness (ODP) to train State and Local agencies to prepare for terrorist actions and to equip specially designed State and Local units to cooperate with Federal agencies on homeland security operations. To help ensure that funding is not wasted, the ODP should (1) set minimum standards for preparedness for States and localities receiving federal assistance and (2) evaluate their performance. If States and localities do not meet the minimum standards, their federal assistance should be discontinued. Funding for equipment can be established as a matching grant program.

Training Support. The Attorney General should direct the FBI Director to implement a core course curriculum on terrorism at the FBI's National Academy at Quantico and the National Executive Institute for State and Local officials. The PATRIOT Act (Section 908) requires the Attorney General, in consultation with the DCI, to provide appropriate training to State and Local officials "who encounter, or may encounter in the course of a terrorist event, foreign intelligence in the performance of their duties." The Attorney General and Director of the FBI should provide instruction for these State and Local officials in the handling of classified and other national security material through the existing Regional Community Policing Institute structure in place in 30 localities.

PRIORITY #4: STRENGTHEN THE VISA APPROVAL PROCESS AND BORDER SECURITY MECHANISMS.

All of the 19 terrorists who organized and implemented the September 11 hijackings and attacks in New York and Washington entered the United States legally, having been approved for visas by U.S. consular officials and permitted entry by INS inspectors. However, some of these terrorists remained in the United States illegally after their visas had expired. The lack of timely, all-source intelligence for the vetting of visa applicants, the general ease of obtaining a visa, and the limited resources for dealing with those who violate the terms of their visa combined to give the terrorists an advantage in gaining access to the United States.

The Department of State (Bureau of Consular Affairs), the INS, and the U.S. Customs Service (USCS) play critical roles in determining who and what enters the United States. September 11 illustrated that the U.S. government has limited capacity to separate and distinguish legitimate travelers from those who may have the goal of attacking the American people. The steps that must be taken to

strengthen the visa approval system and entry–exit mechanisms and to ensure that overstays are reduced include the following.

STRENGTHENING THE VISA APPROVAL PROCESS AND ENTRY–EXIT VERIFICATION MECHANISMS

Key Step #1. The President, through the OHS Director, should mandate the creation of a comprehensive, Federal-level lookout database accessible to officials involved in border security. Decisions made by consulates and the INS are only as good as the information available to their officers. One can expect those with beliefs inimical to the United States to hide their true beliefs, associations, and intended actions to help them gain entry to the country.

The recently approved USA PATRIOT Act does not ensure the sharing of data by all agencies with information that may be relevant to visa/entry decisions. Many Intelligence Community agencies with relevant information and the agencies under the authority of the Secretary of the Treasury (such as the U.S. Customs Service and the Internal Revenue Service) and under the Secretary of Transportation (such as the U.S. Coast Guard) are not required to share information with those responsible for making consular decisions.

The PATRIOT Act (Section 403) mandates that the Attorney General and FBI Director provide the State Department (Consular Affairs) “access to the criminal history record information contained in the National Crime Information Center’s Interstate Identification Index (NCIC–III), the Wanted Persons File, and to any other files maintained by the National Crime Information Center...” Before enactment of the PATRIOT Act, there was some sharing of information among the State Department, the INS, Customs, and the DEA, but the information exchange was not comprehensive. The creation of a comprehensive lookout database is essential to preventing potential terrorists from entering the United States.

Key Step #2. Congress should repeal the requirement that INS inspectors clear passengers on international flights within 45 minutes of each flight’s arrival. Before September 11, airlines had complained about long waits for inspections at international ports of entry at airports, such as New York’s JFK and those in Newark and Miami. Instead of finding a way to spread the arrival times of international flights, the airline and travel industry lobbied Congress to require that “adequate” inspections to clear international flights through the primary point of inspection be accomplished within 45 minutes of arrival. Congress should repeal this “45-minute” rule (Section 286[g] of the Immigration and Naturalization Act, or INA).

Key Step #3. Congress should amend the Visa Waiver Program. Congress should amend the Visa Waiver Program (8 U.S.C. 1187) to:

1. Make aliens from countries designated as “not fully cooperating with U.S. antiterrorism efforts” ineligible for the Visa Waiver Program, which permits citizens of qualifying countries to travel to the United States for tourism or business for 90 days without obtaining a U.S. visa;
2. Deny participation in the program to those countries that do not have adequate controls over their own official identity and travel documents, including passports; and
3. Require that all countries that want to remain in the Visa Waiver Program upgrade their passport systems to include a digitized, machine-readable fingerprint and a facial photo and provide an electronic database to the INS, so that the identity of the alien passport holder can be verified by an INS inspector at a port of entry.

Key Step #4. The Secretary of State should accelerate the development and deployment of technology for biometric travel documents for aliens and U.S. citizens. The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA, P.L. 104-208), the Immigration and Naturalization Service Data Management Improvement Act of 2000 (P.L. 106-15), and the PATRIOT Act of 2001 (P.L. 107-56) all contain provisions regarding the upgrading of technologies to produce and/or read biometric travel documents—visas for aliens and passports for U.S. citizens. The Secretary of State should direct the Assistant Secretary of State for Consular Affairs to expedite the development and issuance of a new tamper-proof and fraud-proof U.S. passport and visa system to deter and minimize the use of fraudulent or stolen U.S. documents by terrorists. The new documents should include a machine-readable fingerprint and a facial photo, in the case of U.S. passports, matched to a computer record of all valid U.S. passport holders. The Border Crossing Card (BCC) to facilitate travel between the United States and Mexico should be continued.

Key Step #5. The Attorney General, working with the Secretary of the Treasury as appropriate, should strengthen the entry process and explore the development of an exit monitoring mechanism. A system should be developed and given adequate resources to address the exit as well as the entry of aliens. Developing a comprehensive entry–exit system presents enormous challenges, but this does not render it impossible or not worth exploring. It does mean that the objective should be accomplished in structured, incremental steps.

Initially, the Attorney General should direct the INS Commissioner and the Chief of the Border Patrol to expand the INS Automated Biometric Identification

System (IDENT system) to all Border Patrol stations and inspection locations. The IDENT system currently is used to identify aliens who have been apprehended for violations of the immigration laws. Apprehended aliens' photographs and fingerprints (prints of the left and right index fingers) are entered into an electronic database. Using this information, a person who subsequently gives a different name may still be tracked in the system, including the number of times he or she has been apprehended and the outcome of each apprehension (removal, release, etc.).

Further, the OHS Director, the Attorney General, the Secretary of the Treasury, and the DCI should continue efforts to expand and increase the integration of the U.S. Customs Service, which is tasked with combating illegal entries of people and goods, into all aspects of border security to ensure coordination of all relevant Federal agencies. Currently, uniformed USCS inspectors and plainclothes investigators are present at all the points of entry to combat smuggling, among other illegal activities.

STRENGTHENING LEAS' ABILITY TO ENFORCE IMMIGRATION OR OTHER LAWS AGAINST ALIENS WHO VIOLATE THEM

Key Step #1. Congress should amend the Immigration and Naturalization Act (INA) and other laws to strengthen the monitoring of visa holders and the removal of visa violators.

Reporting on the Status of Non-Immigrant Visa Holders. Congress should amend the INA to require those who sponsor a non-immigrant visa holder to report on the status of the sponsored alien, such as affirming under penalty of law that the alien is abiding by the terms of his visa. To enhance efforts to track aliens and prevent overstays, those who sponsor a non-immigrant visa should report on the alien's status annually, or as soon as there is a change in the alien's status. This would help INS develop a more effective and useful database of aliens still in the United States. INS investigative resources should also be increased to ensure that the agency is able to follow up on this information when it finds an alien in violation of the time limit on the visa.

Limiting the Use of Voluntary Departure. Congress should amend Section 240B of the INA to eliminate voluntary departure as an option during removal proceedings before an immigration judge. Voluntary departure allows an alien who is ineligible to remain in the United States (for example, because he entered illegally or overstayed a visa) to leave without having an order of deportation entered against him and put in his record. This "voluntary departure" option allows aliens to avoid the consequences of a deportation order, such as being barred for 10 years from receiving another visa. Under this amendment, INS would still be able to grant voluntary departure to aliens who are not placed in removal proceedings (required to

go before an immigration judge) or in removal proceedings where the INS counsel agrees to terminate proceedings in order to grant a voluntary departure.

Voluntary departures benefit aliens rather than expedite the process of removing them. Unless there are disincentives with teeth, aliens will continue to overstay and otherwise violate their visa conditions. Tightening the availability of voluntary departure is one way to show that the Federal government is serious about its immigration laws and the consequences of violating them. Such measures help to constrict the universe of aliens who overstay or otherwise violate the conditions of their visas. Eliminating the availability of “voluntary departure” in removal proceedings might also streamline the process, effectively eliminating an issue for appeals.

Putting the Burden of Proof on Violators of Visas. Congress should amend Section 236(a) of the INA with new language to make it unmistakably clear that, in bond re-determination hearings before immigration judges (cases involving aliens who have been charged with violating immigration laws), aliens charged with violations of the law have the burden of proving that they are neither a danger to the community nor a flight risk.

This should apply to all aliens detained by INS pending removal proceedings, whether or not the grounds upon which their removal is sought are criminal. The presumption should be that anyone detained by INS pending removal proceedings meets one or both of the above requirements, with the presumption open to rebuttal by the respondent; rebuttal evidence should be more than unsubstantiated statements by the respondent. In cases requiring mandatory detention (such as aliens certified as terrorists by the Attorney General under Section 236A of the INA, as amended by Section 412 of the PATRIOT Act) and criminal aliens per Section 236(c) of the INA, the presumption would not be open to rebuttal. This would not change the existing obligation of the INS to prove that the respondent is an alien and is subject to a ground of inadmissibility or deportability; nor would it prevent the respondent from rebutting the INS’s evidence of alienage or the charges of an immigration violation.

Increasing Access to Court Documents. Federal courts should be required to make available to INS all court documents relevant to immigration removal proceedings. Criminal court documents are essential in supporting many of the charges in immigration hearings regarding an alien’s removability. Some courts and LEAs are less than helpful in supplying the documentation necessary to prove that an alien has been engaged in activities that violate the terms of his or her visa or that would make that individual ineligible for immigration relief or benefits.

Judges have been known to seal court documents so that a criminal conviction cannot be used by INS in removal hearings where such documents are needed to prove the elements of the criminal activity that render an alien subject to deportation or ineligible for immigration benefits or relief. For example, a Pre-Sentencing

Investigation is the report of a court-appointed official to the judge on the facts of the crime committed; this report is used by the judge to determine the sentence to be imposed on the defendant. Such reports, which contain details of the criminal activity for which the alien was convicted, can be critical to the enforcement of immigration laws. They may detail the age of the victim, the relationship of the victim to the alien, or the amount of loss to the victim, information that may be essential to proving an alien's removability but which may not be included in the record of conviction. In the case of credit card fraud, the conviction documents may not specify the amount of the victim's loss, but the loss must be known in order to determine the immigration consequences of this crime. Cooperation in providing conviction and related documents should be encouraged for all Local, State, and Federal LEAs and courts as part of a concerted effort to improve respect for and enforcement of immigration laws.

Key Step #2. The Attorney General should direct the implementation of comprehensive procedures for handling immigration cases that have national security aspects or involve classified documents. For example, the Attorney General could designate one judicial location where such cases should be considered, provide for special training of potential trial attorneys in the handling of classified information, and require trial attorneys in these cases, as well as immigration judges, interpreters, bailiffs, and necessary support personnel, to have a security clearance. The suitable location should be one where defense attorneys are readily available.

Key Step #3. The Attorney General should direct Federal LEAs to work with State and Local LEAs to develop a standardized, comprehensive format for criminal “rap sheets.” These sheets should be made available to the INS in a reliable secure format for enforcement purposes—both for determining eligibility for benefits and for use in removal proceedings.

PRIORITY #5: REDUCE THE OPPORTUNITIES FOR IDENTITY THEFT AND FRAUD IN STATE IDENTITY DOCUMENT SYSTEMS.

The September 11 atrocities showed that terrorists will use fraudulently obtained identification to blend in and move through society undetected. It also proved that they will exploit those States with systems most liable to fraud. Any State that continues to run a document system subject to fraud and abuse places the lives of all Americans in jeopardy. The creation of a fraud-proof driver's license and identification card system would make it far more difficult for terrorists to enter the country unlawfully and to move about freely. The new system would also limit the growing problem of identity theft.

Currently, state-issued identity cards suffer from three deficiencies:

1. They are easily counterfeited.
2. There is little effort to determine whether the information the applicant provides is true.
3. There is often little or no effort to determine whether the card applicant is in the United States lawfully.

The present state identity card system should be reformed in the following manner:

Key Step #1. State governments, working with the National Governors' Association, the U.S. Conference of Mayors, the OHS Director, and the Department of Justice, should initiate programs to improve certificates of identity, including the development of new tamper-proof documents. States need to develop mechanisms to determine that the recipients of driver's licenses and other state-issued certificates of residency are indeed valid, legal recipients.

States should not issue certificates of identity or residence except to individuals who provide (a) proof of citizenship or (b) a valid passport and a tamper-proof document demonstrating their lawful presence in the United States. In ascertaining citizenship, states should not accept birth certificates and Social Security cards at face value, since these documents are easy to counterfeit or obtain fraudulently. Instead, the issuing Department of Motor Vehicles should check the authenticity of the information on any document with the agency that issued it; there should be a mechanism to determine whether the same name, birth date, and Social Security number have been used to obtain a driver's license for another individual living elsewhere. There should be an automatic cross-check of death records to bar terrorists and other criminals from attempting to assume the identities of deceased individuals.

States should require aliens who apply for a driver's license to provide a passport and valid tamper-proof U.S. visa. The alien's immigration status, registration number, and permitted length of stay should be included on the license and in the electronic file.

States should redesign all driver's licenses and identity cards to be machine-readable and to include a digitized photograph that can be electronically matched against a duplicate photo in a central DMV electronic file. Police and other organizations seeking to verify identities would use scanning machines to compare the picture and other information on the card with the matching electronic data. The FBI Director also should cooperate in the creation of tamper-proof driver's licenses and identity documents.

The new fraud-proof driver's licenses should be used in all circumstances in which current driver's licenses are used to confirm an individual's identity. These include boarding an airplane, entering a secure or sensitive area, renting or purchasing a vehicle, opening a bank account, and in police traffic stops. In addition, the Federal government or the States might require that fraud-proof identification be used in other transactions, such as renting a hotel room or buying rail or bus tickets. This would further hamper the ability of terrorists to move about the country unlawfully.

Key Step #2: State governments, working in cooperation with the Federal government, should strengthen existing mechanisms for recording all domestic documents (such as birth certificates, death certificates, and driver's licenses). Electronic data from the 50 state DMVs should be pooled so that the authenticity of a driver's license from one state can be confirmed when the license is used in another state. The entire system should be checked automatically for attempted duplicate entries: instances in which two different persons have attempted to use the same name, date of birth, and Social Security number.

Key Step #3. The OHS Director, in coordination with the Chairman of the Federal Trade Commission, the Attorney General, and State governments, should develop a mechanism to enhance the Federal-level mechanism to deter and obstruct identity theft. An enhanced nationwide registry should be established for those who have had documents containing sensitive personal information lost or stolen, such as a passport, driver's license, credit card, or other documents containing such personal information. Individuals who have been victimized by the theft of such documents normally report such losses to local law enforcement authorities, banks, and credit card companies and credit bureaus. A national registry of these cases would provide additional protection against identity theft.

The Identity Theft and Assumption Deterrence Act of 1998 (P.L. 105-318) made identity theft a federal crime and mandated that the Federal Trade Commission (FTC) establish procedures to "log and acknowledge the receipt of complaints" of the victims of identity theft and to refer complaints to "appropriate law enforcement agencies for potential law enforcement action" (Section 5). As currently implemented by the FTC, the victim of identity theft must report to the relevant local LEA, banks, and the major credit bureaus before the FTC refers the complaint to the Department of Justice. This current structure should form the basis for an expanded registry with an active interface with law enforcement in situations of identity theft.

PRIORITY #6: CREATE A MECHANISM TO MONITOR RECENT ANTI-MONEY-LAUNDERING INITIATIVES TO OBSTRUCT THE FINANCING OF TERRORISM.

An oversight mechanism is needed to anticipate how those who threaten the United States may circumvent existing anti-money-laundering restrictions. Many of the deficiencies in pre-September 11 efforts to obstruct, if not stop, the financing of terrorist activities have been addressed in the International Money-Laundering Abatement and Anti-Terrorist Financing Act of 2001 (Title III of the PATRIOT Act). This law represents a good advance in combating money laundering by terrorists and the sponsors of terrorism. Nevertheless, those who seek to harm the United States can still buy the best financial and legal advice available to help them circumvent current reporting and regulatory structures.

Key Step. The Secretary of the Treasury should direct the creation of a mechanism to evaluate how the current law to obstruct terrorists' finances could be circumvented. The Treasury Secretary should direct the Foreign Terrorist Asset Tracking Center, the Financial Crimes Enforcement Network (FinCEN), and the U.S. Customs Service, working with the Attorney General and the DCI, to establish a mechanism to anticipate how the current banking and financial restrictions can be circumvented by terrorists or sponsors of terrorism so that remedial steps can be taken.

CONCLUSION

September 11 starkly demonstrated that attacks on the American homeland can come from unexpected sources using unexpected means. Enhancing the relationship between Federal law enforcement agencies and the Intelligence Community, as well as enhancing the relationship between Federal, State, and Local agencies, is essential to addressing the ongoing threats to the American people. The multifaceted approach should reflect the understanding that there is no one-size-fits-all remedy. The Administration, Congress, state officials, and the private sector have correctly turned their attention to the need to deter and prevent, and to respond to, future terrorist attacks.

The Federal government should foster the development of a uniform methodology for assessing America's vulnerabilities and the means to address those threats, including a national homeland security strategy, to ensure that resources are allocated to meet critical needs. It should take steps to improve the collection of information by Federal agencies and to enhance information sharing with State and Local officials. It must strengthen the visa approval process, the entry-exit system

for aliens traveling to and from the United States, and the ability of law enforcement to enforce existing immigration laws. And it should create a mechanism to monitor recent initiatives to obstruct money laundering by terrorists and their allies.

State and Local governments also have a role as the first responders. They should take immediate steps to identify the critical targets within their respective jurisdictions and assess the threat to those targets, sharing these assessments with Office of Homeland Security. They also should improve the information collection and analysis mechanisms of their respective law enforcement and/or first-responder agencies; designate State and Local officials to interact with their Federal counterparts; and eliminate the opportunities for fraud in state identity document systems. Such a multifaceted, broad-based approach will help assure Americans that government is doing its best to protect them from future terrorist attacks.

Table 5

Status of Key Unimplemented Commission Recommendations for Improving Intelligence and Law Enforcement

Recommendation	Name of Commission	Status
Intelligence Collection. Expand multidisciplinary collection, specifically expanding research and development in signals intelligence (SIGINT) and measurement and signature intelligence (MASINT).	Gilmore Commission Bremer Commission	No known vehicle for the expansion of multidisciplinary collection efforts has yet been introduced.
Language Capability. Develop a larger pool of linguists and an interagency strategy for employing them.	Bremer Commission	The FBI has posted public recruitment for contract linguists. The CIA has added positions for language instructors on the employment site in nine languages.
Intelligence-Sharing. Improve the sharing and dissemination of intelligence information among Federal agencies and between State and Local agencies.	Gilmore Commission Bremer Commission National Defense Panel	On October 29, 2001, Federal officials announced the creation of the Foreign Terrorist Tracking Task Force (FTTF) to “enhance United States efforts to prevent terrorist activity.” Based on the New York Joint Terrorism Task Force, which began in 1980 with members of the NYPD and 11 FBI investigators, the FTTF now includes over 100 members from several agencies at both the state and local levels. There are 36 similar task forces nationwide.
Intelligence Funding. Fund intelligence capabilities at adequate and sustained levels.	Hart–Rudman Commission Bremer Commission	The Intelligence Authorization bill for FY 2002 (H.R. 2883) was signed by the President on December 28, 2001. It reportedly provides an increase in funding for FY 2002, although amounts are classified.
Money Laundering and Financing of Terrorism. Disrupt and halt the sources of financing for terrorist activities.	Bremer Commission	Executive Order 13224, issued on September 23, 2001, suspended the assets and bank accounts of individuals and organizations suspected of involvement in terrorism. Title III of the PATRIOT Act (P.L. 107–56) strengthens legal mechanisms to monitor and obstruct international money laundering by individuals or groups suspected of involvement in terrorism.
Terrorist Deterrence. Develop deterrence initiatives against those states that either sponsor terrorism directly or allow their territory to be used by terrorists; methods should include denial of participation in certain visa programs.	Bremer Commission	Since September 11, numerous pieces of legislation have been introduced in both houses of Congress to address deficiencies in immigration and border enforcement mechanisms. The general thrust of these proposed bills is, inter alia, to strengthen the visa approval and the inspection and admission processes and the monitoring of foreign visitors, especially foreign students; to require the sharing of information among law enforcement and intelligence agencies; and to fund the hiring of additional personnel. The House approved one of the bills, H.R. 3525, the Enhanced Border Security and Visa Entry Reform Act, on December 19, 2001. It would authorize the hiring and training of personnel, require interagency information sharing, restrict the use of visas, and strengthen admission and inspection mechanisms.

TOP PRIORITIES FOR MILITARY OPERATIONS TO COMBAT TERRORISM

*A Report of The Heritage Foundation Working Group on Military Operations*¹

Larry M. Wortzel, Working Group Rapporteur

Since the publication of the National Defense Panel (NDP) report in 1997, there have been clear warnings to the people and policymakers of the United States that the nation's homeland must be protected from terrorist attacks. Other studies also have made it clear that the U.S. armed forces, working with the Intelligence Community and Federal, State, and Local officials, must be prepared not only to identify impending terrorist attacks, but also to preempt or respond to them rapidly.²

First and foremost, the U.S. armed forces must defend the homeland and respond to catastrophic attacks, which can be the result of terrorism or counterstrikes on U.S. civilian targets by enemies, such as Iraq or North Korea, in time of war. Regardless of the origin of an attack, the armed forces must be prepared to protect the homeland and respond immediately to a catastrophe.

1. The members of the Working Group on Military Operations Against Terrorism include David Davis, Chief of Staff, Office of Senator Kay Bailey Hutchison; Colonel James P. Gibbons, USA (Ret.), former Commander, U.S. Army Land Information Warfare Activity; Major General David L. Grange, USA (Ret.), former Commander, 1st Infantry Division; Lieutenant General Patrick M. Hughes, USA (Ret.), former Director, Defense Intelligence Agency, and former Commanding General, U.S. Army Intelligence Agency; Dr. Fred Iklé, Distinguished Scholar, Center for Strategic and International Studies; General Carl E. Mundy, Jr., USMC (Ret.), former Commandant, United States Marine Corps, and former member, Joint Chiefs of Staff; General John H. Tilelli, Jr., USA (Ret.), former Commander, U.S. Army Forces Command, Vice Chief of Staff, United States Army, and Commander in Chief, U.S. Forces Korea; and General Charles E. Wilhelm, USMC (Ret.), former Commander in Chief, U.S. Southern Command. The following individuals also contributed to this report in an advisory capacity: Todd Gaziano, Director, Center for Legal and Judicial Studies, The Heritage Foundation; General Dennis J. Reimer, USA (Ret.), former Chief of Staff, United States Army; and The Honorable James Schlesinger, Special Adviser, Lehman Brothers, Inc., Washington, D.C., former Secretary of Defense.
2. For a summary of recommendations from prior commissions and studies that have not been implemented, see the table at the end of this chapter. The status of post-September 11 legislative efforts may be found in the Appendix.

In fighting terrorism, the best defense is a good offense. U.S. forces must be configured to combat the threat, and also to maintain the capabilities to fight and win conflicts against conventional armed forces. To date, the involvement of U.S. forces in military operations in Afghanistan has been conducted under an extraordinary array of circumstances that in all probability will not be a blueprint for all conflicts in the future.

In any restructuring of forces to meet a rising threat, care must be taken to ensure a continued balance between unconventional and conventional force capabilities. A number of studies have suggested how to accomplish these objectives, but their recommendations are still being debated, and many have not been systematically implemented.

This report by The Heritage Foundation Working Group on Military Operations builds on those recommendations by identifying key priorities for improving military operations and taking firm positions on how best to defend the homeland against terrorism. Specifically:

- **Priority #1: Free the National Guard and Reserves for homeland security and boost port security quickly.** The present configuration of conventional forces, special operations forces, and strategic forces will function well for military operations in support of homeland defense and for conducting a range of operations overseas, including deterrence and fighting terrorism at its roots. The National Guard and Reserves should not be the only military personnel involved in security; active force units must also be involved. But homeland security will require enhancing the capabilities of National Guard and Reserve units to respond to terrorist events, as well as freeing some units from having to add personnel for combat support and combat service support for the active forces. It also will require reinstating a port security program.
- **Priority #2: Protect U.S. borders, coasts, and critical national infrastructure with air defense and missile defense.** The threat of attack from the air—by aircraft, cruise missiles, and ballistic missiles—requires the United States to establish a robust air and cruise missile defense system now and to begin testing ballistic missile defenses on land and at sea at full design capability.
- **Priority #3: Enhance rear-area military operations to protect the homeland and prepare for terrorist attacks.** The U.S. military can assist Local, State, and Federal authorities in counterterrorism efforts by identifying and assessing security levels at critical infrastructure nodes; providing protection for critical infrastructure; providing redundant communications, command, and control systems; and procuring and maintaining equipment that would assist in responses to terrorist attacks. While many commissions have considered this approach, the Training and Doctrine Command of the U.S. Army has pulled the Army out of the mission. The Secretary of Defense should work with the

Director of the Office of Homeland Security (OHS) to have Reserve and National Guard units involved once more in homeland defense education and training and to develop active cooperation and education programs for each state.

- **Priority #4: Provide intelligence support for military operations.** Effective offensive and defense operations against terrorism will require a distributed intelligence and information architecture with intelligence fusion centers that link to a network that allows any Federal agency with access (such as the U.S. Army, Federal Aviation Administration, or Central Intelligence Agency) to query a large shared database. No such database exists today, and information remains compartmentalized in different agency “stovepipes.” To win the war against terrorism, the U.S. Department of Defense (DOD) must have access to cross-referenced strategic and critical databases housed in various Federal agencies. This will require that fusion centers at the Federal, State, and Local levels, where necessary, are manned by personnel cleared for an intelligence compartment related to the war on terrorism and homeland defense.
- **Priority #5: Ensure clear command and control of overseas anti-terrorism operations.** The Department of Defense should resist calls to establish a new command to handle overseas operations against terrorism. Regardless of whether military operations are of an offensive or defensive nature, the geographic Unified Command (such as PACOM, or CENTCOM, which is directing the war in Afghanistan) must be the command-and-control headquarters for overseas military operations. In military parlance, this means that the geographic Unified Command will be the supported command and the war fighter. The United States Special Operations Command (SOCOM) should be a specified supporting command for managing counterterrorism operations and the primary force provider. The Secretary of Defense, in the Defense Guidance, must ensure that SOCOM has the requisite authority and priorities to resource the fight and to develop new systems to support the war against terrorism.

PRIORITY #1: FREE THE NATIONAL GUARD AND RESERVES FOR HOMELAND SECURITY AND BOOST PORT SECURITY.

A debate is raging among defense analysts who argue that tomorrow’s warfare will involve battles similar to today’s war on terrorism, with enemies that mount non-traditional attacks on Americans, perhaps with chemical, biological, radiologic, or nuclear (CBRN) weapons. Others argue that it primarily will involve small,

localized wars of short duration in regions that are vital to American interests. At the same time, the possibility of a major conventional war still exists.

The Working Group on Military Operations believes that the Quadrennial Defense Review (QDR) submitted to the President by Secretary of Defense Donald Rumsfeld in October correctly balances the need for counterterrorist military operations, conventional war, and operations for responding to other forms of “low-intensity conflict.” This is the right approach. The United States should continue its capabilities-based strategy to fight and win wars *and* to deter aggression and terrorism against its people, homeland, and interests.

This strategy must include a robust capability to conduct counterterrorist military operations; to protect U.S. interests should a general war break out on the Korean Peninsula, in the Middle East, or in Southwest Asia; and to respond appropriately in the Pacific region to forces of countries that employ area-denial and anti-access strategies, such as China. Such a strategy will require the Administration to take the following steps:

Key Step #1. The Secretary of Defense should add active duty personnel to current active force levels to put more combat support and combat service support elements into the active military. The Secretary of Defense should ensure that the active armed forces include additional combat and combat service support elements, particularly in the Army, so that the necessary National Guard and Reserve units are able to assume greater responsibility for homeland security. Many combat support and service support units—such as in communications, logistical support, intelligence, medical support, and food service—were moved into the National Guard and Reserves in the late 1980s and 1990s to reduce the size of the active armed forces.

Today, the U.S. Army and U.S. Air Force cannot go to war without activating large numbers of Reserve and National Guard organizations. However, these same Reserve and Guard components are the primary units to support homeland security requirements. They must be freed from their support of the active forces to defend the homeland against terrorism. Combat support and combat service support personnel that are put back in the active forces must be additions to the total active force strength.

Key Step #2. The Secretary of Defense should ensure that the National Guard has standing emergency plans to train for and work with Local authorities on homeland defense and consequence management. The National Guard Bureau, the National Guard State Area Commands (STARCs), and the State Adjutants General must be involved in all State emergency management programs. The STARCs and Continental U.S. Armies (CONUSAs) should be linked to provide

rapid communications and coordination. The STARCs are likely to be the first military responders following civilian requests for assistance in a major crisis or incident.

Each State must have a viable emergency plan, an operations center, and dedicated, redundant command-and-control means of communications in the event of an emergency. The relevant National Guard Bureau regulation, which was written in 1982, should be updated to reflect the new security environment. In addition, many State Adjutants General should update their state crisis action plans.

Key Step #3. The OHS Director should request the National Guard to work with Local and State officials to develop public information campaigns. An information operations plan to prevent panic and misinformation should be included in all military department press plans and consequence or crisis management strategies. This is a key component of the information war against terrorism because one goal of terrorists is to create panic and chaos.

A seamless information warfare operation should involve not only the military, but also the Director of the Office of Homeland Security. The President should appoint a national spokesman, perhaps from OHS, for the release of information about emergencies. The OHS Director should request that the National Guard and State and Local officials in each relevant area appoint spokesmen as well who will communicate with the national spokesman daily regarding any terrorist events.

Key Step #4. The Secretary of Defense, with the Secretary of Transportation and the OHS Director, should re-institute a robust port security program to check all incoming ships and containers. The Secretary of Defense should ensure that U.S. Navy ships, in conjunction with the Coast Guard, are stationed so as to protect sea approaches to key U.S. ports and waterways 12 miles from the coast, not three miles, which is the present Coast Guard standard. The most effective way to get a large weapon of mass destruction into the United States is on a ship or in a container, and joining a ship's crew offers would-be terrorists a way to enter the United States. New equipment is needed to detect smuggled nuclear devices. DOD, in cooperation with the Department of Energy, should promote the research and development of more effective equipment and sensors.

During the Cold War, as a defense against espionage, sabotage, and weapons of mass destruction (WMD), the Coast Guard and U.S. Navy—working with the Maritime Administration of the U.S. Department of Transportation—monitored all Soviet-bloc ships and crews that came into the United States, and some ports were closed for security reasons. But this program ended in the 1990s, and today the Coast Guard can inspect only 3 percent of containers that come into U.S. ports.

On the eve of the terrorist attack on the United States, there was no port security program in place that provided consistent, routine surveillance of ships, cargoes, containers, and crews. The port security system should be reconstituted. All ships entering U.S. territorial waters should be identified, and boarded and searched if authorities determine that is required. Since September 11, ships are required to give 96 hours prior notice of arrival. That notification of arrival should include crew, cargo, and passenger lists and manifests.

PRIORITY #2: PROTECT U.S. BORDERS, COASTS, AND CRITICAL NATIONAL INFRASTRUCTURE WITH AIR DEFENSE AND MISSILE DEFENSE.

As the events of September 11 showed, vital infrastructure in America's cities remains vulnerable to attack from any number of threats, including missiles launched from offshore. Most of the countries that the Department of State has identified as sponsors of terrorism are working to gain WMD and the missiles to deliver them.

Only an effective, tiered missile defense system can protect the nation's homes and people from these weapons. The President took the correct action in notifying Russia that the United States would no longer observe the 1972 ABM Treaty with the Soviet Union. It is urgent that the Department of Defense test and field a ballistic missile defense system as soon as possible.

The Department of Defense should be prepared to protect critical national infrastructure by rapidly deploying air defenses and cruise missile defenses when the need arises. The \$8 billion per year currently programmed in the Defense budget for ballistic missile defense research is adequate funding. Additional steps, however, are also necessary. Specifically:

Key Step #1. Congress should provide additional funding for the deployment of a cruise missile defense system as a component of homeland defense. At present, the United States has the technology to defend the homeland against cruise missiles, which could carry WMD or conventional blast warheads. Cruise missiles have proliferated widely around the world; they can be launched from aircraft or ships, including civilian merchant ships off the U.S. coast. But unlike ballistic missiles, which first are launched up into the atmosphere and follow a parabolic trajectory flying back down to a target, cruise missiles generally fly a straight, almost line-of-sight trajectory. Defending against them requires deploying a robust cruise missile defense system.

Key Step #2. The Secretary of Defense should deploy air defense and cruise missile defense systems to defend major U.S. cities and critical infrastructure. A layered approach to global ballistic missile defense, with both ground-based and sea-based interceptors, would help protect the homeland from ballistic missile attack. To defend against cruise missiles, defensive systems should be stationed around the U.S. coast on ships or at critical sites on land. Among the systems that would be effective are radar-directed, high-speed gun systems; laser and directed-energy weapons; and short-range, high-speed air defense missiles. The Mark 15 Vulcan-Phalanx gun system, short-range, man-portable air defense systems, and air- or ground-based lasers all offer effective and easily fielded defenses against cruise missiles.

PRIORITY #3: ENHANCE REAR-AREA MILITARY OPERATIONS TO PROTECT THE HOMELAND AND PREPARE FOR TERRORIST ATTACKS.

The use of the military in homeland defense against terrorism has limitations. The first priority must be to stop a terrorist act before it can cause catastrophic damage through quick actions. Unless a terrorist event takes place on a military installation, however, Local, State, and Federal law enforcement agencies and medical and emergency services personnel—not the U.S. military—will be the front-line troops, or “first responders,” in dealing with terrorist attacks on the homeland.³

What the U.S. Military Can and Cannot Do. The U.S. military can assist Local, State, and Federal agencies in homeland defense by identifying and assessing security levels at critical infrastructure nodes; providing protections for critical infrastructure; providing redundant communications, command, and control systems; and procuring and maintaining equipment that would assist Local and State responses to terrorist incidents. The Department of Defense can also provide military assistance to civil authorities to help them respond to certain situations involving chemical or biological weapons of mass destruction and nuclear materials.⁴

Neither the Posse Comitatus Act nor other statutes seek to deny, limit, or condition the President's use of the armed forces to respond to a catastrophic terrorist attack on the United States.⁵ However, active-duty armed forces and reserves, while in Federal service, are prevented by the Posse Comitatus Act from engaging directly in most law enforcement functions. The Posse Comitatus Act (18 U.S.C. § 1385)

3. Separate statutes allow the President to use the military to keep the peace in an emergency or disaster not prohibited by the Act—such as a hurricane, riot, or earthquake—and Congress has authorized the use of the military for specific immigration and drug enforcement tasks. Military personnel, moreover, are required to enforce the military justice system on military bases, including making arrests that involve military personnel and others. For more on first responders, see chapter on Civil Defense and chapter on Intelligence and Law Enforcement.

was enacted in 1878 to end certain military practices in the post-Civil War reconstruction era. It does not apply when a governor utilizes the National Guard in state service. In its current form, the Act provides that the Army and Air Force may not be used to “execute the laws” unless “expressly authorized by the Constitution or Act of Congress.”⁶ The Act acknowledges that the President retains some constitutional authority to use the military in certain circumstances. By declaring an emergency in the event of attack, riot, or other major disaster, or the threat thereof, the President can utilize federal armed forces to maintain order and protect life and property.

Military personnel can act decisively to stop a catastrophe or terrorist act occurring in their presence. The Department of Defense may make available military personnel or equipment or provide technical assistance in many situations; thus, the courts have not interpreted the Posse Comitatus Act as prohibiting all assistance to Local, State, and Federal law enforcement operations.

To enhance military operations in homeland defense beyond the scope mentioned above, the Secretary of Defense should clarify command and control. Specifically:

Key Step #1. The Secretary of Defense should make the Commander in Chief (CINC) of the Joint Forces Command also the CINC for military operations to defend the homeland against terrorism.⁷ At present, the U.S. Army is the executive agent for military support for homeland defense operations; its emergency operations center initially receives, processes, and prioritizes the requests that come in from civilian authorities for military support. The Joint Forces Command in Norfolk, Virginia, is DOD’s commander and manager for homeland security and for responses to terrorist incidents or incidents involving weapons of mass destruction. It tasks the service components (the Army, Navy, Marine Corps, Air Force, and Coast Guard

-
4. For a comprehensive discussion of the Posse Comitatus Act, see Charles Doyle, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law*, Congressional Research Service, CRS Report 95-964, June 1, 2000. For the relevant laws on military assistance to civil authorities in WMD-related incidents, see 10 U.S.C. Section 382, *Emergency Situations Involving Chemical or Biological Weapons of Mass Destruction*, and 18 U.S.C. 831, *Prohibited Transactions Involving Nuclear Materials*. Department of Defense Directive 3025.15, *Military Assistance to Civil Authorities*, requires that requests for assistance to civil authorities be evaluated against six criteria: compliance with law; potential use of lethal force by or against DOD forces; safety of DOD forces; impact on DOD budget; and impact on DOD’s readiness to perform its mission.
 5. See Paul Schott Stevens, “U.S. Armed Forces and Homeland Defense: The Legal Framework,” Center for Strategic and International Studies, *CSIS Report*, October 2001, p. 3.
 6. This language creates some ambiguities and exceptions. For example, federal appellate courts disagree as to whether the Act applies to the Navy and Coast Guard, and a logical argument can be made that it should not apply on the high seas.

components assigned to it in DOD's Unified Command Plan) to respond to events around the United States.

The CINC for homeland defense operations must be a Unified Command that has a strong staff familiar with the National Guard and land and maritime operations. It cannot be a highly specialized specified command that is expert at a single facet of warfare (such as air or space defense). At present, the Joint Forces Command has the assets and experience its commander needs to function effectively as CINC for homeland defense.

The Army Forces Command and the Air Force Air Combat Command are component commands of the Joint Forces Command, with subordinate organizations that they train, equip, and control in the United States. The Naval Service elements of the Joint Forces Command (the Atlantic Fleet and the Marine Forces, Atlantic) train, equip, and control organizations east of the Mississippi River. (They work through lateral and higher headquarters to task organizations west of the river.) In the case of the Navy and Marine Corps, the Chief of Naval Operations and the Commandant of the Marine Corps should be responsible for operational support to the CINC Joint Forces Command. This will permit those service chiefs to direct forces throughout the United States.

The Joint Forces Command established the Joint Task Force Civil Support (JTF-CS) at Fort Monroe in Hampton, Virginia, to provide command and control over DOD forces in support of lead Federal agencies—those agencies held responsible by the President under Presidential Decision Directive (PDD) 63 for managing consequences of WMD or other incidents in the United States, its territories, or its possessions. Examples of lead Federal agencies are the Centers for Disease Control and Prevention (CDC) for medical or biological incidents, the Federal Emergency Management Agency (FEMA) for consequence management in major disasters, the Federal Aviation Administration (FAA) for airline crashes, and the Federal Bureau of Investigation (FBI) for criminal investigations. Broadening the mission of the Joint Forces Command, which handles incidents using weapons of mass destruction, to make its commander the CINC for homeland defense is a sensible course of action that takes advantage of that expertise.⁸

-
7. In discussion with some members of the Working Group, an alternative approach was also suggested. Since the U.S. Army Forces Command now controls or coordinates with all Army National Guard elements in the United States, Continental U.S. Armies (CONUSAs), State Area Commands, and State Adjutants General, a logical alternative to designating Joint Forces Command as CINC Homeland Security would be to vest that responsibility in Forces Command and make it a unified command with the responsibility for homeland defense.
 8. The Joint Forces Command will likely require relief from some of its NATO-related responsibilities if this course of action is adopted.

Key Step #2. The Secretary of Defense should use the deliberate planning process to establish a refined list of military responses to terrorist acts in the United States. One approach that has been used in some Unified Commands is the establishment of Standing Joint Task Forces (SJTFFs) to respond to contingencies. But such organizations tend to burden apportioned military staffs with additional personnel, logistics, and administrative requirements, and they can build up staffs that take on a life of their own. It is noteworthy that a number of Federal agencies—FEMA, the Environmental Protection Agency (EPA), CDC—and many military organizations already have pre-planned deployment lists of people and equipment to move in case of emergency, and plans on how to load equipment for transport to respond to crises. This should be the model for establishing military component responses and planning. In fact, DOD uses the same approach for war planning very effectively.

Key Step #3. The Secretary of Defense, in cooperation with the OHS and the Cabinet, should require the development of an interactive network of operations, command, and control centers and service mobilization directorates linked with key Federal and State response agencies. All military and civilian authorities at the Federal and State levels should be able to communicate with each other through redundant but secure systems. The Secretary of Defense, in consultation with Cabinet members and the OHS, must ensure that the operations, command, and control centers in the Joint Chiefs of Staff (JCS) and the service mobilization directorates are tied into the State emergency management operations centers, the STARCs, FEMA, the CDC, and other first responders using dedicated and redundant command, control, communications, and computer (C4) networks. The military departments and Joint Staff support operations should communicate with and involve civilian authorities through directorates of military support in their operations centers. Representatives of other Federal agencies should be co-located in the centers.

In many cases, the geographical areas of responsibility within the United States differ for various agencies with homeland security or consequence management responsibilities. For example, the FEMA, FAA, and Continental U.S. Army (CONUSA) regions and the sub-regions of responsibility for other federal agencies do not always coincide. To resolve the inevitable confusion that results from such differences, the CINC for homeland defense and the Director of the Office of Homeland Security should conduct regular exercises and training sessions that involve all Federal agencies and the States.

Key Step #4. The service branches should ensure that active-duty members, reservists, and National Guard personnel understand how to correctly apprehend suspected terrorists. The service members who are out protecting some locations are basically infantrymen. They usually have little or no instruction in the rules of collecting

evidence, apprehension of suspects, cursory legal searches, or the legal seizure of contraband, weapons, or evidence. Their goal should be to prevent a catastrophic terrorist act.

Key Step #5. The service branches should provide training for the National Guard, FEMA, and other Federal and State agencies on incident response and mitigation.

In many cases, the U.S. armed forces have specialized knowledge and training on planning for and conducting these types of operations, as well as instruction on maintaining, budgeting for, and sustaining equipment. This knowledge can be transferred to first responders at the Local and State levels by including the National Guard, FEMA, and other Federal agencies in the military's formal training programs and exercises on incident response and mitigation.

Key Step #6. The Secretary of Defense should ensure that all components of the Joint Forces Command can directly task units around the United States to respond to incidents. The Navy and Marine Corps components of the Joint Forces Command are essentially only responsible for direction, training, staffing, and equipping of organizations east of the Mississippi River. They should be able to task organizations throughout the United States in a rapid manner without requiring lateral coordination with Navy and Marine Corps headquarters west of the Mississippi. All the components of the Joint Forces, in particular the Navy and Marine Corps, should be able to respond to a terrorist incident or requests for support without passing the mission to another headquarters. The Chief of Naval Operations and the Commandant of the Marine Corps, not a subordinate headquarters with limited regional authority, should be the force provider.

PRIORITY #4: PROVIDE INTELLIGENCE SUPPORT FOR MILITARY OPERATIONS.

Effective military operations depend on timely and accurate intelligence about enemy forces, movements, capabilities, and intentions. Real-time, all-source intelligence fusion centers are required for effective counterterrorism military operations and for homeland defense.

As discussed in the chapter on Intelligence and Law Enforcement, the Director of the OHS, with the Director of Central Intelligence (DCI), should foster the development of an all-source intelligence fusion center for providing information to authorities on a need-to-know basis about the potential terrorists, including where their cells are located and their plans, activities, and stated intentions. The database should be interactive and networked, linking Federal agencies and sophisticated collation and analysis methods to develop intelligence on terrorists.

Five of the terrorists who attacked the United States on September 11 were on the watch lists of different U.S. government agencies. Three of the five were on a CIA watch list. Of the 13 terrorists in the United States on visitors' visas, three were here on expired visas. Thus, information about many of those terrorists and their movements existed in federal databases before that tragic day. However, these databases were not integrated or linked for common retrieval of information. Thus, no single agency—not the FBI, the Department of Defense's intelligence units, the Federal Aviation Administration, the Immigration and Naturalization service, nor the CIA—was able to query all the databases to fuse, collate, and assess the quality of that information.⁹ While it is impossible to say what might have happened had authorities apprehended and questioned the five people on the federal watch lists or the three with expired visas, integrated databases and fusion centers would facilitate such action. To achieve this goal, two key steps must be taken:

Key Step #1. The Defense Department should institute local, low-level counterintelligence source operations for force protection near military installations. Defense counterintelligence agencies (elements funded under DOD's Foreign Counterintelligence Program) should work with Local, State, and Federal law enforcement personnel to develop an information network on potential terrorists or military surveillance in an area. Military police, military intelligence officials, and DOD counterintelligence and security personnel could approach retired military annuitants in the vicinity of military installations to develop a counterintelligence source network.

Key Step #2. The Director of OHS and the Director of Central Intelligence should ensure the creation of all-source fusion centers for collecting and sharing information about terrorist cells, plans, activities, and intentions. As discussed in more detail in the chapter on Intelligence and Law Enforcement, a national fusion center for intelligence and information on the threat to the homeland is vital to protecting the homeland and deploying resources efficiently and effectively. Local, State, and other Federal personnel who require access to this information must undergo necessary background investigations by Federal authorities. In addition, States and Localities will have to build information storage and processing facilities and systems that meet federal standards for the handling of classified national security information.¹⁰

9. With respect to the terrorists that attacked the United States on September 11, whenever the FBI places a suspected terrorist on a watch list, it circulates that person's photo to local police, immigration officers, or customs agents. Though some of the hijackers were on U.S. intelligence agency watch lists when they boarded the planes on September 11, the intelligence/information was not shared with the FAA, which could have used it to alert the airlines.

PRIORITY #5: ENSURE CLEAR COMMAND AND CONTROL OF OVERSEAS ANTI-TERRORISM OPERATIONS.

The Department of Defense and the Joint Staff have an effective and functional Unified Command Plan that sets out the responsibilities of the U.S. Armed Forces to conduct war and defend the United States. It would be a mistake to attempt to reorganize that structure in the middle of any war, including the current war on terrorism. The Administration should rely on the Unified Command Plan and the geographic Unified Commands (PACOM, EUCON, SOUTHCOM, CENTCOM) to fight the war on terrorism overseas.

Key Step #1. The Secretary of Defense should keep SOCOM as a force provider (supporting CINC), not the major war fighter, and assure that SOCOM has adequate resources to carry out its mission. The Secretary of Defense should resist calls to establish a command to handle overseas operations against terrorism. In war fighting, the U.S. military employs a geographic Unified Command structure as the supported CINC to direct and control overseas combat, covert actions, and military intelligence-gathering operations. This structure provides the necessary command, control, communications, computer, and intelligence (C4I) capabilities for coordinating operations. It also has the logistics support infrastructure necessary for conducting operations. In addition, each Unified Command has an integrated special operations organization and liaison officers from within the U.S. Intelligence Community.

Thus, the geographic Unified Command remains the best-equipped and best-structured organization to control major military operations. The Special Operations Command (SOCOM) should be a specified command for managing counterterrorism operations so that it can direct training and operations, properly resource the fight, and develop new systems to support the fight.

The major war fighter, or supported CINC, should be the geographic Unified Command. Some defense analysts have suggested that SOCOM should become the supported command (the war fighting CINC in charge of all forces, support, and operations) in the war on terrorism. There also have been calls for a major increase in the number of special operations forces. But there are practical limits on the number of personnel that can be recruited and trained for special operations. These limits are a function of the demanding mental, physical, technical, and linguistic requirements for participating in special operations, as well as the relatively small number of people who volunteer for such duty. An expanded armed force, however,

10. For detailed descriptions of the information to be collected and the process for disseminating it, see chapter on Intelligence and Law Enforcement.

would provide a larger base of personnel from which to draw such dedicated volunteers.

As the main campaign against the al-Qaeda network in Afghanistan achieves its goals, the war against terrorism will likely shift to other areas of the world, where clandestine infiltration and exfiltration as well as unilateral direct actions could become the more common methods of destroying terrorist cells. Rather than increase funding for more special operations personnel, the Administration should focus on ensuring that a healthy mix of CIA and Special Operations Command personnel are on the staffs of the geographic CINCs and that the JCS headquarters and CIA are appropriately cross-staffed to permit proper coordination of such operations.

SOCOM must be able to direct the training and operations, prepare the budgets to resource the fight, and develop surveillance and reconnaissance systems like Predator and Global Hawk to support the fight. SOCOM should not have to compete for resources in the Unified Command Plan with the Unified Commands for specialized resources or assets. To ensure that SOCOM's acquisitions and budget requirements are properly prioritized, the Secretary of Defense must make sure that the Defense Guidance specifically charges SOCOM with those responsibilities. In addition, the Under Secretaries of Defense must provide the political leadership to ensure that the service bureaucracies do not simply return to business as usual.

Key Step #2. The commander in chief for homeland defense should prepare pre-planned force packages for initiating rapid responses to contingencies. The geographic CINC should plan for the movement and arrival of forces with dedicated movement packages and notional time-phased force deployment lists. The service component commands and the headquarters of the Unified Commands should use the deliberate planning process and time-phased force deployment lists to plan for forces that can rapidly respond to contingencies. The creation of numerous standing joint task forces is not recommended, since it could tax the staffs of the component commands and create more bureaucracy in the Unified Commands.

For lower-intensity operations overseas that require close coordination with the Intelligence Community, and for other covert activities, the geographic CINC should continue to be the supported CINC. Having a CIA liaison in each geographic Unified Command also will facilitate coordinated operations.

Key Step #3. The Secretary of Defense should ensure that the Defense Guidance sets out the nation's clear priorities regarding the conduct of the war against terrorism. These priorities—especially surveillance, reconnaissance, logistics, communications, and intelligence support for the fight—must be reflected in Defense research and

acquisitions plans, policies, and budgets to ensure that any bureaucratic inertia or parochial interests do not hinder the effort.

CONCLUSION

Any attempt to completely reorganize the armed forces in the middle of the war on terrorism would be a mistake. The current Unified Command Plan will work well in fighting the war on terrorism overseas and defending the homeland. The United States Special Operations Command needs the responsibility and political backing in budget battles to acquire the proper new intelligence and reconnaissance systems as well as other assets for this fight against terrorism. For the defense of the homeland, the National Guard Bureau must update its own regulations and begin to train and work closely with civilian first responders at the Local level in responding to crises.

Information operations are a necessary component of the war on terrorism to prevent panic among the U.S. population. The United States, which is now defenseless against ballistic missiles, must deploy defenses against both ballistic and cruise missile attacks. And the Department of Defense must establish a linked, searchable, and interactive intelligence database so that information acquired by different government agencies can be exploited to ensure the war's success.

Table 6

**Status of Key Unimplemented Commission Recommendations
for Counterterrorist Military Operations and Structures**

Recommendation	Name of Commission	Status
<p>Terrorist Attacks: Detection and Attribution Capabilities. Invest in capabilities to detect CBRN attacks and attribute them to likely aggressors. Credible retaliatory capability, essential for deterrence, depends on strong attribution capabilities to identify perpetrators and their supporters. Such capabilities will include laboratory facilities, equipment, and personnel necessary.</p>	Defense Science Board	Current detection and attribution capabilities are insufficient. The Department of Defense has made no known proposals to increase its capabilities with regard to the events of September 11.
<p>Warning Capability. Strengthen warning capabilities. Facilitate rapid communications for conveying information concerning a terrorist warning and preemptive strikes. Conduct a lessons-learned study of U.S. government warning across the entire intelligence cycle.</p>	Defense Science Board	Current warning capabilities are insufficient. The Department of Defense has not yet implemented plans for increasing warning capabilities.
<p>Annual Net Threat Assessment. Develop an “annual net threat assessment of the foreign and domestic threat of CBRN attack and terrorism.” Provide Federal planners with the basis for assessing the emerging risk of such attacks and develop an integrated analysis structure for planning U.S. programs and response.</p>	Defense Science Board	Current threat assessment is insufficient. GAO reports recommend re-evaluating the role of threat assessment for homeland security. No vehicle for the implementation of such assessment capabilities is known to exist.
<p>Defense Review. Congress and the Secretary of Defense should move the Quadrennial Defense Review to the second year of a presidential term.</p>	Hart–Rudman Commission	The Department of Defense has made no public proposal to move the Quadrennial Defense Review to the second year of any President’s term.
<p>Acquisition System. The Secretary of Defense should establish and employ a two-track acquisition system, one track for major acquisitions and a second “fast track” for a limited number of potential breakthrough systems, especially those for command and control.</p>	Hart–Rudman Commission	No known vehicle exists for implementation of a two-track acquisition system.
<p>Prototyping and Testing. The Secretary of Defense should foster innovation by directing a return to the pattern of increased prototyping and testing of selected weapons and support systems.</p>	Hart–Rudman Commission	Current strategy is ineffective. No vehicle exists for increased prototyping and testing.
<p>Expeditionary Capabilities. The Defense Department should devote its highest priority to improving and furthering expeditionary capabilities.</p>	Hart–Rudman Commission	Current strategy is ineffective and insufficient. Requires continued support and improvement.
<p>National Guard. The Secretary of Defense, at the President’s direction, should make homeland security a primary mission of the National Guard, and the Guard should be reorganized, properly trained, and adequately equipped to undertake that mission.</p>	Hart–Rudman Commission	National Guard is currently underutilized in homeland security. Requires reorganization of State Area Command (STARC) units to be able to mobilize more quickly and effectively.
<p>Note: Information on the reports issued by these commissions may be found in the bibliography.</p>		

APPENDIX

**TABLE A-1: STATUS OF ANTI-TERRORISM
ACTIONS BY THE EXECUTIVE BRANCH**

**TABLE A-2: STATUS OF ANTI-TERRORISM
LEGISLATION**

Table A-1

Status of Anti-Terrorism Actions by the Executive Branch

The status of key decisions made by the Chief Executive and Federal agencies to address homeland security needs is summarized below. Also included are actions taken by Administrations prior to September 11 that deal specifically with proposals or issues raised in this report.

Actions	Description	Status
Presidential Decision Directive 63 "Critical Infrastructure Protection"	Establishes 2003 deadline for formulating a national strategy to protect critical infrastructure. Designates 12 areas as critical: information and communications; banking and finance; water supply; transportation; emergency law enforcement; emergency fire service; emergency medicine; electric power, oil, and gas supply and distribution; law enforcement and internal security; intelligence; foreign affairs; and defense. Assigns a lead Federal agency to each.	Signed May 1998. Bureaucratic structure for assessing critical infrastructure largely in place, but not all recommendations of directive have been implemented.
Executive Order 13224 "Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism"	Places a suspension on assets and bank accounts of individuals and organizations suspected of terrorist involvement or activity	Signed September 23, 2001. Between September 11, 2001, and December 4, 2001, the United States blocked more than \$27.7 million in assets of the Taliban and the al-Qaeda network. Other nations have blocked at least \$33 million. Over 1,100 accounts are under review.
Executive Order 13228 "Establishing the Office of Homeland Security and the Homeland Security Council"	Creates the Office of Homeland Security with responsibility for coordinating government homeland security efforts. Creates the Homeland Security Council to advise the President.	Signed October 8, 2001.
Executive Order 13231 "Critical Infrastructure Protection in the Information Age"	Establishes information systems as critical infrastructure. Creates the President's Infrastructure Protection Board, with senior members of executive branch departments, agencies, and offices, which will advise the President and oversee government and private-sector protection efforts. Creates the National Infrastructure Advisory Council (NIAC) to provide the private-sector perspective.	Signed October 16, 2001. Neither the Board nor the Council has met as of December 13, 2001.
Presidential Order "Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism"	Establishes authority for military commissions to conduct trials involving non-U.S. citizens accused of terrorism or involvement with terrorist activities.	Signed October 13, 2001. Department of Defense is developing policies and procedures for military commissions, rules of procedure and evidence, and qualifications for counsel.
INS Restructuring Plan	Separates immigration services and immigration enforcement into two bureaus. Eliminates the Regional Director and District Director positions. Unifies the Office of General Counsel. Establishes a Chief Information Officer, an Ombudsman in the Bureau of Immigration Enforcement, and the Office of Juvenile Affairs.	Implemented November 14, 2001. INS Commissioner to appoint a Director of Restructuring who, with field managers, will try to change the reporting relationship while plans for agency restructuring are finalized. Reform should be completed by end of FY 2003.
FBI Reorganization Plan	Creates four new Executive Assistant Director positions to increase emphasis on counterterrorism and relations with State and Local law enforcement. Creates Cybercrime Division and Security Division to deal with computer-facilitated crime. Opens four offices: Law Enforcement Coordination, Chief Technology Officer, Office of Records Management, and Intelligence Office. Disbands the Investigative Services Division and integrates it into the new components. Phase II will include changes at the FBI Divisional and Office levels to eliminate duplication, realign resources, and consolidate functions.	Implemented December 3, 2001. Executive Assistant Directors have been hired under Phase I; Phase II is not yet implemented.
Department of Defense Reorganization Proposal	Reportedly establishes a Homeland Defense Command that would join one of the existing unified commands. Also requests two new Under Secretary of Defense positions for homeland security and intelligence.	Announcement of the Homeland Defense Command is expected soon. Leading candidates for this mission reportedly are the North American Aerospace Defense Command or the Joint Forces Command. The Secretary of Defense asked Congress on November 26, 2001, for the authority to create the two new Under Secretary positions and to include them in the FY 2002 authorization.

Table A-2

Status of Anti-Terrorism Legislation

The status of legislation to address the aspects of homeland security discussed in this report is summarized below. Every effort has been made to provide the most current information; however, due to the ongoing efforts of policymakers to protect the homeland, some of these proposals may have been implemented by the time this volume is released.

Title	Key Sponsors	Proposal	Status
Amending the Immigration and Nationality Act (S. 1424)	Senator Edward Kennedy (D-MA)	Amends the Immigration and Nationality Act to provide non-immigrant "S" visas to aliens who supply information about terrorist organizations to law enforcement agencies.	Enacted into law on October 1, 2001, as P.L. 107-45.
Airport and Seaport Terrorism Prevention Act (S. 1429)	Senator John Edwards (D-NC)	Improvement of security at airports and seaports.	Referred to Committee on Commerce, Science, and Transportation on September 14, 2001.
Federal Aviation Security Act (Sky Marshals Bill) (S. 1447)	Senator Ernest Hollings (D-SC)	Amends Federal transportation law to make FAA responsible for security at all U.S. airports and establishes the Aviation Security Coordination Council (nationalizes airport security).	Enacted into law on November 19, 2001, as P.L. 107-71.
Air Transportation Safety and System Stabilization Act (S. 1450)	Senators Thomas Daschle (D-SD) and Trent Lott (R-MS)	Compensates air carriers up to \$5 billion total for losses that are a result of the attacks on September 11, 2001.	Passed by the Senate on September 21, 2001, vitiated on September 22, 2001, and postponed indefinitely.
Critical Infrastructure Information Act of 2001 (S. 1456)	Senator Robert Bennett (R-UT)	Encourages disclosure and exchange of infrastructure information; enhances analysis, prevention, and detection of critical information.	Referred to Committee on Energy and Natural Resources on October 9, 2001.
A bill to authorize the President to provide assistance to Pakistan and India through September 30, 2003 (S. 1465)	Senator Sam Brownback (R-KS)	Authorizes the President to provide defense articles, services, or assistance to Pakistan and India through 2003 if in the best interests of preventing international terrorism.	Enacted into law on October 27, 2002, as P.L. 107-57.
State Bioterrorism Preparedness Act (S. 1520)	Senator Evan Bayh (D-IN)	Assists states in preparing for and responding to biological or chemical terrorist attacks.	Referred to Committee on Health, Education, Labor, and Pensions on October 9, 2001.
National Energy Infrastructure Security Program Establishment Act (S. 1529)	Senator Mary Landrieu (D-LA)	Directs the Assistant to the President for Homeland Security to establish the National Energy Infrastructure Security Program.	Referred to Committee on Energy and Natural Resources on October 10, 2001.
Combating Terrorism Act (S.Amdt. 1562 to H.R. 2500)	Senator Orrin Hatch (R-UT)	Requires a readiness assessment of the National Guard, recommendations by the Attorney General and HHS, improved recruitment of terrorist informants by the CIA, and a report on the legal authority of wiretapping.	Amendment passed on September 13, 2001. H.R. 2500 passed by the House on July 19, 2001, but motion to reconsider in Senate laid on the table on September 24, 2001

Table A-2 Cont.

Title	Key Sponsors	Proposal	Status
Water Infrastructure Security and Research Development Act (S. 1593)	Senator James Jeffords (I-VT)	Requires the Administrator of the Environmental Protection Agency to establish a grant program to support research projects on critical infrastructure protection for water supply systems.	Report filed in Committee on Energy and Public Works on December 10, 2001, and placed on legislative calendar.
Enhanced Border Security Act (S. 1618)	Senators Edward Kennedy (D-MA) and Sam Brownback (R-KS)	Enhances overall border security.	Referred to the Judiciary Committee on November 1, 2001.
Visa Entry Reform Act (S. 1627)	Senators Dianne Feinstein (D-CA) and Jon Kyl (R-AZ)	Secures the international borders throughout the United States.	Referred to the Judiciary Committee on November 1, 2001.
Bioterrorism Preparedness Act (S. 1765)	Senators Edward Kennedy (D-MA) and Bill Frist (R-TN)	Authorizes \$3.2 billion to address gaps in biodefense and surveillance systems. Focuses on Federal assistance to State and Local governments, public health emergency preparedness, development of pharmaceuticals, and enhancing safety of food supply.	Read twice and placed on the Senate calendar on December 5, 2001.
National Homeland Security Agency Act (H.R. 1158)	Representative Mac Thornberry (R-TX)	Establishes the National Homeland Security Agency.	Joint hearings held April 24, 2001, by Subcommittees on Economic Development, Public Buildings, and Emergency Management and National Security, Veterans Affairs, and International Relations.
Computer Security Enhancement Act (H.R. 1259)	Representative Constance Morella (R-MD)	Requires the Institute of Standards and Technology to develop uniform standards for the sensitive computer systems of Federal agencies.	Passed by the House on November 27, 2001; received in the Senate on November 28, 2001; referred to Committee on Commerce, Science, and Transportation.
National Missile Defense Deployment Criteria Act (H.R. 2786)	Representative Edward Markey (D-MA)	Provides deployment criteria for a national missile defense system and provides for operationally realistic testing of the system against countermeasures.	Referred to Committee on Armed Services, Committee on Rules, and Committee on International Relations on August 2, 2001.
Intelligence Authorization Act for Fiscal Year 2002 (H.R. 2883)	Representative Porter Goss (R-FL)	Authorizes appropriations for Intelligence Community (amounts classified) with increased reporting requirements for terrorist-related activities, requires the DCI to rescind the existing guidelines that hinder the recruitment of foreign assets.	Passed by the House on October 5, 2001, and by the Senate on November 8, 2001; sent to the President on December 18, 2001. Signed on December 28, 2001 (P.L. 107-108).
Emergency Supplemental Appropriations Act (H.R. 2888)	Representative C. W. (Bill) Young (R-FL)	Makes emergency supplemental appropriations of \$40 billion for disaster assistance, antiterrorism initiatives, and recovery efforts.	Enacted into law on September 18, 2001, as P.L. 107-38.
Air Transportation Safety and System Stabilization Act (H.R. 2926)	Representative Don Young (R-AK)	Provides \$5 billion compensation to the airline industry and caps the liability of an air carrier.	Enacted into law on September 22, 2001, as P.L. 107-42.

Table A-2 Cont.

Title	Key Sponsors	Proposal	Status
Aviation Security Improvement Act of 2001 (H.R. 2913)	Representative Jack Quinn (R-NY)	Directs FAA employees to carry out the screening of passengers and property on flights, instead of air-carrier employees.	Referred to the Subcommittee on Aviation on September 21, 2001.
Keeping America Safe Act (H.R. 2928)	Representative Robert Andrews (D-NJ)	Amends the Immigration and Nationality Act to provide for the removal of aliens who aid or abet a terrorist organization or individual.	Referred to the Subcommittee on Immigration and Claims on September 28, 2001.
Anti-Terrorism Act (H.R. 2975)	Representative James Sensenbrenner (R-WI)	Provides the appropriate tools to combat terrorism and amends the Foreign Intelligence Surveillance Act of 1978.	Passed by the House on October 12, 2001, and received by the Senate on October 15, 2001.
Financial Anti-Terrorism Act (H.R. 3004)	Representative Michael Oxley (R-OH)	Combats the financing of terrorism and other financial crimes.	Incorporated into Title III of PATRIOT Act (P.L. 107-56).
State Bioterrorism Preparedness Act (H.R. 3153)	Representative Rod Blagojevich (D-IL)	Assists states in preparing for and responding to biological or chemical terrorist attacks.	Referred to Committee on Energy and Commerce on October 17, 2001; referred to Subcommittee on Health on October 29, 2001.
Bioterrorism Prevention Act (H.R. 3160)	Representative Billy Tauzin (R-LA)	Amends the Antiterrorism and Effective Death Penalty Act of 1996 and requires HHS to create new regulations for biological agents.	Passed by the House on October 23, 2001, and received by the Senate on October 24, 2001.
USA PATRIOT Act (Uniting and Strengthening America Act) (H.R. 3162)	Representative James Sensenbrenner (R-WI)	Title I: Develops enhanced domestic security through modified presidential authority under the International Emergency Powers Act. Title II: Allows for interception of wire, oral, and electronic communication for counterintelligence surveillance. Title III: Enhances monitoring of international money laundering and abatement activity of individuals or institutions involved with terrorist activity. Title IV: Establishes enhanced border security and immigration measures. Title V: Removes obstacles to investigation of terrorists. Title VI: Provides aid to victims and families of victims of terrorism. Title VII: Increases information sharing for critical infrastructure protection. Title VIII: Strengthens the criminal law against terrorism. Title IX: Improves intelligence through stricter requirements for sharing intelligence information. Title X: Provides various amendments and appropriations to improve homeland security.	Enacted into law on October 26, 2001, as P.L. 107-56.
Cyber Security Enhancement Act (H.R. 3482)	Representative Lamar Smith (R-TX)	Increases cyber security levels.	Referred to the House Committee on the Judiciary on December 13, 2001.

A p p e n d i x

Table A-2 Cont.

Title	Key Sponsors	Proposal	Status
Visa Entry Reform Act (H.R. 3229)	Representative Elton Gallegly (R-CA)	Requires the Director of the Office of Homeland Security to establish and supervise a single computerized database to screen and identify inadmissible or deportable aliens and make the information available to immigration, Customs, law enforcement, and intelligence personnel. Also directs the establishment of a Terrorist Lookout Committee at each embassy and the development of machine-readable visas with biometric identification. Also provides for additional consular, Customs, and INS investigative personnel as well as the implementation and expansion of the foreign student monitoring program.	Referred to the House Subcommittee on Coast Guard and Maritime Transportation on November 7, 2001.
Seaport Security Enhancement Act (H.R. 3432)	Representative John Cooksey (R-LA)	Requires that the Coast Guard Sea Marshal program be carried out in the 20 ports in the U.S. considered by the Secretary of Transportation to be the most vulnerable to a terrorist attack by use of a commercial vehicle.	Referred to the House Committee on Transportation and Infrastructure on December 6, 2001.
Enhance the border security of the United States (H.R. 3525)	Representative James Sensenbrenner (R-WI)	Enhances the overall border security of the United States.	Passed under suspension of the rules by the House on December 19, 2001. Received by the Senate and referred to the Committee on the Judiciary on December 20, 2001.
USA ACT "To prevent, prepare for, and respond to the threat of terrorism in America, and for other purposes." (H.R. 3555)	Representative Robert Menendez (D-NJ) (House Democratic Task Force on Homeland Security Bill)	Proposes \$25 billion in spending on Homeland Security financed by freezing the top three tax rate cuts from the President's tax bill. Spending for homeland security includes \$2.1 billion to the CDC; \$9.1 billion for transportation security; \$2.7 billion to secure technology infrastructure; \$2 billion to Federal and Local government agencies; and \$183 million to improve interagency and intergovernmental coordination.	Referred on December 20, 2001 to the House Committee on Energy and Commerce, and in addition to the Committees on Transportation and Infrastructure, Education and the Workforce, Government Reform, Ways and Means, Armed Services, International Relations, Intelligence (Permanent Select), Financial Services, and the Judiciary
The Pipeline Infrastructure Protection to Enhance Security and Safety Act (H.R. 3609)	Representative Don Young (R-AK)	Obligates the Secretary of Transportation to require the operators of pipeline facilities to develop and implement a terrorism security program and provides for review of these programs by the Secretary.	Referred on December 20, 2001 to the Committee on Transportation and Infrastructure, and the Committee on Energy and Commerce

SELECTED BIBLIOGRAPHY

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission), *Toward a National Strategy for Combating Terrorism*, Washington, D.C., December 2000.

Baily, Dr. Kathleen C., *The Biological and Toxic Weapons Threat to the United States*, National Institute for Public Policy, Washington, D.C., October 2001.

Brake, Jeffrey D., *Terrorism and the Military's Role in Domestic Crisis Management: Background and Issues for Congress*, CRS Report for Congress, April 19, 2001.

Center for Strategic and International Studies, *Defending America in the 21st Century: New Challenges, New Organizations, New Policies*, CSIS Working Group Report on Homeland Defense, Washington, D.C., 2000.

Ciluffo, Frank J., Sharon L. Cardash, and Gordon N. Lederman, *Combating Chemical, Biological, Radiological and Nuclear Terrorism: A Comprehensive Strategy*, A Report of the CSIS Homeland Defense Project, Washington, D.C., May 2001.

Cordesman, Anthony H., *Defending America: Redefining the Conceptual Borders of the Homeland Defense; Homeland Defense: Coping with the Threat of Indirect, Covert, Terrorist and Extremists Attack with Weapons of Mass Destruction*, Executive Summary, Center for Strategic and International Studies, Washington, D.C., February 14, 2001.

———, *Defending America: Redefining the Conceptual Borders of the Homeland Defense; Homeland Defense: Terrorism, Asymmetric Warfare and Nuclear Weapons*, Final Draft, Center for Strategic and International Studies, Washington, D.C., February 14, 2001.

Defense Science Board, *Protecting the Homeland*, Washington, D.C., February 2001.

Department of Defense Plan for Integrating National Guard and Reserve Component Support for Response to Attacks Using Weapons of Mass Destruction, Prepared by the DOD Tiger Team, Washington, D.C., January 1998.

- Housman, Robert, and Dee Martin, *Protecting America's Critical Energy Infrastructure from Terrorist Attack*, released by Bracewell & Patterson LLP, November 7, 2001.
- Institute for Security Technology Studies at Dartmouth College, *Combating Terrorism: A Compendium of Recent Counterterrorism Recommendations from the Authoritative Commissions and Subject Matter Experts*, Hanover, N.H., September 16, 2001.
- Moteff, John D., *Critical Infrastructures: Background and Early Implementation of PDD-63*, CRS Report for Congress, June 2001.
- National Commission on Terrorism (Bremer Commission), *Countering the Changing Threat of International Terrorism*, Washington, D.C., 1998.
- National Defense Panel, *Transforming Defense: National Security in the 21st Century*, Arlington, Va., December 1997.
- Patrick, William C. III, *The Threat of Biological Warfare*, Transcript of Remarks Made at the George C. Marshall Institute Roundtable, Washington, D.C., February 13, 2001.
- President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, October 1997.
- Report of the Interagency Commission on Crime and Security in U.S. Seaports*, Washington, D.C., Fall 2000.
- Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities*, Washington, D.C., January 2001.
- Responding to the Biological Weapons Challenge: Developing an Integrated Strategy*, Report of a Senior Working Group of the Chemical and Biological Arms Control Institute, Alexandria, Va., 2000.
- Roberts, Brad, ed., *Terrorism with Chemical and Biological Weapons: Calibrating the Risks*, Chemical and Biological Arms Control Institute, Alexandria, Va., 1997.
- Select Commission on Immigration and Refugee Policy (Hesburgh Commission), *U.S. Immigration Policy and the National Interest: Final Report and Recommendations of the Select Commission on Immigration and Refugee Policy*, Washington, D.C., March 1981.

- Stevens, Paul Schott, *U.S. Armed Forces and Homeland Defense: The Legal Framework*, Center for Strategic and International Studies, Washington, D.C., October 2001.
- U.S. Commission on Immigration Reform (Jordan Commission), *U.S. Immigration Policy: Restoring Credibility: Report of the U.S. Commission on Immigration Reform*, Interim Report, 1994; Final Report, 1997.
- U.S. Commission on National Security/21st Century (Hart–Rudman Commission), *New World Coming: American Security in the 21st Century* (Phase I); *Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom* (Phase II); *Roadmap for National Security: Imperative for Change* (Phase III), Washington, D.C., 1999–2001.
- U.S. Department of Defense, *Quadrennial Defense Review*, Washington, D.C., 2001.
- U.S. Department of Transportation, *US Infrastructure Assurance Roadmaps*, Department of Transportation Status Report, August 1998.
- U.S. General Accounting Office, *Anthrax Vaccine: Changes to the Manufacturing Process*, Statement of Nancy Kingsbury, Ph.D., Managing Director, Applied Research and Methods, GAO–02–181T, October 23, 2001.
- , *Bioterrorism: Federal Research and Preparedness Activities*, GAO–01–951, September 2001.
- , *Bioterrorism: Coordination and Preparedness*, Statement of Janet Heinrich, Director, Health Care–Public Health Issues, GAO–02–129T, October 5, 2001.
- , *Bioterrorism: Public Health and Medical Preparedness*, Statement of Janet Heinrich, Director, Health Care–Public Health Issues, GAO–02–141T, October 9, 2001.
- , *Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination*, NSIAD–98–39, December 1997.
- , *Combating Terrorism: Opportunities to Improve Domestic Preparedness Program Focus and Efficiency*, NSIAD–99–3, November 1998.
- , *Combating Terrorism: Issues to Be Resolved to Improve Counterterrorist Operations*, NSIAD–99–135, May 1999.

- , *Combating Terrorism: Use of National Guard Response Teams Is Unclear*, T-NSIAD-99-184, June 1999.
- , *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attack*, NSIAD-99-163, September 1999.
- , *Combating Terrorism: Chemical and Biological Medical Supplies Are Poorly Managed*, GAO/HEHS/AIMD-00-36, October 29, 1999.
- , *Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction and Training*, NSIAD-00-64, March 2000.
- , *Combating Terrorism: Federal Response Teams Provide Varied Capabilities; Opportunities Remain to Improve Coordination*, GAO-01-14, November 2000.
- , *Combating Terrorism: Accountability Over Medical Supplies Needs Further Improvement*, GAO-01-463, March 30, 2001.
- , *Combating Terrorism: Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, April 2001.
- , *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822, September 2001.
- , *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences*, GAO/AIMD-00-1, October 1999.
- , *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323, April 2001.
- , *Information Sharing: Practices That Can Benefit Infrastructure Protection*, GAO-02-24, October 2001.
- White House Commission on Aviation Safety and Security (Gore Commission), *The White House Commission on Aviation Safety and Security*, Washington, D.C., February 12, 2001.

THE HERITAGE FOUNDATION'S VISION FOR AMERICA

The Heritage Foundation is committed to building an America where freedom, opportunity, prosperity, and civil society flourish.

MISSION STATEMENT

Founded in 1973, The Heritage Foundation is a research and educational institute—a think tank—whose mission is to formulate and promote conservative public policies based on the principles of free enterprise, limited government, individual freedom, traditional American values, and a strong national defense.

Heritage's staff pursues this mission by performing timely and accurate research addressing key policy issues and effectively marketing these findings to its primary audiences: members of Congress, key congressional staff members, policymakers in the executive branch, the nation's news media, and the academic and policy communities. Heritage's products include publications, articles, lectures, conferences, and meetings.

Governed by an independent Board of Trustees, The Heritage Foundation is a non-partisan, tax-exempt institution. Heritage relies on the private financial support of the general public—individuals, foundations, and corporations—for its income, and accepts no government funds and performs no contract work. Heritage is one of the nation's largest public policy organizations. More than 200,000 contributors make it the most broadly supported in America.

FOR A PUBLICATIONS CATALOG CONTACT:

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002-4999
1-800-544-4843
Fax: 202-543-9647

Or visit our online bookstore: *www.heritage.org/bookstore/*

