WHITE PAPER

RAND

Homeland Security

A Compendium of Public and Private Organizations' Policy Recommendations

John V. Parachini, Lynn E. Davis, Timothy Liston

National Security Research Division

Approved for public release; distribution unlimited

This publication was supported by RAND using its own funds.

ISBN: 0-8330-3351-4

RAND white papers are authoritative publications that draw on a strong body of prior research to summarize key findings relevant to pending decisions or policy problems. White papers are reviewed by RAND's corporate management to assure that they adequately represent RAND's best work in the subject as well as significant differences of opinion.

RAND is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND® is a registered trademark. RAND's publications do not necessarily reflect the opinions or policies of its research sponsors.

© Copyright 2003 RAND

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from RAND.

Published 2003 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact Distribution Services: Telephone: (310) 451-7002; Fax: (310) 451-6915; Email: order@rand.org

Preface

Providing for the security of the U.S. homeland is a multidimensional and complex effort involving federal, state, and local governments. Since the September 11 terrorist attacks, the Bush Administration has taken numerous steps to improve the nation's safety, including the creation of a new Department of Homeland Security. This paper provides a compendium of past recommendations from various public and private organizations on how the new department might achieve the ambitious goals of the *National Strategy for Homeland Security*, the administration's definitive statement of its plans for enhanced homeland security.

This study stems from RAND's continuing program of self-sponsored independent research. We acknowledge the support for such research provided, in part, by the independent research and development provisions of RAND's contracts for the operation of its U.S. Department of Defense federally funded research and development centers.

This research was overseen by RAND's National Security Research Division (NSRD). NSRD conducts research and analysis for the Office of the Secretary of Defense, the Joint Staff, the Unified Commands, the defense agencies, the Department of the Navy, the U.S. intelligence community, allied foreign governments, and foundations.

Comments and inquiries on the material contained in this document may be addressed to John_Parachini@rand.org, (703) 413-1100, extension 5579; or to Lynn_Davis@rand.org, (703) 413-1100, extension 5399.

Contents

Preface iii

Tables vii

Acknowledgments ix

1. INTRODUCTION 1

2. STRATEGY FOR HOMELAND SECURITY 5
   Background 5
   Unresolved Issues 5
   Allocation of Finite Resources 6
   Recommendations for a Comprehensive Strategy 7
      CSIS Report (Executive Summary of CSIS Working Group Reports) 7
      Gilmore Commission Second Annual Report 7
      Hart-Rudman Commission Report 8

3. SUBSTANTIVE POLICY INITIATIVES 11
   Intelligence and Warning of Threats or Attacks 11
      Bremer Commission Report (National Commission on Terrorism) 13
      Gilmore Commission Second Annual Report 14
      Gilmore Commission Fourth Annual Report 15
      CSIS Report (Executive Summary of CSIS Working Group Reports) 15
      Hart-Rudman Commission Report 16
      Brookings Institution Report 16
      Heritage Foundation Report 17
   Border and Transportation Security 17
      Gilmore Commission Third Annual Report 18
      Brookings Institution Report 19
      Heritage Foundation Report 19
   Domestic Counterterrorism Emergency Preparedness and Response, with Federal, State, and Local Coordination 21
      Gilmore Commission Second Annual Report 22
      Gilmore Commission Third Annual Report 23
      Hart-Rudman Commission Report 23
      Bremer Commission Report (National Commission on Terrorism) 23
      President's Critical Infrastructure Commission Report 23
      CSIS Report (Executive Summary of CSIS Working Group Reports) 24
      Heritage Foundation Report 24
   Protecting Critical Infrastructures and Key Assets 25
      Gilmore Commission Third Annual Report 25

CSIS Report (Executive Summary of CSIS Working Group Reports) 26
Bremer Commission Report (National Commission on Terrorism) 26
Brookings Institution Report 27
Heritage Foundation Report 27
Defending Against Catastrophic Threats 28
CSIS Report (Executive Summary of CSIS Working Group Reports) 29
Gilmore Commission Third Annual Report 29
Brookings Institution Report 30
Heritage Foundation Report 30
The Law 30
Bremer Commission Report (National Commission on Terrorism) 31
Gilmore Commission Third Annual Report 31
CSIS Report (Executive Summary of CSIS Working Group Reports) 32
Hart-Rudman Commission Report 32
Science and Technology 32
Bremer Commission Report (National Commission on Terrorism) 33
CSIS Report (Executive Summary of CSIS Working Group Reports) 33
Hart-Rudman Commission Report 33
Gilmore Commission Second Annual Report 34
Gilmore Commission Third Annual Report 35
Brookings Institution Report 35
Information Sharing and Systems 35
Heritage Foundation Report 36

4. CONCLUSIONS 37

Appendix
A. ORGANIZATIONS' MAJOR RECOMMENDATIONS 39
B. COMMISSION MEMBERS 47

Bibliography 57

Tables

A.1. Recommendations on Intelligence and Warning 40
A.2. Recommendations on Border and Transportation Security 41
A.3. Recommendations on Domestic Counterterrorism Emergency Preparedness and Response, with Federal, State, and Local Coordination 42
A.4. Recommendations on Protecting Critical Infrastructures and Key Assets 43
A.5. Recommendations on Defending Against Catastrophic Threats 44
A.6. Recommendations on the Law 45
A.7. Recommendations on Science and Technology 46

Acknowledgments

We wish to thank those who reviewed this paper along the way to its completion. Suzanne Spaulding, former staff director of the National Commission on Terrorism, and Frank Hoffman, a former Study Group Member for the U.S. Commission on National Security/21st Century, helped to clarify the recommendations in this paper from the commissions and other organizations. The document's reviewers—Lois Davis, Michael Wermuth, and William Rosenau of RAND—all provided valuable comments that helped us to create a document that we hope enhances the effectiveness of the new Department of Homeland Security. Tamara Hemphill provided valuable administrative support on earlier versions of this document, Rachel Swanger helped to manage the study project and ensure its completion, and Nancy DelFavero edited the document with great care and considerably improved the final product.

1. Introduction

Over the past several years, a number of public and private institutions, advisory panels, and various "think tanks" have addressed the challenge of how to best approach the task of providing security for the U.S. homeland. The mandates of each of these organizations have differed, as have their areas of focus. Some groups have dealt solely with the three major aspects of the homeland security challenge—intelligence, counterterrorism, and critical infrastructure—and other groups have addressed other aspects of homeland security as well as the three main ones. However, all of these efforts have criticized the lack of a guiding U.S. homeland security strategy, and all have found deficiencies in the U.S. government's organization and processes for dealing with threats to national security.[1]

In the aftermath of the September 11 terrorist attacks, President George W. Bush undertook major changes in the way the Executive Branch is organized in order to better deal with the various aspects of homeland security. He first created within the White House an Office of Homeland Security, headed by the Assistant to the President for Homeland Security.[2] The president also established a new interagency coordinating body, the Homeland Security Council. In June 2002, he went on to propose a new Department of Homeland Security with four divisions: Border and Transportation Security; Emergency Preparedness and Response; Chemical, Biological, Radiological, and Nuclear Countermeasures; and Information Analysis and Infrastructure Protection (Bush, 2002a). The U.S. Congress in legislating the establishment of the new department endorsed most of the president's proposals, with only some refinements.[3]

As the Department of Homeland Security assumes its responsibilities, the past findings of various organizations can offer important guidance to the new department.[4] This paper presents various advisory groups' major

---

[1]Most of the recommendations that these groups have made regarding a strategy for homeland security were offered before the September 11 terrorist attacks, and some were formulated following those events.

[2]See The White House (2001) for a description of the functions and responsibilities of the three components of the homeland security organization (the Office of Homeland Security, the Homeland Security Council, and the Director of the Office of Homeland Security).

[3]On November 25, 2002, President George W. Bush signed H.R. 5005, the Homeland Security Act of 2002, which establishes the Department of Homeland Security.

[4]These commissions and think tanks have paid significant attention to how the U.S. government should be organized for homeland security, given the consensus that has emerged with the Bush

recommendations on strategic and substantive policy issues, which have not yet been adopted by the Bush Administration but that we feel warrant additional examination. This paper uses as its framework the six critical mission areas and four foundations of homeland security, as defined in President Bush's *National Strategy for Homeland Security* (Bush, 2002b) and as listed later in this introduction.

The *National Strategy for Homeland Security* is the statement of plans and goals for the federal government's activities regarding homeland security. When President Bush sent it to Congress on July 16, 2002, he described the document as a "comprehensive plan" that "lays out clear lines of authority and clear responsibilities; responsibilities for federal employees and for governors and mayors and community and business leaders and the American Citizens" (Office of the Press Secretary, 2002). In the *National Strategy for Homeland Security,* the president stated the need for money and manpower to be reallocated to increase homeland security.

As noted earlier, the *National Strategy for Homeland Security* identifies six critical mission areas and four foundations of homeland security.[5] The critical mission areas are intelligence and warning, border and transportation security, domestic counterterrorism emergency preparedness and response, protecting critical infrastructures and key assets, defending against catastrophic threats, and emergency preparedness and response (we address all but the last mission area in this paper). The four foundations are the law, science and technology, information sharing and systems, and international cooperation (again, we address all but the last foundation). Also included in the national strategy is a statement of basic principles to guide the allocation of funding for homeland security and a statement of priorities for the future of U.S. counterterrorism activities.

The *National Strategy for Homeland Security* states its primary objective as follows:

> [The] *National Strategy for Homeland Security* has set a broad and complex agenda for the United States. The Strategy has defined many different goals that need to be met, programs that need to be implemented, and responsibilities that need to be fulfilled. The principal purpose of a strategy, however, is to set priorities. It is particularly important for government institutions to set priorities explicitly, since these institutions generally lack a clear measure of how successfully they provide value to citizenry (Bush, 2002b).

Administration's plans that call for both a White House office and a new department for homeland security.

[5]In this paper, we address only five of the six critical mission areas and only three of the four foundations because the reports we reviewed for this study did not offer major recommendations on every mission area and foundation.

For this study, we reviewed independent reports on terrorism prepared by several public and private groups. The reports were widely distributed and extensively reviewed by the Bush Administration, and were discussed in congressional hearings and in the news media. The reports represent most of the significant efforts to date concerning recommended policy changes and policy initiatives to enhance homeland security.

The reports we reviewed are as follows:

- *Protecting the American Homeland: A Preliminary Analysis,* Washington, D.C.: Brookings Institution Press, 2002; www.brook.edu/dybdocroot/ (hereafter referred to in this paper as the Brookings Institution Report).
- *Defending the American Homeland: A Report of the Heritage Foundation Homeland Security Task Force,* Washington, D.C.: The Heritage Foundation, January 2002; www.heritage.org (hereafter referred to in this paper as the Heritage Foundation Report).
- Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (known as the Gilmore Commission; www.rand.org/nsrd/terrpanel/); *Toward a National Strategy for Combating Terrorism,* Second Annual Report to the President and the Congress, December 15, 2000 (hereafter referred to in this paper as the Gilmore Commission Second Annual Report); *For Ray Downey,* Third Annual Report to the President and the Congress, December 15, 2001 (hereafter referred to as the Gilmore Commission Third Annual Report); and *Implementing the National Strategy,* Fourth Annual Report to the President and the Congress, December 15, 2002 (hereafter referred to as the Gilmore Commission Fourth Annual Report).[6]
- U.S. Commission on National Security/21st Century (known as the Hart-Rudman Commission; www.nssg.gov), *Road Map for National Security: Imperative for Change,* Phase III Report, February 15, 2001 (hereafter referred to in this paper as the Hart-Rudman Commission Report).
- Center for Strategic and International Studies (CSIS; www.csis.org), *Defending America in the 21st Century,* Executive Summary of Four Working Group Reports on Homeland Defense, Washington, D.C.: CSIS, 2000; available at www.csis.org/homeland/reports/defendamer21stexecsumm.pdf (hereafter referred to in this paper as the CSIS Report).

[6]At the time of this study, the fourth annual report contained only a limited number of advance recommendations. Since then, the complete report has been issued.

- National Commission on Terrorism (the National Commission or Bremer Commission), *Countering the Changing Threat of International Terrorism,* June 7, 2000, available at http://w3.access.gpo.gov/nct/ (hereafter referred to in this paper as the Bremer Commission Report).
- The President's Commission on Critical Infrastructure Protection (President's Critical Infrastructure Commission), Critical Infrastructure Assurance Office, *Critical Foundations Protecting America's Infrastructures,* October 1997, available at www.ciao.gov/resource/pccip/report_index.htm (hereafter referred to in this paper as the President's Critical Infrastructure Commission Report).

In Sections 2 and 3 of this paper, we quote recommendations from these reports verbatim. In only a few cases do the reports offer the same recommendations on a given topic. We cite these excerpts so that readers can use this paper as a guide for further individual study of the reports. However, many of the substantive recommendations[7] in the reports require further examination and analysis before they can be seriously considered for adoption by the U.S. government. Section 4 offers our conclusions on the reports' various recommendations.

Appendix A of this paper lists the major recommendations that the Bush Administration has not already adopted or announced as being among its major initiatives in the *National Strategy for Homeland Security*, but which we feel warrant additional examination. The appendix is organized according to the critical mission areas and foundations identified in the strategy statement. Organized in this fashion, the appendix serves as a checklist of commission recommendations that the various offices of the new department and the appropriate congressional oversight committees may consider as they move forward in formulating a comprehensive U.S. homeland security strategy. Appendix B lists the members of the commissions and other groups that produced the reports that we quote in this paper.

[7] As opposed to recommendations that focus on governmental organization or overall strategy, substantive recommendations address specific tactical issues concerning intelligence or scientific research, for example.

2. Strategy for Homeland Security

Background

President George W. Bush's *National Strategy for Homeland Security* outlines and prioritizes the nation's objectives in this critical area: "Prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism; and minimize the damage and recover from attacks that do occur" (Bush, 2002b, p. 3). This national strategy statement gives the new Department of Homeland Security "a central role" in implementing the national strategy and directs the new department to "serve as the primary federal point of contact for state and local governments, the private sector, and the American people" (Bush, 2002b, p. 5). As also outlined in the strategy, after the new department is established, "the White House Office of Homeland Security will continue to play a key role in advising the President and coordinating the interagency process." The office will also "certify that the budgets of other executive branch departments will enable them to carry out their homeland security responsibilities" (Bush, 2002b, p. 13).

The *National Strategy for Homeland Security* also calls for the federal government to divide homeland security functions into six critical mission areas: intelligence and warning, border and transportation security, domestic counterterrorism emergency preparedness and response, protection of critical infrastructures and key assets, defense against catastrophic threats, and emergency preparedness and response. The statement also outlines the critical foundations for homeland security: the law, science and technology, and information sharing and systems. (In Section 3 of this paper, we present various organizations' recommendations in these areas.)

Unresolved Issues

A number of commissions, government advisory panels, and think tanks have long called for the president to develop and promulgate an overall strategy for U.S. domestic security. The *National Strategy for Homeland Security* captures this general recommendation and examines it with an eye toward greater specificity. But what is still missing, as suggested by the commissions and organizations whose reports on domestic security are the subject of this paper, is a strategy that covers activities beyond those of the federal government. The establishment of

the Department of Homeland Security as the primary contact for state and local authorities addresses this issue, but, as these organizations have pointed out, many other deficiencies in the relationship between state and local authorities and the federal government still exist. While establishing a primary point of contact for state and local governments, the private sector, and the public is an important step in creating a national strategy for homeland security, many issues remain unresolved by this organizational change.

State and local authorities will look to the Department of Homeland Security for guidance on issues ranging from equipment acquisition to personnel training to coordination with federal law enforcement authorities. How effectively the new department leadership handles some of these issues in the early days of the department's operation presents a prime opportunity to affirm the importance of the department's creation.

Allocation of Finite Resources

Allocation of finite homeland security resources is a critical challenge for all levels of government, and state and local authorities have been looking to the federal government for guidance in this area. Allocation and prioritization of federal dollars to state and local responders will help to solidify a lasting relationship between the new department and the terrorism response community. Unfortunately, the organizations whose reports we reviewed offer scant guidance on how to prioritize and allocate funds among a host of important missions.

All but one of the reports we reviewed for this paper failed to indicate the budgetary implications of the recommendations contained within them. The exception is the Brookings Institution Report, which consistently weighs the dollar costs of its recommendations. Although there is some merit in crafting recommendations that are free from budgetary constraints that might unduly constrain creative thinking, government departments and agencies ultimately must make judgment calls on how to allocate finite resources.

As the U.S. government seeks to enhance homeland security, an understanding of the budgetary implications of the organizations' various recommendations is of critical importance to the national leadership. None of the three congressionally established commissions whose reports we reviewed—the National Commission on Terrorism, the Hart/Rudman Commission, and the Gilmore Commission—addresses the budgetary issues surrounding the enhancement of homeland security. A significant challenge that policymakers will face in the future is how to manage the trade-offs between the need to create

a national strategy of homeland security and the need to effectively manage available resources.

The U.S. Congress requires the Executive Branch to file an annual report on the government's funding of counterterrorism and antiterrorism programs (*Annual Report to Congress on Combating Terrorism*, 2002). In that report, the Executive Branch provides spending figures and justification for its budget allocations for counterterrorism efforts. The annual budget requests from the new Department of Homeland Security will provide further details on how the government plans to allocate resources for homeland security.

Once the new department submits its annual budget to congressional committees, the process of budgeting and balancing of trade-offs begins. To avoid the vicissitudes that are typical in intergovernmental budgeting, the country would be well served if the new department could link its budget requests to an overarching homeland security strategy.

Recommendations for a Comprehensive Strategy

What follows are general recommendations on how the federal government might shape a national strategy for addressing terrorist threats. As stated in Section 1, these are, in our opinion, the major recommendations that the Bush Adminstration has not already adopted but that warrant further examination. These recommendations are taken verbatim from the reports we reviewed for this paper.

CSIS Report (Executive Summary of CSIS Working Group Reports)

"The most obvious need in the area of homeland defense is a national plan and a comprehensive, multiyear program. . . . A national plan . . . must encompass federal-, state-, and local-level responsibilities. This plan must include threat assessments, objectives, key concepts, and means. It would cover all details of the nation's defense against terrorists, as well as plans for critical infrastructure protection" (CSIS Report, 2000, pp. 9, 13).

Gilmore Commission Second Annual Report

"The next President [should] develop and present to the Congress a national strategy for combating terrorism within one year of assuming office. The next Administration should begin this process of developing a national strategy by a thoughtful articulation of national goals (ends) of the program, focusing on

results rather than process. The structure and specifics of the national program should derive logically and transparently from the goals, not the other way around" (Gilmore Commission Second Annual Report, 2000, p. 3).

"Essential Characteristics of a Comprehensive Functional Strategy for Combating Terrorism: national in scope not just federal; appropriately resourced and based on measurable performance objectives; focused on the full range of deterrence, prevention, preparedness, and response across the spectrum of threats—domestic and international; for domestic programs, built upon requirements from and fully coordinated with relevant local, state, and federal authorities" (Gilmore Commission Second Annual Report, 2000, p. 4).

"The first step in developing a coherent national strategy is for the Executive Branch to define some meaningful, measurable expression of what it is trying to achieve in combating terrorism . . . The national strategy must express preparedness goals in terms of an 'end state' toward which the program strives . . . The nation's strategy for combating terrorism requires results-based goals" (Gilmore Commission Second Annual Report, 2000, p. 5).

"Setting priorities is essential in any strategy, but priorities require clear, results-based objectives. With some meaningful sense of objectives, it will be possible to develop coherent priorities and an appropriate set of policy prescriptions. For instance, should the nation seek a different level of preparedness for large urban centers than for rural areas?"(Gilmore Commission Second Annual Report, 2000, p. 6).

"The strategy must be approved by the President and updated annually. . . . The strategy must contain a detailed implementation plan, with specific milestones for its accomplishment. Most important, the strategy must articulate a methodology for continually measuring and monitoring domestic preparedness. That methodology must be accomplished in close coordination with the States" (Gilmore Commission Second Annual Report, 2000, p. 8).

Hart-Rudman Commission Report

"The President should develop a comprehensive strategy to heighten America's ability to prevent and protect against all forms of attack on the homeland, and to respond to such attacks if prevention and protection fail" (Hart-Rudman Commission Report, 2001, p. 10).

"We believe that homeland security can best be assured through a strategy of 'layered defense' that focuses first on prevention, second on protection, and third

on response . . . Preventing a potential attack comes first. . . . Most broadly, the first instrument is U.S. diplomacy . . . The second instrument of homeland security consists of U.S. diplomatic, intelligence, and military presence overseas . . . Vigilant systems of border security and surveillance are a third instrument" (Hart-Rudman Commission Report, 2001, pp. 11–12).

In the next section, we present major recommendations for substantive policy initiatives on homeland security that have not yet been adopted by the Bush Administration.

3. Substantive Policy Initiatives

Given their specific mandates and areas of interest, the organizations whose reports we examined for this paper offer various recommendations for substantive policy initiatives in the area of U.S. homeland security. In only a few instances do their recommendations address similar problem areas. This paper does not contain all of the organizations' recommendations on homeland security, nor does it contain recommendations that have already been adopted by the Bush Administration. Rather, it captures only the major recommendations that have yet to be adopted by Executive Branch departments and agencies.

In the following subsections, we present recommendations on five of the six critical mission areas (intelligence and warning, border and transportation security, domestic counterterrorism emergency preparedness and response, protection of critical infrastructures and key assets, and defense against catastrophic threats) and three of the four foundations of a homeland security strategy (the law, science and technology, and information sharing and systems) identified in the *National Strategy for Homeland Security*.[1]

Intelligence and Warning of Threats or Attacks

After the September 11 attacks, the Bush Administration generally eschewed calls to restructure the intelligence community. Instead, the administration increased spending on the intelligence community's counterterrorism capabilities, sought to reorient the Federal Bureau of Investigation (FBI) to be more proactive, and urged better sharing of information among the FBI, the intelligence community, and border security entities.

As stated in a February 2003 press release from the White House, the president announced in his second State of the Union address a new initiative calling upon the "the Director of Central Intelligence, the Director of the FBI, working with the Attorney General, and the Secretaries of Homeland Security and Defense to develop the Nation's first unified Terrorist Threat Integration Center." The new center, headed by an official who will report to the Director of Central Intelligence, "will merge and analyze terrorist-related information collected

[1]The reports that we reviewed for this paper did not offer major recommendations regarding all of the mission areas and foundations.

domestically and abroad in order to form the most comprehensive possible threat assessment" (Office of the Press Secretary, 2003).

The Department of Homeland Security has been given the mission of "information analysis," i.e., to fuse intelligence and law enforcement information with the goal of preventing terrorist attacks. The *National Strategy for Homeland Security* stresses the critical role that the intelligence community plays in creating a national homeland security strategy and how homeland security must now be specifically included in the scope of the community's intelligence collection and analysis activities.

According to the national strategy statement, "The intelligence community must enhance its capacity to obtain intelligence relevant to homeland security requirements" (Bush, 2002b, p. 17). In applying this new focus to potential and actual threats to the homeland, the document states, "The new Department will provide real-time actionable information—in the form of protective actions that should be taken in light of terrorist threats, trends, and capabilities, and U.S. vulnerability—to policymakers, federal, state, and local law enforcement agencies and the private sector, based on the review and analysis of homeland security information."

As did a few of the reports we studied, the *National Strategy for Homeland Security* urges that the FBI develop an analytic intelligence capability. Similarly, it also proposes that the Department of Homeland Security take responsibility for conducting comprehensive vulnerability assessments, which several of the organizations also suggested in various ways. The *National Strategy for Homeland Security* also proposes that the Department of Homeland Security implement a Homeland Security Advisory system that will disseminate "information regarding the risk of terrorist acts to federal, state, and local authorities, the Private sector, and the American People" (Bush, 2002b, p. 18).

However, the issue of how the intelligence community can best be structured to meet the perceived needs of the homeland security mission remains an area of contention between the Bush Administration and some members of Congress. Almost all the commissions and other organizations limited their focus to offering recommendations on how the FBI, the White House, and the CIA should conduct their counterterrorism operations, and specifically, offer recommendations on how the Department of Homeland Security can best pursue its intelligence and warning responsibilities.[2]

---

[2]In its fourth annual report, the Gilmore commission proposed a "National Counter Terrorism Center." Although there are some similarities between this proposal and President Bush's Terrorist

A fundamental issue that remains to be addressed after examining the commissions' reports and the national strategy statement is how the intelligence community should be sharing sensitive information. Intelligence officials fear that information they may have on foreign terrorists that is shared with the FBI or state and local officials, for example, might be disclosed during the trial process. Additionally, the extent of the intelligence sharing that some of the reports have recommended would be unprecedented. A huge backlog already exists for clearing federal employees and contractors to enable them to work with classified information. Extending access to classified information to potentially thousands of state and local officials will only add to the burden of security clearance investigators.

The following subsections contain a selection of the major recommendations offered by the advisory panels on issues related to intelligence and warning that have not already been adopted by the Bush Administration.

Bremer Commission Report (National Commission on Terrorism)

"The FBI's terrorism investigations are governed by two sets of Attorney General guidelines. [One set of guidelines is] the guidelines for Foreign Intelligence Collection and Foreign Counterintelligence Investigations, which are classified and cover the FBI's investigations of international terrorism. . . . Domestic terrorism is governed by [the second set of guidelines,] the Attorney General guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations. The Attorney General and the Director of the Federal Bureau of Investigation should develop guidance to clarify the application of both sets of guidelines. This guidance should specify what facts and circumstances merit the opening of a preliminary inquiry or full investigation and should direct agents in the field to investigate terrorist activity vigorously, using the full extent of their authority" (Bremer Report, 2000, pp. 9–10).

"The Attorney General should direct that the Office of Intelligence Policy and Review not require information in excess of that actually mandated by the probable cause standard in the Foreign Intelligence Surveillance Act statute . . . [and should] substantially expand the Office of Intelligence Policy and Review staff and direct it to cooperate with the Federal Bureau of Investigation" (Bremer Report, 2000, p. 12).

Threat Integration Center (TTIC), there are also some significant differences. The text of the Gilmore Commission Fourth Annual Report recommendation is quoted on page 15.

"The President should direct the Director of Central Intelligence, the Secretary of Defense, and the Director of the Federal Bureau of Investigation to work with Congress to ensure that adequate resources are devoted to meet essential technology requirements of the National Security Agency and the Federal Bureau of Investigation and to expand and accelerate the DCI's [Director of Central Intelligence's] Counterterrorist Center's activities" (Bremer Report, 2000, p. 15).

"The Attorney General should clarify what information can be shared and direct maximum dissemination of terrorist-related information to policymakers and intelligence analysts consistent with the law" (Bremer Report, 2000, p. 16).

Gilmore Commission Second Annual Report

"We recommend that an Assistant Director for Intelligence in the National Office direct the intelligence function for Combating Terrorism, [and] should be 'dual-hatted' as the National Intelligence Officer (NIO) for Combating Terrorism at the National Intelligence Council . . . [and we recommend] the establishment of a 'Council to Coordinate Intelligence for Combating Terrorism' to provide strategic direction for intelligence collection and analysis, as well as a clearance mechanism for product dissemination and other related activities" (Gilmore Commission Second Annual Report, 2000, pp. 9–10).

"We recommend a thorough review, by a panel of Department of Justice (DOJ) officials and knowledgeable citizens outside the Federal government, of the terrorism portion of the Attorney General's 'Domestic Guidelines' . . . We recommend that the panel review the domestic guidelines for clarity, in the interests of strengthening them, while providing for the protection of civil rights and liberties" (Gilmore Commission Second Annual Report, 2000, p. 21).

"The Foreign Intelligence Surveillance Act (FISA) governs domestic national security investigations. The procedures of the Office of Intelligence Policy and Review (OIPR) in the Department of Justice, required to present a matter to the special Foreign Intelligence Surveillance Court established under FISA, require far more justification than the Act does. We recommend that the Attorney General direct OIPR to modify its procedures to conform to the FISA statutory requirements" (Gilmore Commission Second Annual Report, 2000, p. 21).

"We recommend that the National Office for Combating Terrorism provide coordination and advocacy for both foreign and domestic terrorism-related intelligence activities, including the development of national net assessments of terrorist attacks" (Gilmore Commission Second Annual Report, 2000, p. 8).

Gilmore Commission Fourth Annual Report

"Recommendation: That the President direct the establishment of a National Counter Terrorism Center (NCTC). That entity should be a 'stand-alone' organization outside of the FBI, CIA, or the proposed Department of Homeland Security (DHS). The objective is to consolidate in one entity the analysis of foreign-collected and domestically collected intelligence and information on international terrorists and terrorist organizations [that] threaten attacks against the United States" (Gilmore Commission Fourth Annual Report, 2002, p. 1).

"Recommendation: That the collection of intelligence and other information on international terrorist activities inside the United States, including the authorities, responsibilities and safeguards under the Foreign Intelligence Surveillance Act (FISA), which are currently in the FBI, be transferred to the NCTC . . . The collection component of the NCTC should be based on the concept of the Foreign Terrorist Tracking Task Force created by the Attorney General in the Fall of 2002—multiple-agency representation and robust technological capabilities—but with authority to collect intelligence and information within the United States" (Gilmore Commission Fourth Annual Report, 2002, p. 4).

CSIS Report (Executive Summary of the CSIS Working Group Reports)

"Invest in all-source intelligence capabilities. Multidisciplinary intelligence collection is crucial to provide indications and warning of a possible attack as well as insights into the cultures and mind-sets of terrorist organizations and to illuminate key vulnerabilities that can be exploited and leveraged to disrupt terrorist activities before they occur" (CSIS Report, 2000, p. 16).

"Invest in intelligence analytical capabilities. The intelligence community, including the FBI, must invest in expertise—linguists, CBRN [chemical, biological, radiological, and nuclear] weapons experts, and regional specialists—to buttress its analytical ability to track terrorists who consider using CBRN weapons"(CSIS Report, 2000, p. 17).

"Invest in detection and attribution capabilities. A credible retaliatory capability, essential for effective deterrence, depends on a strong attribution capability to identify the perpetrators and their supporters. These capabilities include laboratory facilities, other equipment, and the personnel necessary for CBRN attribution" (CSIS Report, 2000, p. 16).

"Carry out a 'Net Assessment of Intelligence Capabilities to Deal with Asymmetric Terrorist Attacks.' Develop a comprehensive net assessment of current and projected U.S. intelligence capabilities to deal with the problems of warning, detection, defense, targeting, and damage assessment, with a supporting net technical assessment of the capabilities to use national technical means and the current and future capabilities of key organizations like the National Security Agency and the National Reconnaissance Office, and the role of human intelligence" (CSIS Report, 2000, p. 17).

"Tighten coordination among the nonproliferation, counterproliferation, and counterterrorism communities. Rotational assignments at the analyst level should be encouraged"(CSIS Report, 2000, p. 17).

Hart-Rudman Commission Report

"The President should order the setting of national intelligence priorities through National Security Council guidance to the Director of Central Intelligence" (Hart-Rudman Commission Report, 2001, p. 23).

"The intelligence community should place new emphasis on collection and analysis of economic and science/technology security concerns, and incorporate more open-source intelligence into analytical products. Congress should support this new emphasis by increasing significantly the National Foreign Intelligence Program (NFIP) budget for collection and analysis" (Hart-Rudman Commission Report, 2001, p. 25).

"This Commission, in sum, urges an overall increase in the NFIP budget to accommodate greater priority placed on non-military intelligence challenges. Military intelligence needs also remain critical, however, so a simple reallocation of existing resources will not suffice. To ensure the continuing technological strength of the community, and to build cutting-edge intelligence platforms, there is no escaping the need for an increase in overall resources for the intelligence community" (Hart-Rudman Commission Report, 2001, p. 26).

Brookings Institution Report

"The Bush administration has proposed increasing FBI counterterrorist staffing by 450 individuals. We believe that a much larger expansion may be required . . . Devoting 5,000 agents, analysts, and language specialists to counterterrorism and counterintelligence . . . seems warranted" (Brookings Institution Report, 2002, p. 32).

Heritage Foundation Report

"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 OHS Director should establish a national strategy to protect the homeland based on the national assessments" (Heritage Foundation Report, 2002, pp. 56–57).

"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" (Heritage Foundation Report, 2002, pp. 58–59).

"Cabinet Secretaries with law enforcement responsibilities should hold LEA [law enforcement agency] officials accountable for both the quality of their intelligence collection and their ability to collect evidence to develop a case for prosecution . . . State and Local governments should reestablish LEA intelligence units . . . 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" (Heritage Foundation Report, 2002, p. 60).

"The Attorney General—through the FBI Director and the relevant SAC [FBI Special Agent in Charge] 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" (Heritage Foundation Report, 2002, p. 60).

Border and Transportation Security

The Bush Administration proposes to consolidate all relevant government entities responsible for border and transportation security into the Department of Homeland Security. As stated in the *National Strategy for Homeland Security*, "the Department of Homeland Security will manage who and what enters our homeland in order to prevent the entry of terrorists and the instruments of terror while facilitating the legal flow of people, goods, and service on which our economy depends" (Bush, 2002b, p. 22). This initiative echoes the recommendations of a few of the organizations whose reports we reviewed,

but it is bolder in capturing far more government entities and personnel who are involved in border and transportation security.

The *National Strategy for Homeland Security* further states that "the United States will screen and verify the security of goods and identities of people before they can harm the international transportation system," and "will require visitors to present travel documentation that includes biometric identifiers." It proposes that the new Department of Homeland Security "develop and deploy non-intrusive inspection technologies to ensure rapid and more thorough screening of goods and conveyances." As part of this effort, the *National Strategy for Homeland Security* calls for establishing "security criteria to identify high-risk containers," placing "inspectors at foreign seaports" and "recapitalizing the U.S. Coast Guard" (Bush, 2002b, p. 23). The new department will also be charged with "track[ing] and monitor[ing] international students and exchange visitors" (Bush, 2002b, p. 23). What the commissions and other organizations quoted in this paper do in this regard is suggest ways to implement these general goals in practice.

Although the commissions and other organizations have identified a number of valuable approaches and technologies to enhance border and transportation security, they do not offer guidance on two critical issues: privacy and cost. Enhancing security at border crossings and at major transportation hubs will raise significant issues of personal privacy. While there is considerable eagerness on the part of members of Congress, the news media, and the public to provide intelligence and law enforcement authorities with greater resources to prevent another terrorist attack, the budget requirements for these resources must be accompanied by modifications to some legal and administrative restrictions on FBI and CIA activities to combat terrorism. Inevitably, achieving greater security while safeguarding personal privacy may entail a considerable amount of new federal expenditures (e.g., to upgrade aging computer systems, train staff to focus on asymmetric threats, and develop new approaches to detection and prevention). These issues were largely unaddressed in the documents we reviewed for this paper.

In the following subsections, we quote selected recommendations on border and transportation security that the Bush Administration has not already adopted.

Gilmore Commission Third Annual Report

"We recommend that the Congress enact legislation requiring all shippers to submit cargo manifest information on any shipment transiting U.S. borders at a minimum simultaneous with the arrival of such goods at any U.S. port of entry, with the imposition of severe penalties for noncompliance . . . [and] in

consultation with other Executive Branch agencies, expand Coast Guard authority to include vessels that are owned in a majority percentage by U.S. persons" (Gilmore Commission Third Annual Report, 2001, pp. 38–39).

"We recommend that the Office of Homeland Security develop a coordinated, fully resourced plan for R&D and for fielding and integration of sensor and other detection and warning systems . . . [and that] the U.S. government negotiate more comprehensive treaties and agreements with Canada and Mexico for combating terrorism" (Gilmore Commission Third Annual Report, 2001, pp. 39–40).

"We recommend that the Office of Homeland Security ensure that all agencies with border responsibilities are included as full partners in the intelligence collection, analysis, and dissemination process, as related to border issues" (Gilmore Commission Third Annual Report, 2001, p. 37).

"We recommend that the President direct the establishment of a 'Trusted Shipper' program within the relevant agencies of government . . . The Congress should provide authority and resources to Federal enforcement agencies for granting incentives to Trusted Shippers, in the form of facilitated shipping process and financial assistance for using enhanced technology" (Gilmore Commission Third Annual Report, 2001, p. 38).

Brookings Institution Report

"[G]iving local law enforcement officers access to federal databases could help them find individuals who no longer belong in the country. Local agencies may then need help with investments in information systems" (Brookings Institution Report, 2002, p. 41).

"Like some shippers clearing Customs, trucking firms might qualify for an 'EZ-pass' as part of a tighter security system. Such firms would undertake detailed background checks of drivers and would have biometric features to ensure that only approved drivers operate trucks carrying hazardous materials. The firms could introduce GPS [global positioning system] monitoring of truck movements, [and] remote disabling systems to stop a truck that had been hijacked" (Brookings Institution Report, 2002, p. 46).

Heritage Foundation Report

"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 . . . 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 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" (Heritage Foundation Report, 2002, p. 25).

"The Administration should create an interagency center to analyze data on people and products entering the United States by sea. This interagency center . . . would cross-check passenger, crew, and cargo manifests of all vessels entering American territorial waters with all Federal watch lists" (Heritage Foundation Report, 2002, p. 25).

"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 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" (Heritage Foundation Report, 2002, p. 27).

"The U.S. Customs Service should experiment with a point-of-origin inspections program for maritime trade . . . 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 . . . If the pilot program proves successful and cost-efficient, the Administration should include point-of-origin inspection agreements in international trade agreements" (Heritage Foundation Report, 2002, p. 25).

"Congress should repeal the requirement that [Immigration and Naturalization Service] INS inspectors clear passengers on international flights within 45 minutes of each flight's arrival" (Heritage Foundation Report, 2002, p. 65).

"Congress should amend the Visa Waiver Program so as to:

1. Make aliens from countries designated as 'not fully cooperating with U.S. antiterrorism efforts' ineligible for the Visa Waiver program . . . ;
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" (Heritage Foundation Report, 2002, p. 66).

Domestic Counterterrorism Emergency Preparedness and Response, with Federal, State, and Local Coordination

With the creation of a Department of Homeland Security, the Bush Administration aims to institute two fundamental changes in how the country confronts terrorism: First, the new department, the FBI, and other collaborating law enforcement and intelligence organizations will redefine their counterterrorism mission "to focus on prevention of all terrorist acts within the United States, whether international or domestic in origin." Second, the creation of a cabinet-level department combines many domestic activities such as terrorism prevention, consequence management, and consequence response.[3] The department "will simplify the process by which governors, mayors, and county leaders interact with the federal government" (Bush, 2002b, p. 13). Along these lines, the *National Strategy for Homeland Security* states "the President [should] call on each governor to establish a single Homeland Security Task Force (HSTF) for the state, to serve as his or her primary coordinating body with the federal government"(Bush, 2002b, p. 14).

The Bush Administration has established a new Office of Intelligence in the FBI, and the *National Strategy for Homeland Security* proposes "complete FBI restructuring to emphasize prevention of terrorist attacks" (Bush, 2002b, p. 37). To achieve this reorientation of the FBI, the bureau will increase its "Flying Squads . . . consisting of agents with specific counterterrorism expertise" who "will travel to field when their expertise is needed, and will bring valuable information back to FBI headquarters for analysis" (Bush, 2002b, p. 27). The *National Strategy for Homeland Security* also proposes "the establishment of a new expansive multi-agency National Joint Terrorism Task Force at FBI Headquarters" (Bush, 2002b, p. 27).

Reorienting the focus and approach of law enforcement officials to enhance counterterrorism is a major challenge for all levels of government. The *National*

---

[3] *Consequence management* and *consequence response* refer to the actions of emergency and police personnel and other authorities after an attack. Many experts believe that effective consequence response will mitigate the severity and number of casualties in the event of an attack.

Strategy for Homeland Security is the most authoritative statement on how federal departments and agencies intend to focus their energies on homeland security.

The reports we reviewed offer various ideas and models for accomplishing coordination among federal, state, and local authorities in the areas of law enforcement and consequence management. However, many of these reports give scant attention to the difficulties presented by the institutional change that certain recommendations would require (e.g., the FBI placing more of a focus on terrorism prevention in addition to managing the forensic investigation building toward prosecution, or the CDC viewing bioterrorism as an increasingly important public health issue). A major challenge for the Department of Homeland Security will be in acting as the key point of contact for state and local officials and at the same time ensuring that federal entities interface with these officials effectively.

In the following subsections, we quote selected recommendations on federal, state, and local coordination on domestic counterterrorism emergency preparedness and response that the Bush Administration has not already adopted.

Gilmore Commission Second Annual Report

"To assist in providing broad strategic guidance and to serve as part of the approval process for the domestic portion of strategy, plans, and programs of the National Office for Combating Terrorism, we recommend the establishment of a national 'Advisory Board for Domestic Programs.' That Board should include one or more sitting State governors, mayors of several U.S. cities, the heads of several major professional organizations, and nationally recognized subject matter experts in combating terrorism, in addition to senior representatives of the major Federal entities that have responsibility for combating terrorism. The President and the Congress should each appoint members to this board" (Gilmore Commission Second Annual Report, 2000, p. 14).

"We recommend that the senior emergency management entity in each State function as the prime 'Focal Point' for that State for domestic preparedness for terrorism" (Gilmore Commission Second Annual Report, 2000, p. 23).

"We recommend that the Assistant Director for Domestic Programs in the National Office for Combating Terrorism develop exercise scenarios that are realistic and meet the needs of the State and local response entities . . . Training and exercises should also include as scenarios the more likely, but less catastrophic, smaller-scale Chemical Biological Radiological Nuclear Explosive

(CBRNE) attacks, and exercises must include 'all' disciplines and all levels of response" (Gilmore Commission Second Annual Report, 2000, pp. 30–31).

Gilmore Commission Third Annual Report

"We recommend consolidating information and application procedures for Federal grant programs for terrorism preparedness in the Office of Homeland Security and that all funding and grant programs be coordinated through the States" (Gilmore Commission Third Annual Report, 2001, p. 10).

Hart-Rudman Commission Report

"The mission of the NHSA [National Homeland Security Agency] must include specific planning and operational tasks to be staffed through the Directorate for Emergency Preparedness and Response. These include: Setting training and equipment standards, providing resource grants, and encouraging intelligence and information sharing among state emergency management officials, local first responders, the Defense Department, and the FBI. Integrating the various activities of the Defense Department, the National Guard, and other federal agencies into the Federal Response Plan . . ." (Hart-Rudman Commission Report, 2001, p. 19).

Bremer Commission Report (National Commission on Terrorism)

"The President should direct (1) the [interagency counterterrorist] Subgroup, under the direction of the national coordinator for counterterrorism, to exercise annually the government's response to a catastrophic terrorism crisis, including consequence management; and (2) all relevant agencies to plan, budget, and participate in counterterrorism and consequence-management exercises coordinated by the Exercise Subgroup and ensure senior officer level participation, particularly in the annual exercises" (Bremer Report, 2000, p. 41).

President's Critical Infrastructure Commission Report

"We recommend the President appoint a high-level council [composed] of CEOs from throughout the critical infrastructures, senior government officials (Cabinet rank), and representatives of state and local government. The Council would meet regularly to provide a forum for high-level discussion of proposed policies and directions for the nation in this critical area, to encourage and advocate partnership in infrastructure protection, and to make appropriate

recommendations to the President. The Council should provide policy advice to the President. It should meet no less than twice annually, and create whatever sub-structure it needs. A standing executive committee consisting of the Chair, selected Council members, and the Director of the National Office should meet often to manage the Council's work. The National Infrastructure Support Office would provide staff support for the Council's work. Members of the Council should be permitted to contribute staff and program support from their organizations (both public and private) to assist the Council in its work" (President's Critical Infrastructure Commission Report, 1997, p. 52).

CSIS Report (Executive Summary of the CSIS Working Group Reports)

"The Vice President would chair a new National Emergency Planning Council that would include representatives from all departments, agencies, states, and territories. This council would be the senior body for federal and state coordination on matters relating to critical infrastructure protection or response to terrorist incidents. . . . The council would meet twice yearly, once at the principal level (vice president, governors, CEOs) and once at the subordinate level" (CSIS Report, 2000, pp. 13–14).

"The vice president and his new staff should develop a new and comprehensive series of exercises, simulations, and evaluations. The purpose of these activities will be to identify and improve the readiness of the government to carry out potential tasks and coordinate an effective response to all incidents, especially those that involve CBRN weapons or that might otherwise create mass destruction. At the same time, these exercises should be specifically designed to identify and to help resolve conflicts of legal authority and potential civil rights issues. In conjunction with this series of exercises, the federal government must develop ways . . . to improve the lessons-learned process so as to ensure that learning from exercises takes place and that the resulting knowledge receives the widest possible dissemination" (CSIS Report, 2000, p. 16).

Heritage Foundation Report

"The President should direct Federal agencies to streamline the current grant process that supports State and Local terrorism response and prevention activities . . . 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" (Heritage Foundation Report, 2002, p. 42).

Protecting Critical Infrastructures and Key Assets

Protecting the nation's critical infrastructure poses a major challenge for the U.S. government, and responsibility for this protection resides in various White House offices as well as in the new Homeland Security Department. The goal of the Bush Administration, as defined by the *National Strategy for Homeland Security,* is that "the United States will forge an unprecedented level of cooperation throughout all levels of government, with private industry and institutions, and with the American people, to protect our critical infrastructure and key assets from terrorist attacks." The *National Strategy for Homeland Security* calls upon "the Department of Homeland Security to work with the federal departments and agencies, state and local governments, and the private sector to implement a comprehensive national plan to protect critical infrastructure and key assets" (Bush, 2002b, p. 31).

The *National Strategy for Homeland Security* also proposes that the Secretary of Homeland Security and the Attorney General "convene a panel with appropriate representatives from federal, state, and local government, in consultation with the private sector, to examine whether employer liability statutes and privacy concerns hinder necessary background checks of personnel with access to critical infrastructure facilities or systems" (Bush, 2002b, p. 34). Additionally, the DHS will review protective measures and consider "establishing 'security zones' and controlling access around vulnerable port facilities" (Bush, 2002b, pp. 34–35).

The reports we reviewed have a few suggestions for organizational and substantive initiatives related to protecting critical infrastructures and key assets. Unlike the *National Strategy for Homeland Security*, the reports tend to separate physical infrastructure issues from cyber-infrastructure issues.

In the following subsections, we quote selected recommendations from those reports on protecting infrastructures and key assets that the Bush Administration has not already adopted.

Gilmore Commission Third Annual Report

"We recommend that Congress create an independent commission, tasked to evaluate programs designed to promote cyber security, to recommend strategies for better security, and with the requirement to report its recommendations to

the President and the Congress" (Gilmore Commission Third Annual Report, 2001, p. 42).

"We recommend that the President establish a government-funded, not-for-profit entity that can represent the interests of all affected stakeholders, public and private—national security, law enforcement, other government functions, and business and industry interests and concerns—to provide cyber detection, alert, and warning functions. That entity would serve as a 'fusion center' and clearinghouse, at or near real-time, for information on impending or actual cyber attacks" (Gilmore Commission Third Annual Report, 2001, p. 43).

"We recommend that Congress and the Executive Branch convene a 'summit' to address, on an urgent basis, necessary changes to a wide range of federal statutes, in order to provide necessary protection and incentives for enhancing cyber assurance" (Gilmore Commission Third Annual Report, 2001, p. 44).

CSIS Report (Executive Summary of the CSIS Working Group Reports)

"Government can improve cooperation with the private sector in many ways . . . Conduct information-sharing on vulnerabilities and warnings of ongoing attacks or threats; share information on hacker modus operandi and on solutions and defenses to established threats and attacks. Continue to facilitate discussions within industry sectors, interaction with information sharing and analysis centers (ISACs), and assistance in collecting, 'sanitizing,' and disseminating pertinent warnings of threats and attacks. Build on the successful elements of the National Information Protection Center (NIPC) model . . . Establish a single point of national coordination for cyber concerns and alerts . . . Unlike NIPC, this new virtual center would not be housed within the Department of Justice, but rather within an organization less restricted by its own information-protection and law-enforcement mission" (CSIS Report, 2000, p. 23).

Bremer Commission Report (National Commission on Terrorism)

"The Secretary of State, in concert with other departments and agencies, should take the lead in developing an international convention aimed at harmonizing national laws, sharing information, providing early warning, and establishing accepted procedures for conducting international investigations of cyber crime" (Bremer Report, 2000, p. 33).

Brookings Institution Report

"Insurance companies could provide incentives for adopting the more costly approach of relocating systems or replacing existing air and heat systems to accommodate the finest class of air filters" (Brookings Institution Report, 2002, p. 54).

"Tougher building safety codes offer another avenue of protection, especially in new commercial buildings. They should focus on structural integrity, minimizing the probability of collapse even after an explosive attack, and making the buildings more resistant to fire" (Brookings Institution Report, 2002, p. 55).

"An attack on a nuclear facility or a plant containing toxic chemicals could result in thousands, if not millions, of deaths and injuries . . . One step that could be taken to defend against aerial attack: placing steel towers around the site to destroy any plane entering the immediate neighborhood. Such an idea may not be necessary but would address the vulnerability problem fairly inexpensively and reliably" (Brookings Institution Report, 2002, pp. 54–55).

"Given the costs associated with 'hardening' new buildings and the trade-off between risk and cost, any such 'anti-terrorism' building codes should probably apply only to the largest new structures, those that would hold thousands of people" (Brookings Institution Report, 2002, p. 55).

"Large buildings should maintain slight overpressure relative to the outside air to keep out agents that might have been released in the vicinity" (Brookings Institution Report, 2002, p. 55).

Heritage Foundation Report

"Designate the Global Position 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" (Heritage Foundation Report, 2002, p. 12).

"The Defense Department should be made responsible for coordinating GPS security with private-sector stakeholders and other federal agencies" (Heritage Foundation Report, 2002, p. 20).

"The executive branch should 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) before making procurement decisions . . . Many experts . . . 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 . . . The President should direct GSA [General Services Administration] 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 [Office of Management and Budget] should evaluate both the GOVNET and standard Internet options in consultation with OHS, the Office of Science and Technology Policy (OSTP), and the Special Advisor to the President for Cyber Space Security to determine which one would provide better security for the dollar" (Heritage Foundation Report, 2002, p. 22).

Defending Against Catastrophic Threats

The *National Strategy for Homeland Security* states that the Department of Homeland Security "will unify much of the federal government's efforts to develop and implement scientific and technological countermeasures against human, animal, and plant diseases that could be used as terrorist weapons" (Bush, 2002b, p. 38). It indicates that the U.S. government "will seek to detect chemical, biological, radiological, or nuclear weapons and prevent their entry into the United States. If terrorists use chemical, biological, radiological, or nuclear weapons . . . communities and emergency personnel will be organized, trained, and equipped to detect and identify dangerous agents, respond rapidly, treat those who are harmed, contain the damage, and decontaminate the area" (Bush, 2002b, p. 38).

The *National Strategy for Homeland Security* identifies six major initiatives for this mission area. Some of these initiatives include "a new system of procedures and technologies to detect and prevent the transport of nuclear explosives" toward American borders, "research and efforts aimed at new and better passive and active detection systems," and systems that can "detect whether an individual has been immunized against a threat pathogen or has recently handled threat materials" (Bush, 2002b, p. 38).

Several organizations that authored the reports we studied paid particular attention to medical and health requirements, focusing on the need to increase resources, improve assessments and surveillance of outbreaks of disease, and expand vaccination and "surge" capabilities (e.g., a hospital increasing its capability to handle many more patients than it ordinarily does). They also recommended that specific steps be taken in this regard, some of which may

have significant cost implications. Only the Brookings Institution Report addresses how much additional funding would be needed or what the implications would be for the health care industry and the economy were their recommendations to be actually implemented. The DHS will need to evaluate the cost-benefit trade-offs of many of the recommendations in this mission area.

In the following subsections, we quote selected recommendations, not already adopted by the Bush Administration, on defending against catastrophic threats.

CSIS Report (Executive Summary of the CSIS Working Group Reports)

"Capitalize the public health structure. Core functions of public health (e.g., disease surveillance and laboratory capability) will form the foundation for detecting, investigating, and responding to bioterrorist threats. Development of these core functions requires investing in communications facilities, administrative support, and surge personnel capabilities so that the public health system can lead the effort to contain and eradicate epidemics. Run exercises to test capabilities and determine what is cost-effective" (CSIS Report, 2000, p. 20).

"Direct FEMA [Federal Emergency Management Agency] and CDC [the Centers for Disease Control] to develop the national response capacity for the rapid assessment of a bioterrorist emergency occurring anywhere in the United States. These agencies will need to develop a Biological Emergency Support Team (BEST) that can rapidly assess and set priorities following the consequences of a bioterrorist event" (CSIS Report, 2000, p. 20).

"Expand the provisions on biological terrorism in the Terrorism Annex of the Federal Response Plan. The current U.S. plan for an organized response must be updated to include preparedness for a biological attack, which presents a host of unique and complicated challenges and requires reexamining lead agency roles and missions" (CSIS Report, 2000, p. 21).

Gilmore Commission Third Annual Report

"We recommend that medical systems fully implement the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) Revised Emergency Management Standard. That standard requires that accredited facilities establish and maintain a comprehensive plan for response to disasters and emergencies, including terrorism, within an all-hazards framework" (Gilmore Commission Third Annual Report, 2001, p. 28).

"We recommend that the Congress provide sufficient resources to the U.S. Department of Health and Human Services (DHHS) for full implementation of the 'Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response' of the CDC . . . of the 'Laboratory Response Network for Bioterrorism' of the CDC . . . [and] of the CDC Secure and Rapid Communications Networks" (Gilmore Commission Third Annual Report, 2001, pp. v–vi).

"We recommend that DHHS, in coordination with the Office of Homeland Security, develop standard models for health medical responses to a variety of hazards for use at Federal, State, and local levels and in conjunction with the private sector" (Gilmore Commission Third Annual Report, 2001, p. 29).

"We recommend the establishment of a government-owned, contractor-operated national facility for the research, development, and production of vaccines and therapeutics for specified infectious—especially contagious—diseases . . . [and] that the Office of Homeland Security, with advice from its related national advisory board and in coordination with the DHHS and DVA [Department of Veterans Affairs] review and recommend appropriate changes to plans for the stockpile of vaccines and other critical supplies" (Gilmore Commission Third Annual Report, 2001, pp. 30–31).

Brookings Institution Report

"Another pressing imperative is to improve the ability of the health system to recognize and contain biological and chemical attacks. Early recognition of and intervention in a biological attack would substantially reduce casualties and costs involved. The health industry can help improve its ability to recognize and contain a biological or chemical attack through medical training" (Brookings Institution Report, 2002, pp. 70–71).

Heritage Foundation Report

"The President should guarantee patent protection on pharmaceuticals related to terrorism . . . The FDA should prioritize applications for fast-track approval of pharmaceuticals" (Heritage Foundation Report, 2002, pp. 39–40).

The Law

The *National Strategy for Homeland Security* describes the law as one of the critical foundations for enhancing homeland security. The statement identifies 12 major initiatives in the legal area. Some of the initiatives for federal law include

streamlining information sharing among intelligence and law enforcement agencies, expanding existing extradition authorities, and reviewing authority for military assistance in domestic security (Bush, 2002b, p. 48).

The reports we reviewed also consider the legal framework to be a critical part of the homeland security strategy and urge that executive and congressional branch officials give attention to complex legal issues. Given the range of new legal developments since September 11 and the new authorities contained in recently passed legislation, the secretary of the new department should place considerable emphasis on reviewing the legal foundations for homeland security.

In the following subsections, we quote selected recommendations the Bush Administration has not already adopted regarding the law.

Bremer Commission Report (National Commission on Terrorism)

"The President should direct the preparation of a manual on the implementation of existing legal authority necessary to address effectively a catastrophic terrorist threat or attack. The manual should be distributed to the appropriate federal, state, and local officials and be used in training, exercises, and education programs. The President should determine whether any additional legal authority is needed to deal with catastrophic terrorism and make recommendations to Congress as necessary" (Bremer Report, 2000, p. 38).

Gilmore Commission Third Annual Report

"We recommend that the Office of Homeland Security develop an information and education program on the legal and procedural problems involved in a health and medical response to terrorism, and in coordination with the Department of Justice and the American Bar Association, consider the efficacy of model laws or other programs to enhance future responses to such events" (Gilmore Commission Third Annual Report, 2001, p. 33).

"We recommend that the Congress and the Executive Branch convene a 'summit' to address, on an urgent basis, necessary changes to a wide range of federal statutes " (Gilmore Commission Third Annual Report, 2001, p. 44).

"We recommend that the Secretary of Defense publish a compendium, in layman's terms, of the statutory authorities for using the military domestically to combat terrorism, with detailed explanations about the procedures for implementing those authorities" (Gilmore Commission Third Annual Report, 2001, p. 53).

CSIS Report (Executive Summary of the CSIS Working Group Reports)

"An interagency task force, with state and local representation, should immediately begin efforts to identify legal issues raised by a CBRN threat or attack and work to resolve those issues, whether through proposing new laws or simply clarifying the application of existing laws" (CSIS Report, 2000, p. 23).

Hart-Rudman Commission Report

"A sound homeland security strategy requires the overhaul of much of the legislative framework for preparedness, response, and national defense programs. Congress designed many of the authorities that support national security and emergency preparedness principally for a Cold War environment. The new threat environment—from biological and terrorist attacks to cyber attacks on critical systems—poses vastly different challenges. We therefore recommend that Congress refurbish the legal foundation for homeland security in response to the new threat environment" (Hart-Rudman Commission Report, 2001, p. 26).

Science and Technology

The *National Strategy for Homeland Security* identifies 11 major initiatives in the area of science and technology. The document refers to "America's vast science and technology base [that] provides a key advantage" in the war on terrorism. It further states that the Department of Homeland Security will spearhead efforts to "explore evolutionary improvements to both the current capabilities and development of revolutionary new capabilities" (Bush, 2002b, p. 52). Underscoring the central role of the DHS, the *National Strategy for Homeland Security* states that "the Department, working with other agencies, will set standards to assist the acquisition decisions of state and local governments and private-sector entities" (Bush, 2002b, p. 52).

The Department of Homeland Security will be an important bureaucratic player, but not the only significant one, to influence technology for homeland security. Recommendations for new programs and for adjustments in spending priorities on research and development are contained throughout most of the commissions' and other groups' reports. However, few of the reports address the financial implications of their recommendations on investments in technology, and the DHS will eventually need to address these financial issues.

In the following subsections, we quote selected recommendations in the area of science and technology that the Bush Adminstration has not already adopted.

Bremer Commission Report (National Commission on Terrorism)

"Given the urgency of near-term needs, long-term research and development projects on technologies useful to fighting terrorism will be short-changed unless Congress and the President can agree on special procedures and institutional arrangements to work on research that is risky and has more distant payoffs" (Bremer Report, 2000, p. 42).

CSIS Report (Executive Summary of the CSIS Working Group Reports)

"Early on, the vice president and the national coordinator need to assess the United States present and future needs against its ongoing research efforts and make detailed recommendations to the president and the Congress. A net assessment is needed on this set of options, as well as on others that include an analysis of potential deployment costs and requirements, countermeasures, and relative costs and benefits" (CSIS Report, 2000, pp. 15–16).

Hart-Rudman Commission Report

"The President should propose, and the Congress should support, doubling the U.S. government's investment in science and technology research and development by 2010" (Hart-Rudman Commission Report, 2001, p. 31). "We recommend that OSTP, in conjunction with the National Science Foundation—and with the counsel of the National Academies of Science—design a system for the ongoing basic inventory stewardship of the nation's capital knowledge assets. The job of inventory stewardship could be vouchsafed to the National Science Board, the governing body of the National Science Foundation, were it to be provided staff for this purpose" (Hart-Rudman Commission Report, 2001, p. 33).

"The President should empower his Science Advisor to establish non-military R&D objectives that meet changing national needs, and to be responsible for coordinating budget development within the relevant departments and agencies" (Hart-Rudman Commission Report, 2001, p. 33).

"The President, in tandem with strengthening the White House Office of Science and Technology Policy, should raise the profile of its head—the Science Advisor to the President. The Science Advisor needs to be empowered as a more

significant figure within the government, and we believe the budget function we have recommended for him will be instrumental for this purpose" (Hart-Rudman Commission Report, 2001, p. 33).

"The Commission recommends that the President, with aid from his Science Advisor directing NSF's [National Science Foundation's] National Science Board, should reassess and realign, as necessary, government needs for science and technology personnel for the next quarter century. Indeed, such a review ought to be made routine. The Science Advisor with the National Science Board and OPM [Office of Personnel Management], in consultation with the National Academies of Science, should periodically reevaluate Executive Branch needs for science and technology personnel" (Hart-Rudman Commission Report, 2001, p. 34). "We therefore recommend that the President's Science Advisor, beyond his proposed budget coordination role, should lead an effort to revise government R&D practices and budget allocations to make the process more competitive" (Hart-Rudman Commission Report, 2001, p. 35).

"A Science and Technology office would advise the NHSA [National Homeland Security Agency] Director on research and development efforts and priorities for all three directorates" (Hart-Rudman Commission Report, 2001, p. 16).

Gilmore Commission Second Annual Report

"We recommend that the Technical Support Working Group (TSWG) become an adjunct to the National Office for Combating Terrorism in the same manner that it now serves in the NSC [National Security Council] process and that it expand its coordination role for technical aspects of [Research, Development, Testing, and Evaluation] RDT&E for combating terrorism" (Gilmore Commission Second Annual Report, 2000, pp. 36–37).

"We recommend that the Assistant Director for RDT&E and National Standards of the National Office for Combating Terrorism either enter into a formal relationship with OSTP or have appropriate members of the OSTP staff detailed to the National Office for Combating Terrorism on a rotational basis . . . [and] develop, as part of the national strategy, a comprehensive plan for long-range research for combating terrorism" (Gilmore Commission Second Annual Report, 2000, p. 37).

Gilmore Commission Third Annual Report

"We recommend that Federal agencies design related training and equipment programs as part of all-hazards preparedness" (Gilmore Commission Third Annual Report, 2001, p. 9).

"We recommend that the Office of Homeland Security, on the advice of its related national advisory board, and in coordination with the responsible Federal agencies, develop a comprehensive plan for the full spectrum of medical and health research for terrorism-related medical issues, including the psychological repercussions of terrorism and pre-hospital intervention" (Gilmore Commission Third Annual Report, 2001, p. 33).

Brookings Institution Report

"For maximum effectiveness, consequence management needs input from research and development, not only in the way of new vaccines and antibiotics but also information about newly discovered or newly recurring infectious diseases and treatments for chemical and radiological terrorism. Furthermore, researchers should explore methods for strengthening the human body's immune system" (Brookings Institution Report, 2002, p. 75).

Information Sharing and Systems

Information sharing and information systems together are another critically important foundation of the *National Strategy for Homeland Security*. Five major initiatives are identified in the national strategy statement to ensure "the proper use of people, processes, and technology [so that] homeland security officials throughout the United States . . . have complete and common awareness of threats and vulnerabilities" (Bush, 2002b, p. 56). Some of the innovative initiatives cited in the national strategy statement include the creations of "a Collaborative Classified Enterprise environment to share sensitive information securely among all relevant government entities," and the establishment of "a secure video conferencing capability connecting officials in Washington, DC with all government entities in every state" (Bush, 2002b, p. 57).

The Department of Homeland Security will confront a wide range of political, legal, cultural, and technical issues as it seeks to integrate the various repositories of government data and share information among state and local authorities. Many of the reports we reviewed urge greater information integration and wider dissemination of information to relevant authorities at all levels of government.

However, most of these recommendations on information sharing and information systems tend to be very general, and the reports lack practical guidance on the critical task of implementing many of the recommendations.

On balance, the commissions and other organizations did not offer many actionable recommendations on the important topic of information sharing, and those recommendations that were offered were already incorporated into the *National Strategy for Homeland Security.* However, the Heritage Foundation did offer one recommendation with a unique degree of specificity.

Government access to personal records raises important privacy issues that must be balanced against security needs. This topic warrants considerably more examination beyond what the various advisory groups have done.

Heritage Foundation Report

"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)" (Heritage Foundation Report, 2002, p. 71).

4. Conclusions

The reports from the various commissions and think tanks that we quoted in this paper provide a wealth of valuable guidance that can be used to inform the future efforts of the new Department of Homeland Security and its congressional oversight committees. Even though publication of most of the reports predated the September 11 terrorist attacks, the recommendations in those reports are relevant to the challenges the government currently faces with homeland security.

In the spring of 2001, the Bush Administration began to seriously consider the recommendations we reviewed for this paper (Office of the Press Secretary, 2001). But it was not until after the events of September 11 that those recommendations were acted upon. Since then, many of those recommendations are being implemented or have been incorporated into the *National Homeland Security Strategy,* the Bush Administration's 2002 statement of plans and goals regarding homeland security.

However, additional evaluation of the pros and cons of the various remaining recommendations is needed before those recommendations can be implemented. As stated in a previous analysis of the performance of advisory commissions, "Any commission will be a creature of the political forces that created it, will be embedded in the political context of the moment, and will be subject to larger political forces" (Harris, unpublished).

The three congressionally established commissions that published reports we reviewed for this paper—the National Commission on Terrorism (Bremer Commission), the Hart-Rudman Commission, and the Gilmore Commission—were in part an expression by Congress of its dissatisfaction with the Clinton Administration's policies and plans to combat terrorism. The primary aim of these commissions was to draw attention to the seriousness of the terrorist threat to the U.S. homeland, and they had some success in making people aware of that threat, especially in Congress.

Although most of the organizations that prepared the reports we reviewed had analysts and other support staff whom they relied upon to formulate their recommendations, many of those recommendations are overly generalized, urge more spending than is feasible, or urge the government to take various actions without providing clear guidance on how to best prioritize those actions. More

detailed and systematic scrutiny of these recommendations is needed before any of the remaining recommendations can be implemented as government policy.

The challenge ahead is to determine which of the many worthy recommendations offered to the new Department of Homeland Security warrant action and which warrant additional study. After that, those ideas that do warrant action will need to be integrated with other DHS programs and made part of the budget of the new department, requiring new spending priorities to be set and choices to be made on the global war against terrorism.

A. Organizations' Major Recommendations

The tables in this appendix list what we feel are the commissions' or think tanks' major recommendations on homeland security that the Bush Administration has *not* already adopted.[1] The organizations offered other recommendations, many of which became part of the administration's *National Strategy for Homeland Security.*

The recommendations are organized according to the critical mission areas and foundations identified by the administration. As such, the appendix can serve as a checklist of recommendations that the various offices of the new Department of Homeland Security and the appropriate congressional oversight committees might consider as they move forward in formulating a comprehensive U.S. homeland security strategy.

[1]The recommendations of the President's Commission on Critical Infrastructure Protection are not listed here because those recommendations were for the most part already captured in the *National Strategy on Homeland Security.*

Table A.1

Recommendations on Intelligence and Warning

	BC	GC	HRM	CSIS	HF	BI
Clarify FBI guidelines on terrorism investigations	X	X				
Attorney general to supply guidance to Office of Intelligence Policy and Review on standards of evidence	X	X				
National Intelligence Officer on terrorism to be "dual-hatted" at National Intelligence Council and White House Office for Combating Terrorism		X				
Establish Terrorism Intelligence Coordinating Council		X			X	
Establish Intelligence Fusion Center					X	
Office of Homeland Security to direct intelligence assessments					X	
Conduct assessment of intelligence capabilities for homeland security				X		
Place priority on recruitment of human intelligence sources			X			
National Intelligence Council should dedicate a National Intelligence Officer to homeland security and asymmetric threats			X			
Establish a National Counter Terrorism Center outside of FBI, CIA, or Department of Homeland Security		X				
Establish a Foreign Intelligence Surveillance Act court–like body for the National Counter Terrorism Center		X				

NOTE: BC=Bremer Commission; GC=Gilmore Commission; HRM=Hart-Rudman Commission; CSIS=Center for Strategic and International Studies; HF=Heritage Foundation; BI=Brookings Institution.

Table A.2

Recommendations on Border and Transportation Security

	BC	GC	HRM	CSIS	HF	BI
Repeal Immigration and Naturalization Service 45-minute rule					X	
Establish "Trusted Shipper" E-Z pass trade lanes system		X				X
Require shippers to submit cargo manifest information prior to arrival in the United States		X				
Agencies with border responsibilities would be full partners in intelligence matters relating to border issues		X				
Give local law enforcement access to federal databases and improve their information systems						X
Develop and deploy system to cross-check airline reservations with government-wide databases					X	
Establish interagency center to cross-check people and products entering the United States					X	
Congress should amend Visa Waiver Program					X	

NOTE: BC=Bremer Commission; GC=Gilmore Commission; HRM=Hart-Rudman Commission; CSIS=Center for Strategic and International Studies; HF=Heritage Foundation; BI=Brookings Institution.

Table A.3

Recommendations on Domestic Counterterrorism Emergency Preparedness and Response, with Federal, State, and Local Coordination

	BC	GC	HRM	CSIS	HF	BI
Consolidate all grant-making to states and localities in Office of Homeland Security or National Homeland Security Agency		X	X		X	
Office of the Vice President should facilitate interagency coordination				X		
Establish Advisory Board for Domestic Programs with membership from state and local governments		X				
Senior emergency management entity in each state should serve as the "focal point" for domestic preparedness for terrorism		X				
Federal authorities should develop realistic scenarios for state and local needs		X				
Annual exercises should be conducted to test intergovernmental management of catastrophic terrorist incidents			X			

NOTE: BC=Bremer Commission; GC=Gilmore Commission; HRM=Hart-Rudman Commission; CSIS=Center for Strategic and International Studies; HF=Heritage Foundation; BI=Brookings Institution..

Table A.4

Recommendations on Protecting Critical Infrastructures and Key Assets

	BC	GC	HRM	CSIS	HF	BI
Establish independent commission to promote cyber-security		X				
Establish government-funded, not-for-profit cyber-fusion center and clearinghouse		X				
Convene Legislative-Executive Branch summit to draft federal statutes to enhance cyber-security		X				
Establish virtual center similar to the National Information Protection Center outside of the Department of Justice				X		
Secretary of State should develop international convention on cyber-crime	X					
Insurance companies should be a vehicle for forcing changes in building construction codes					X	
Maintain slight overpressure in large buildings (air being expelled to prevent foreign particles from entering)					X	
Place steel towers around toxic chemical and nuclear power facilities					X	
Department of Defense should coordinate guarding Global Positioning System frequencies with private sector						X
Federal government should restudy how to enhance government cyber-security						X

NOTE: BC=Bremer Commission; GC=Gilmore Commission; HRM=Hart-Rudman Commission; CSIS=Center for Strategic and International Studies; HF=Heritage Foundation; BI=Brookings Institution..

Table A.5

Recommendations on Defending Against Catastrophic Threats

	BC	GC	HRM	CSIS	HF	BI
Implement Joint Commission on Accreditation of Healthcare Organizations emergency management standards		X				X
Enhance Federal Response Plan prescriptions to handle bioterrorism		X		X		
Enhance medical communications capability		X				X
Establish government-owned, contractor-operated vaccine and therapeutics production facility			X			
U.S. Department of Health and Human Services in coordination with Office of Homeland Security should develop models for health response at all levels of government		X				
Enhance disease surveillance capacity		X		X	X	X
"Fully fund" the public health system and test it for cost-effectiveness by using exercises				X		
Federal Emergency Management Agency and Centers for Disease Control should develop a Biological Emergency Support Team				X		
Expand provisions for bioterrorism in Federal Response Plan				X		
Improve health industry's ability to recognize and contain chemical and biological attacks through training						X
Guarantee patent protection on pharmaceuticals related to bioterrorism					X	

NOTE: BC=Bremer Commission; GC=Gilmore Commission; HRM=Hart-Rudman Commission; CSIS=Center for Strategic and International Studies; HF=Heritage Foundation; BI=Brookings Institution..

Table A.6

Recommendations on the Law

	BC	GC	HRM	CSIS	HF	BI
Compile a manual on legal authorities	X					
Conduct presidential review to determine needed additional legal authorities	X					
Congress should review and refurbish legal authorities			X			
Create joint Office of Homeland Security, Department of Justice, and American Bar Association educational program on legal authorities		X				
Convene Congress and Executive Branch summit meeting to review legal authorities		X				
Secretary of Defense should publish compendium of legal authorities		X				
Interagency and intergovernmental task force should review legal authorities in light of Chemical Biological Radiological Nuclear threat				X		

NOTE: BC=Bremer Commission; GC=Gilmore Commission; HRM=Hart-Rudman Commission; CSIS=Center for Strategic and International Studies; HF=Heritage Foundation; BI=Brookings Institution..

Table A.7

Recommendations on Science and Technology

	BC	GC	HRM	CSIS	HF	BI
Conclude Congressional and Executive Branch pact on R&D	X					
Vice President and Director of Office of Homeland Security should determine R&D priorities				X		
Double funding for R&D should be approved by 2010			X			
Office of Science and Technology Policy, National Science Foundation, and National Academy of Sciences should set R&D spending objectives			X			
Office of Science and Technology Policy should be responsible for coordinating R&D spending priorities		X	X			
Establish a science and technology office in the National Homeland Security Agency			X			
Technical Support Working Group should provide support to Office of Homeland Security for R&D spending		X				
Develop a comprehensive plan for R&D spending		X				
Encourage research on how to strengthen human immune system						X

NOTE: BC=Bremer Commission; GC=Gilmore Commission; HRM=Hart-Rudman Commission; CSIS=Center for Strategic and International Studies; HF=Heritage Foundation; BI=Brookings Institution..

B. Commission Members

Gilmore Commission, Third Annual Report

The Gilmore Commission's official designation is the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction.

The Gilmore Commission advisory panel is charged with assessing the capabilities for responding to terrorist incidents in the U.S. homeland involving weapons of mass destruction. The panel will examine response capabilities at the federal, state, and local levels, with a particular emphasis on the latter two. The secretary of defense, in consultation with the attorney general, the secretary of energy, the secretary of health and human services, and the director of the Federal Emergency Management Agency, entered into a contract with the National Defense Research Institute, a RAND federally funded research and development center, to establish the advisory panel in accordance with the Fiscal Year 1999 House Appropriations Act (H.R. 3616, Section 1405).

The panel members include the following individuals:

James S. Gilmore III, Governor, Commonwealth of Virginia, *Chairman*

L. Paul Bremer, Private Consultant, U.S. Department of State

Raymond Downey, Commander, City of New York Fire Department

Ellen Embrey, U.S. Department of Defense Representative

George Foresman, Deputy State Coordinator, Virginia Department of Emergency Services

William Garrison, Major General, U.S. Army (Retired)

Ellen M. Gordon, President, National Emergency Management Association

James Greenleaf, Former Associate Deputy for Administration, Federal Bureau of Investigation

William Jenaway, Chief of Fire and Rescue Services, King of Prussia, Pennsylvania

William Dallas Jones, Director, California Office of Emergency Services

Paul M. Maniscalco, Past President, National Association of Emergency Medical Technicians, and Deputy Chief/Paramedic, New York Fire Department, Emergency Management Services Chief

John O. Marsh, Jr., Attorney at Law, Former Secretary of the Army, Former Member of U.S. Congress

Kathleen O'Brien, City Coordinator, City of Minneapolis, Minnesota

M. Patricia Quinlisk, Medical Director/State Epidemiologist, Department of Public Health, State of Iowa

Patrick Ralston, Executive Director, State Emergency Management Agency; Executive Director, Department of Fire and Building Services; and Executive Director, Public Safety Training Institute, State of Indiana

William Reno, Lieutenant General, U.S. Army (Retired)

Joseph Samuels, Jr., Chief of Police, Richmond, California, and Third Vice President, International Association of Chief of Police

Kenneth Shine, President, Institute of Medicine, National Academy of Sciences

Hubert William, President, The Police Foundation

Gilmore Commission, Second Annual Report

The Gilmore Commission Second Annual Report membership was the same as the Third Annual Report membership, except for the addition of the following individual:[1]

James Clapper, Jr., Lieutenant General, U.S. Air Force (Retired); Corporate Executive, and Former Director, Defense Intelligence Agency, *Vice Chairman*

Hart-Rudman Commission

The following passage is from the official charter of the Hart-Rudman Commission (U.S. Commission on National Security/21st Century [USCNS/21]):

[1]Since the writing of this paper, the Gilmore Commission published a Fourth Annual Report. The recommendations from that report that are contained in this paper were issued only on an advanced basis.

> The Department of Defense recognizes that America should advance its position as a strong, secure, and persuasive force for freedom and progress in the world. Consequently, there is a requirement to: 1) conduct a comprehensive review of the early 21st century global security environment, including likely trends and potential "wild cards"; 2) develop a comprehensive overview of American strategic interests and objectives for the security strategy we will likely encounter in the 21st century; 3) delineate a national security strategy appropriate to that environment and the nation's character; 4) identify a range of alternatives to implement the national security strategy by defining the security goals for American society, and by describing the internal and external policy instruments required to apply American resources in the 21st century; and 5) develop a detailed plan to implement the range of alternatives by describing the sequence of measures necessary to attain the national security strategy, to include recommending concomitant changes to the national security apparatus as necessary.

The commission members include the following individuals:

Gary Hart, Former U.S. Senator, Colorado, *Co-Chair*

Warren B. Rudman, Chairman, President's Foreign Intelligence Advisory Board, *Co-Chair*

Anne Armstrong, Counselor to the President under the Nixon and Ford Administrations; U.S. Ambassador to the United Kingdom

Norman R. Augustine, Chairman, Executive Committee Lockheed Martin Corporation

John Dancy, Chief Diplomatic Correspondent, NBC News

John R. Galvin, General, U.S. Army (Retired); Supreme Allied Commander Europe

Leslie H. Gelb, President, Council on Foreign Affairs

Newt Gingrich, Former Speaker of the House of Representatives

Lee H. Hamilton, Former Member of the House of Representatives, Ninth District, Indiana

Lionel H. Olmer, Former Undersecretary of Commerce for International Trade

Donald B. Rice, Former Secretary of the Air Force; Former President and Chief Executive Office of the RAND Corporation

James Schlesinger, Former Secretary of Defense; Former Secretary of Energy; Former Director, Central Intelligence Agency

Harry D. Train, Admiral, U.S. Navy (Retired); Commander-in-Chief, U.S. Atlantic Command NATO Supreme Allied Commander, Atlantic

Andrew Young, Former U.S. Ambassador to the United Nations

CSIS Working Group

The CSIS Report that we cite in this paper is the Executive Summary of four Center for Strategic and International Studies Working Group reports on homeland defense. The Executive Summary is available at www.csis.org/homeland/reports/defendamer21stexecsumm.pdf.

The working group reports are as follows:

Combating Chemical, Biological, Radiological, and Nuclear Terrorism: A Comprehensive Strategy by Frank J. Cilluffo, Sharon L. Cardash, and Gordon N. Lederman, 2001; see www.csis.org/pubs/2001_combatingcbrnt.htm for a summary of the document.

Cyber Threats and Information Security: Meeting the 21st Century Challenge by Arnaud de Borchgrave, Frank J. Cilluffo, Sharon L. Cardash, and Michèle M. Ledgerwood, May 2001; see www.csis.org/pubs/2001_cyberthreatsandis.htm for a summary of the document.

Defense of the U.S. Homeland Against Strategic Attack by Daniel Gouré, December 2000; available at www.csis.org/homeland/reports/defenseofushmld.pdf.

Homeland Defense: A Strategic Approach by Joseph J. Collins and Michael Horowitz, December 2000; available at www.csis.org/homeland/reports/hdstrategicappro.pdf.

The Working Group chairpersons include the following individuals:

Arnaud de Borchgrave

Frank Cilluffo

Joseph J. Collins

Daniel Gouré

Michael Horowitz

Bremer Commission (National Commission on Terrorism)

The National Commission on Terrorism (Bremer Commission) was established by Section 591 of the Foreign Operations, Export Financing, and Related Programs Appropriation Act, 1999 (as contained in the Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999 [P.L. 105-277]).

Congress gave the commission six months to review the laws, regulations, directives, policies, and practices for preventing and punishing international terrorism directed against the United States, assess their effectiveness, and recommend changes.

The commission members include the following individuals:

Richard K. Betts, Director of the International Security Policy program, Columbia University, School of International and Public Affairs

L. Paul Bremer III, former Ambassador-at-Large for Counter-Terrorism

Wayne A. Downing, General, U.S. Army (Retired), Former Commander-in-Chief of the U.S. Special Operations Command

Jane Harman, Former Representative, California's 36th Congressional District

Fred C. Iklé, Former Undersecretary of Defense for Policy; Director for the U.S. Arms Control and Disarmament Agency

Juliette N. Kayyem, Associate of the Executive Session on Domestic Preparedness, John F. Kennedy School of Government, Harvard University

John F. Lewis, Jr., Former Assistant Director-in-Charge of the National Security Division of the FBI

Gardner Peckham, Former Senior Policy Advisor to the Speaker of the U.S. House of Representatives

Maurice Sonnenberg, Senior International Advisor to Bear, Stearns, and Co.

R. James Woolsey, Former Director of the Central Intelligence Agency

President's Commission on Critical Infrastructure Protection

The mission of the President's Commission on Critical Infrastructure Protection is to recommend a national policy for protecting and assuring critical national infrastructures.

The commission members include the following individuals:

Robert T. Marsh, *Chairman*

Merritt Adams, AT&T

Richard P. Case, IBM

Mary J. Culnan, Georgetown University

Peter H. Daly, Department of the Treasury

John C. Davis, National Security Agency

Thomas J. Falvey, Department of Transportation

Brenton C. Greene, Department of Defense

William J. Harris, Association of American Railroads

David A. Jones, Department of Energy

William B. Joyce, Central Intelligence Agency

Stevan D. Mitchell, Department of Justice

Irwin M. Pikus, Department of Commerce

John R. Powers, Executive Director, Federal Emergency Management Agency

Paul Rodgers, National Association of Regulatory Utility Commissioners

Susan Simens, Federal Bureau of Investigation

Frederick M. Struble, Federal Reserve Board

Nancy J. Wong, Pacific Gas and Electric Company

The Heritage Foundation Homeland Security Task Force

As stated in the Heritage Foundation Report (2002):

"The Heritage Foundation Homeland Security Task Force was formed days after the September 11 attacks. . . . The Task Force members . . . 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 task force members include the following individuals:

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, *Chairman*

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, *Chairman*

Kim R. Holmes, Vice President, The Heritage Foundation, *Project Director*

Working Group on Infrastructure Protection and Internal Security

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

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

Colonel Joseph Muckerman, U.S. Army (Retired); Former Director of Emergency Management, Office of the Secretary of Defense; Former Faculty Member, Army War College and National Defense University

Captain Bruce Stubbs, U.S. Coast Guard (Retired); 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

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

Albert Ashwood, Director, Oklahoma Emergency Management

Daniel Dire, Department of Emergency Medicine, University of Alabama

Daniel Gouré, Senior Fellow, Lexington Institute

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

Colonel Joseph Muckerman, U.S. Army (Retired); 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

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

Louis Dupart, 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, U.S. Army (Retired); Executive Vice President for Operations, Innovative Logistic 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

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, 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

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, N.C.; Former Chief of Police, Rochester, N.Y.; Former Associate Director, Office of National Drug Control Policy, State and Local Affairs

Working Group on Military Operations

Larry M. Wortzel, Director, Asian Studies Center, The Heritage Foundation, *Rapporteur*

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

Colonel James P. Gibbons, U.S. Army (Retired); Former Commander, U.S. Army Land Information Warfare Activity

Major General David L. Grange, U.S. Army (Retired); 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

General Patrick M. Hughes, U.S. Army (Retired); Former Director, Defense Intelligence Agency; Former Deputy Chief of Staff for Intelligence, U.S. Army

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

General Carl E. Mundy, Jr., U.S. Marine Corps (Retired); Former Commandant, U.S. Marine Corps; Former member, Joint Chiefs of Staff

General John H. Tilelli, Jr., U.S. Army (Retired); Former Commander, U.S. Army Forces Command, Vice Chief of Staff, U.S. Army, and Commander in Chief, U.S. Forces Korea

General Charles R. Wilhelm, U.S. Marine Corps (Retired); Former Commander, U.S. Southern Command

Brookings Institution Press

As stated in the Brookings Institution Report (2002):

"The purpose of this study is to provide a framework for thinking about how to address the country's vulnerabilities and to identify key priorities and approaches to eliminate or reduce those vulnerabilities. It also suggests an approach to identifying who should pay for which counterterrorism measures, and proposes ways the government could be more effectively organized to carry out its new set of critical national security tasks."

The authors of the *Protecting the American Homeland: A Preliminary Analysis* report include the following individuals:

Michael E. O'Hanlon

Peter R. Orszag

Ivo H. Daalder

I. M. Destler

David L. Gunter

Robert E. Litan

James B. Steinberg

Bibliography

Annual Report to Congress on Combating Terrorism, pursuant to Fiscal Year 1998 National Defense Authorization Act (Public Law 105-85), June 24, 2002 (available at www.whitehouse.gov/omb/legislative/combating_terrorism06-2002.pdf).

Bremer Report, National Commission on Terrorism (the Bremer Commission), *Countering the Changing Threat of International Terrorism,* June 7, 2000 (available at http://w3.access.gpo.gov/nct/).

Brookings Institution Report*, Protecting the American Homeland: A Preliminary Analysis,* Washington, D.C.: Brookings Institution Press, 2002; www.brook.edu/dybdocroot/.

Bush, President George W., *Remarks by the President in Address to the Nation*, Washington, D.C., June 2002a (available at www.dhs.gov/dhspublic/display?theme=44&content=169).

Bush, President George W., The White House, Office of Homeland Security, *National Strategy for Homeland Security,* Washington, D.C., July 2002b (available at www.dhs.gov/interweb/assetlibrary/nat_strat_hls.pdf).

Cilluffo, Frank J., Sharon L. Cardash, and Gordon N. Lederman, *Combating Chemical, Biological, Radiological, and Nuclear Terrorism: A Comprehensive Strategy*, Washington, D.C.: Center for Strategic and International Studies, 2001 (see www.csis.org/pubs/2001_combatingcbrnt.htm for a summary of the document).

Collins, Joseph J., and Michael Horowitz, *Homeland Defense: A Strategic Approach*, Washington, D.C.: Center for Strategic and International Studies, December 2000 (available at www.csis.org/homeland/reports/hdstrategicappro.pdf).

CSIS Report, Center for Strategic and International Studies (www.csis.org), *Defending America in the 21st Century: New Challenges, New Organizations, and New Policies,* Executive Summary of Four Working Group Reports on Homeland Defense, Washington, D.C.: CSIS, 2000 (available at www.csis.org/homeland/reports/defendamer21stexecsumm.pdf).

de Borchgrave, Arnaud, Frank J. Cilluffo, Sharon L. Cardash, and Michèle M. Ledgerwood, *Cyber Threats and Information Security: Meeting the 21st Century Challenge*, Washington, D.C.: Center for Strategic and International Studies, May 2001 (see www.csis.org/pubs/2001_cyberthreatsandis.htm for a summary of the document).

Gilmore Commission Second Annual Report, Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (known as the Gilmore Commission; www.rand.org/nsrd/terrpanel/), *Toward a National Strategy for Combating Terrorism,* Second Annual Report to the President and the Congress, Washington, D.C., December 15, 2000.

Gilmore Commission Third Annual Report, Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *For Ray Downey,* Third Annual Report to the President and the Congress, Washington, D.C., December 15, 2001.

Gilmore Commission Fourth Annual Report, Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Implementing the National Strategy,* Fourth Annual Report to the President and the Congress, Washington, D.C., December 15, 2002.

Gouré, Daniel, *Defense of the U.S. Homeland Against Strategic Attack*, Washington, D.C.: Center for Strategic and International Studies, December 2000 (available at www.csis.org/homeland/reports/defenseofushmld.pdf).

Hart-Rudman Commission Report, U.S. Commission on National Security/21st Century (known as the Hart-Rudman Commission; www.nssg.gov), *Road Map for National Security: Imperative for Change,* Phase III Report, Washington, D.C., February 15, 2001.

Harris, Scott A., "Advisory Commissions: Factors Affecting Success," RAND project memorandum prepared for Commission on Roles and Capabilities of the U.S. Intelligence Community, unpublished, p. 19.

Heritage Foundation Report, *Defending the American Homeland: A Report of The Heritage Foundation Homeland Security Task Force,* Washington, D.C.: The Heritage Foundation, January 2002; www.heritage.org.

Office of the Press Secretary, The White House, *Domestic Preparedness Against Weapons of Mass Destruction,* Statement by the President, Washington, D.C., May 8, 2001.

Office of the Press Secretary, The White House, "President Releases National Strategy for Homeland Security," July 16, 2002 (available at www.whitehouse.gov/news/releases/2002/07/print/20020716-2.html).

Office of the Press Secretary, The White House, "Fact Sheet: Strengthening Intelligence to Better Protect America," February 14, 2003 (available at www.whitehouse.gov/news/releases/2003/02/20030214-1.html).

President's Critical Infrastructure Commission Report, The President's Commission on Critical Infrastructure Protection, Critical Infrastructure Assurance Office, *Critical Foundations Protecting America's Infrastructures,* Washington, D.C., October 1997 (available at www.ciao.gov/resource/pccip/PCCIP_Report.pdf).

The White House, *Executive Order Establishing Office of Homeland Security,* Washington, D.C., Executive Order 13228, October 8, 2001.