

***Defense Science Board  
2005 Summer Study***

on

**Reducing Vulnerabilities  
to Weapons of Mass  
Destruction**



*Volume I  
Main Report*

**May 2007**

Office of the Under Secretary of Defense  
For Acquisition, Technology, and Logistics  
Washington, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB).

The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions and recommendations in this report do not necessarily represent the official position of the Department of Defense.

The Defense Science Board 2005 Summer Study on Reducing Vulnerabilities to Weapons of Mass Destruction completed its fact finding in August 2005.

This report is unclassified and releasable to the public.

# Table of Contents

## Volume I. Main Report

Preface.....	v
Executive Summary.....	vii
Chapter 1. Introduction.....	1
Chapter 2. Analytic Methodology.....	5
Scenario Analysis.....	5
Chapter 3. The Threat.....	12
Chapter 4. Intelligence.....	15
Improving Collection—The “Dots”.....	16
Improving Analysis and Information Management—“Connecting The Dots”.....	17
Enabling More Effective Collection and Analysis.....	20
Chapter 5. Prevent Attack—The First Priority.....	23
Deny Weapon Acquisition.....	23
Credible U.S. Policies.....	25
Detection and Interdiction in Transit.....	29
Chapter 6. Mitigation and Recovery.....	30
National Preparedness.....	30
DOD Responsibilities.....	39
Chapter 7. Managing the Enterprise.....	46
DOD Organization.....	47
Metrics: Readiness.....	47
Chapter 8. Summary of Recommendations.....	50
Investment in Reducing the Threat.....	50
Bottom Line.....	56
Appendix A. Terms of Reference.....	57
Appendix B. Task Force Membership.....	60
Appendix C. Presentations to the Task Force.....	63
Appendix D. Glossary.....	66

## **Volume II. Supporting Papers**

Chapter 1. Scenario and Systems Analysis

Chapter 2. Intelligence

Chapter 3. Defensive Countermeasures against Weapons of Mass  
Destruction: Assessments and Recommendations

Chapter 4. Categorizing Federal Investments for Reducing the  
Threat of Weapons of Mass Destruction

## **Preface**

This study was completed with an initial reporting of findings and recommendations provided in mid-August 2005, about two weeks before the devastation of New Orleans, Louisiana by Hurricane Katrina. Unfortunately, the findings of this study in the areas of "mitigation and recovery" were demonstrated to be almost universally valid. The weaknesses in planning and in command, control, and communication and lack of clarity in lines of responsibility and authority that are discussed herein were quite obvious in the response to Katrina.

Special attention should be given to the discussions in this report concerning "truly catastrophic" events and the potential need to rapidly bring the active duty military into a dominant, albeit temporary, role. Katrina fits the definition intended in this report of truly catastrophic—state and local responders were overwhelmed and the capabilities, discipline, clear line of command and control, and communications that the military could have brought to bear would have made a real difference in the early stages of response.



## Executive Summary

Reducing U.S. vulnerabilities to weapons of mass destruction is a topic of great importance to the nation's security. The technology of weapons of mass destruction (WMD) has proliferated in the past decade as information and capabilities have become more accessible. Thus, actions to prevent such an attack should have high priority for the U.S. government and the Department of Defense.

Why is the threat from weapons of mass destruction so important today? After all, the United States faced the potential of massive destruction from nuclear weapons in the former Soviet Union for nearly half a century during the Cold War. The principle answer lies in the uniqueness of the security environment today. The growing spread of weapons of mass destruction provides small groups of individuals with the ability to deliver devastating harm to the United States. Such power, in the past, could only be delivered by nation-states with large economic, political, industrial, military, and social resources. Furthermore, these resources were valued by nation-states and could be readily held at risk—making such policies as “mutually assured destruction” effective in dealing with the threat.

In contrast, a loose band of terrorists, with few assets and no permanent geographic base, has the potential to deliver massive damage. With few tangible physical assets at risk and a willingness to “die in the pursuit of their cause,” conventional measures of deterrence are at best elusive. It is for this reason that the full spectrum of potential responses—including prevention, interdiction, mitigation, and recovery responses—needs to be brought to bear on the problem. This “full spectrum” theme is the cornerstone of the findings of this study.

Much of the ongoing dialogue and activity concerning the WMD challenge has focused on limited aspects of a single modality—whether biological, chemical, nuclear, or radiological. Concerns such as detection, defeat, or consequence management tend to be addressed in isolation and specific to a single modality. This segmented approach

does not lend itself to the development of an integrated system and approach for responding to and managing the threat.

As a result, the Defense Science Board took a fresh approach in examining the WMD challenge—one that addresses the problem from an end-to-end perspective in order to assess the proper balance of requirements and resource allocation. The strategy adopted by the study is as follows:

1. Do everything possible to **prevent** the worst people from acquiring and using the worst weapons.
2. Increase the urgency of efforts to **mitigate** the consequences and **recover** from the impact of an attack.
3. **Identify** the perpetrators and their supporters and devise clear and plan options for **response** to an attack.

**In the end, the task force concluded that no single approach is sufficient.** All contribute, but all have limitations. To better position the United States against this threat the task force recommends actions in the following six areas:

- Improve intelligence
- Deny weapon acquisition
- Develop retaliation policies
- Improve national mitigation and recovery capabilities
- Establish DOD pilot programs and develop catastrophe response plans
- Develop and use readiness metrics for enterprise management

## **Improve Intelligence**

Improving intelligence is a necessary enabler for all other steps to reduce WMD vulnerability. This challenge is beyond the scope of any one country or organization to solve alone. Still, DOD can help create a truly integrated WMD intelligence community focused on improving strategic “knowledge” through innovative collection, dramatically



revitalized analysis, and a “war room” mentality for attacking the problem and influencing the plans and perspectives of relevant actors.

Specifically, we believe that the Under Secretary of Defense for Intelligence and the Director of National Intelligence should implement and go beyond the recommendations of the 9/11 and WMD commissions in the following areas:

- Move to **greater emphasis on tracking key individuals and entities with WMD expertise** and their links to radial states and groups. Monitor their financial transactions and transportation means and nodes, including across foreign and domestic intelligence lines and between federal and state and local entities.
- Support measures to **increase fielding of deep penetration intelligence programs**. Exploit capabilities for technical collection attuned to the WMD threat and establish enhanced mechanisms for communication and data processing.
- Continue to **build capabilities for effective persistent surveillance, including the contribution made by tagging, tracking, and locating capabilities**. Implement the recommendations of prior Defense Science Board studies to bring order and reliable funding to the development and deployment of tagging, tracking, and locating systems.
- Ensure that the efforts to increase collected information in the above areas are **driven by analysts and the users of intelligence and informed by expert target development**.
- **Establish federated data bases** that focus on individuals and their activities and that connect information across agencies and across domestic and foreign intelligence sources.
- Create on-going, broadly-based mechanisms and relationships to **develop a better understanding of the motives, objectives, and values of potential adversaries who might use WMD**.
- **Establish a mission manager** with responsibility to coordinate and integrate the intelligence community's efforts with respect to terrorist pursuit of WMD, including coordination with domestic law enforcement.

## Deny Weapon Acquisition

The first priority for the nation is to prevent an attack. Toward that end, the United States needs to take actions to make the adversary's job as difficult and dangerous as possible and to minimize the likelihood that he will achieve his goals. The worst forms of WMD—nuclear and, in some cases, biological—would likely be acquired by terrorists from nation-state proliferators. So there is much to gain by reducing the stockpiles of these weapons worldwide and securing weapons materials.

Furthermore, many forms of WMD—chemical, biological, and radiological—are available in the United States. It appears that the easiest approach for terrorists would be to steal, purchase, produce, or exploit weapons materials inside the United States, as the United States has excellent infrastructure for scientific and technological development and makes this infrastructure readily accessible.

The task force recommends that the U.S. government

- **Strengthen and broaden international cooperative efforts in nonproliferation** to include treaties, the Proliferation Security Initiative, Nunn-Lugar, and special diplomatic efforts. The reach of these efforts should expand to include other countries, biological weapons, and “loose expertise.”
- **Remove easy access to WMD material in the United States**, particularly radiological and chemical. Actions that should be taken include increasing physical security around sites near major population centers, using transportation routes away from major population centers, and, when possible, substituting materials that can be easily weaponized for those that are less so (many industrial chemicals have less toxic formulations).

## Develop Credible Retaliation Policies

The President has made clear the nation's intent to punish anyone who uses WMD against the United States or its interests abroad, or in any way aids and abets this use. The task force believes this to be the right policy.

The credibility of declaratory policies depends on the ability of the United States to identify the source of the attack through technical forensics combined with intelligence information. Every effort should be made to improve these capabilities to provide accuracy and speed of attribution.

Developing response options is the other essential ingredient for effective policies of deterrence. Response options should be developed prior to an attack and must take advantage of all elements of national power including diplomatic, economic, and military responses. Relying on ad hoc responses, in the midst of chaos, is not an effective approach. Rather, a disciplined and comprehensive process is needed to address the subject well in advance, so that, at a minimum, the issues and options are identified.

The task force believes that the following actions are essential to improving the nation's ability to attribute attacks and develop retaliation policies.

- **Continue to articulate clear policies for retaliation.**
- **Improve tactical forensics capabilities** as much as possible in order to improve attribution.
- **Extend planning of retaliation options** that could punish potential attackers and their supporters and suppliers for a wide variety of participants and participation in an attack. Create a WMD-retaliation planning structure to develop military options and the equivalent capability at the national level to bring to bear all organs of national power. Subject these plans to simulations, gaming, exercises, and red teaming to gain insight into options and enhance effectiveness should execution be required. Publicize the existence of retaliation plans.

## **Improve National Mitigation and Recovery Capabilities**

Should prevention fail the next priority for the nation is to minimize the impact of an attack on the United States. Mitigation and recovery is a national responsibility that involves many federal, state,

and local organizations. Despite the many efforts and programs in progress, the nation is still poorly prepared to mitigate the impact of a WMD attack. This lack of preparation appears to result from several key factors: fuzzy lines of responsibility and authority among local, state, regional, and federal agencies involved; a lack of a sense of urgency; and a tendency to emphasize physical effects of an attack with little regard for the psychological.

Reducing the nation's vulnerability to WMD requires a comprehensive approach across the spectrum from intelligence and prevention to mitigation, recovery, and response. A coherent approach must overcome the challenges of coordinating among many layers of government responsibility as well as involve the private sector, with greater cooperation and collaboration essential. Further, maintaining public support and understanding must be recognized as an important element of national preparedness.

In the area of national mitigation and recovery, the task force recommends the following:

- **Focus on the highest payoff mitigation and recovery efforts** to include:
  - **Executable planning, exercises, and command, control, and communications (C3)**, including a fully interoperable communications and information system across all organizations involved.
  - **Radically increased medical surge capabilities**, such as emergency medical technician training for DOD civilian employees and telemedicine support. Developing a medical surge capability should be a high national priority.
  - **Research and development on specific, modality-unique, high-payoff countermeasures**. Such countermeasures include advanced medical countermeasures, advanced decontamination technology and techniques, effective detect-to-warn and detect-to-treat capabilities, and automated detection and air-flow control for facilities.

- **Publicly articulate the situation regarding terrorist use of WMD** clearly and honestly, with realistic assessments and guidance, to gain and maintain public support and to increase the sense of urgency. Participation by the President, Secretary of Defense, and senior officials in the Department of Homeland Security is essential.

## **Establish DOD Pilot Programs and Develop Catastrophe Response Plans**

Responsibilities for mitigation and recovery fall on both civil departments and the Department of Defense. DOD has clear responsibility for protecting its forces both at home and abroad and assuring the ability to project force. To accomplish this mission, however, DOD depends heavily on civil infrastructure—a gray zone of responsibility in which DOD plays a role in mitigation and recovery. Thus, a more comprehensive approach to base and local community protection is needed, one that takes a systematic look across all modalities, is informed by risk assessment, and is implemented with standards and best practices.

As well, DOD has unique capabilities that could contribute to a national architecture for mitigation and recovery—capabilities such as planning and exercising, extensive experience with C3 and information systems, operating in adversarial conditions, and extensive resources that can be brought to bear in the event of a truly catastrophic attack. The task force believes that the nation should draw on DOD's expertise and experience, in advance of an attack, to help lead and train a national mitigation and recovery capability. Furthermore, DOD should be prepared to provide all needed capabilities should it be called on in response to an attack. Detailed catastrophe planning must be undertaken now—planning analogous to classic “war planning” in which DOD is so effective.

The Department of Defense should accelerate action on its responsibilities in mitigation and recovery and, at the same time, lead the way for the civil community. In this area the task force recommends three initial actions as follows:

- Establish **a comprehensive base protection pilot program to protect four military installations** building on prior pilot programs.
- **Design and develop robust, interoperable situation awareness and C3 capabilities.** Negotiate with the Department of Homeland Security to lead in the development and prototyping of a national C3 capability.
- **Develop detailed plans**—modeled after “war plans”—for execution of DOD responsibilities, if directed to provide full support of an attacked region for mitigation and recovery operations.

## Develop and Use Readiness Metrics for Enterprise Management

A new organizational approach, with requisite staff and budget resources, will be required to create an effective counter-WMD effort within the U.S. government. **The task force believes that one single individual must be charged with this responsibility—someone who is positioned to see the whole WMD picture and who can provide to the President an assessment of the nation’s capabilities and readiness to address the threat from WMD. Today, no one has that visibility.**

To aid in the development of these regular assessments, the task force recommends that the nation **develop an enterprise readiness process and system** that can provide assessment of each of the major capabilities required to reduce U.S. vulnerability to WMD and overall national preparedness. Such assessments can help to prioritize activities, inform resource allocation, and measure progress. Recommended actions include the following:

- Create a small group chartered and empowered to **develop a readiness process**, reporting to the Secretary of Homeland Security or the White House.
- Initially **create a special cell** in the Office of the Secretary of Defense, Program Analysis and Evaluation **to provide an**

**objective review** and analysis (including metrics) of government-wide efforts to reduce vulnerability to WMD.

- **Create red teams and conduct regular simulation exercises** to challenge the assessments and collect data against which to evaluate metrics.

## **In Conclusion**

In summary, the task force has identified six high-payoff areas of recommendations that will greatly reduce U.S. vulnerabilities to weapons of mass destruction. These recommendations reflect opportunities for the nation that are very high payoff at relatively low cost. Yet, despite the high payoff and low cost, the task force found no evidence that these efforts are being aggressively pursued.

Effective implementation of all six recommendations would, in the assessment of the task force, significantly reduce the impact of most forms of WMD—chemical, biological, radiological. A nuclear attack is in a class by itself and remains a serious threat. Campaign attacks also remain potentially catastrophic due to the potential for widespread destruction. To implement these initial recommendations would require about \$4 billion of additional investment annually. It is an investment that the country should make.





## Chapter 1. Introduction

Reducing U.S. vulnerabilities to weapons of mass destruction is a topic of great importance to the nation's security. President Bush has repeatedly talked about keeping the worst weapons out of the hands of the worst people as a national priority. It is the worst people who are the most likely to use weapons of mass destruction. And the U.S. homeland is a likely place for them to do so.

The technology of weapons of mass destruction has propagated in the past decade as information and capabilities have become more accessible. That is not to say that it would be easy to execute an attack using weapons of mass destruction (WMD), as many complex tasks must be accomplished to do so effectively. But it does mean that actions to prevent such an attack should have high priority for the U.S. government and the Department of Defense.

At the request of the Secretary of Defense and under the direction of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD [AT&L]), the Defense Science Board (DSB) conducted a study on reducing vulnerabilities to weapons of mass destruction to aid the department in addressing this vital concern.<sup>1</sup> Much of the ongoing dialogue and activity concerning this challenge has focused on limited aspects of a single modality—whether biological, chemical, nuclear, or radiological. Concerns such as detection, defeat, or consequence management tend to be addressed in isolation and specific to a single modality.

While these single-modality approaches are useful, they do not lend themselves to the development of an integrated system and approach for responding to and managing this threat—one that addresses the problem from an end-to-end perspective and would support assessment of the proper balance of requirements and resource allocation. The current segmented approach does not allow for such assessments. Furthermore, the nation must be able to handle the different modalities

---

1. Appendix A contains the complete terms of reference for this study.

singularly or in combination, and must be able to manage the spectrum of response from preemption to consequence management. Without a systematic approach, it is impossible to properly identify capability gaps, changes in priorities, or changes in the threat across this spectrum. An integrated approach would better support end-to-end assessment of the state of affairs in WMD defense.

Thus, as directed by the USD (AT&L), this study addresses the challenge of reducing vulnerabilities to WMD from a fresh perspective. The principles underlying this study include the following:

- Concentrate on defending the homeland against terrorist use of WMD or clandestine use by a nation-state
- Examine the problem from a broad national perspective, not limited to that of the Department of Defense
- Take a systematic look across all WMD modalities
- Include civil and military considerations
- Consider the challenge both at home and abroad

Because of the breadth of such an effort, the scope of the study was limited by the following. WMD is defined as including chemical, biological, radiological, and nuclear. The study did not directly examine attacks on information systems, multiple conventional attacks, or attacks by electromagnetic pulse or other similar events. Yet, in the end, many of the recommendations set forth in this study could apply to those types of attacks as well. The study did not attempt to assess the details of ongoing programs except as they had an impact on broader goals.

The study drew experts from government, industry, academia, research and development centers, laboratories, the medical profession, and many others to support its effort to address this topic in a systematic way. As such, these experts were not organized in the typical way, by individual modalities—chemical, biological, nuclear, and radiological. Instead the team was organized in panels to address system analysis, cross-modalities, mitigation and recovery, intelligence, and investment,

with ad hoc panels forming as needed to address topics such as understanding the adversary and response options.<sup>2</sup>

The task force listened to many presentations to gain an understanding of current planning, investment, and capability development in DOD and across the government at the national, state, and local levels; to understand the current state of intelligence regarding the threat; and to learn about the efforts underway and organizational structures in place today.<sup>3</sup> This base of understanding informed the panel deliberations and contributed to formulation of the final recommendations.

The chapters that follow detail the findings and recommendations of the task force.<sup>4</sup> Chapter 2 begins with the analytic methodology, followed in Chapter 3 by a brief survey of the threat. The subjects covered in Chapters 4 through 7 focus on the primary areas of recommendations. They are as follows:

- Intelligence
- Preventing an attack
- Mitigation and recovery
- Managing the enterprise

The report concludes with a final chapter summarizing the recommendations, including a top-level investment analysis and estimate of costs to implement the recommendations.

Before turning to the next chapter, the strategy adopted by the study is this:

1. Do everything possible to **prevent** the worst people from acquiring and using the worst weapons.

---

2. Appendix B contains the membership of the task force.

3. Presentations to the task force—during both plenary and individual panel sessions—are listed in Appendix C.

4. The chapters in this main report provide an overview of the analysis conducted by the task force and the findings and recommendations of the task force. Much analytic work and detailed assessments underlie these conclusions and are contained in a second volume of supporting reports.

2. Increase the urgency of efforts to **mitigate** the consequences and **recover** from the impact of an attack.
3. Improve the means to **identify** the perpetrators and their supporters and devise clear and more comprehensively expand options for **response** to an attack.

**In the end, the task force concluded that no single approach is sufficient. All contribute, but all have limitations.**

## Chapter 2. Analytic Methodology

This study examined a very long list of potential actions that might be taken to respond to the WMD threat. Some of these actions were unique to a single modality and others were more broadly applicable. One of the major goals for the study, as set by the Secretary of Defense, was to find a systematic approach to prioritize these diverse options in a disciplined manner. In response, this study developed such an approach, described in detail in volume 2 and summarized in this chapter. This methodology was used to determine the highest payoff items for recommendation by the study.

### Scenario Analysis

As a basis for its assessment of potential approaches to the WMD threat, the task force analyzed 14 scenarios that span the nuclear, biological, chemical, and radiological modalities (table 1). These scenarios were based on scenarios developed for the Department of Homeland Security (DHS), with some modification, as indicated in table 1.

To provide context for the analysis, we assigned a “class” of perpetrator to each scenario in order to understand the extent to which this variable might impact our ability to deal with the situation. For this purpose, the task force used three characteristic adversaries, as follows:

- A hostile state actor that was geographically based
- A major nonstate actor with a large organization but who was not geographically based or characterized by a fixed infrastructure (e.g., al Qaeda)
- A splinter group either separate from, or acting independently of, a nonstate parent (e.g., Jemaah Islamiyah, Aum Shinrykyo)

**Table 1.** Fourteen Scenarios Analyzed

1.	Improvised nuclear device using highly enriched uranium stolen from the former Soviet Union	<b>Nuclear</b>
2.	Nuclear-tipped cruise missile off false flagged freighter into Los Angeles***	
3.	Nuclear blackmail of coalition states near end of regime change***	
4.	Volunteer-carried bio attack using stolen flu samples*	<b>Biological</b>
5.	Machined anthrax spores dispersed through airborne sprayer**	
6.	Plague in pressure canisters in airport and sports arena	
7.	Foot and mouth disease contamination of feed and transport sites	
8.	Meat and orange juice processing plants contaminated with liquid anthrax	<b>Chemical</b>
9.	Blowing up high pressure chlorine tank in industrial park	
10.	Sarin purchased on black market introduced into office building heating, ventilating, and air conditioning system	
11.	Multi-agent toxic industrial chemical release from coordinated attack on refinery and port	
12.	WWII Japan blister agent released by small plane on sports stadium	
13.	Chemical attack on U.S. base in the Middle East***	
14.	Coordinated three-city cesium radiological dispersal device attack using truck bombs	<b>Radiological</b>
* Converted from natural disaster in DHS scenario ** Converted from truck dispersal in DHS scenario *** Created for DSB Study		

For each scenario, the task force evaluated what occurred during the event, the terrorist workflow required to carry out the event from initial planning through execution and escape, the consequences of an unmitigated attack, and the major civil and medical response tasks. Using the adversary work flow and today's mitigation and response capabilities, the task force looked for both near- and mid-term opportunities for improvements in five principal areas of effectiveness used throughout the study—prevention, interdiction, mitigation, attribution, and retribution.<sup>5</sup> For those improvements that appeared to have a significant impact, their relative contribution was measured on a zero to one scale, roughly corresponding to the following definitions. In addition, the numerical range was evenly divided into a qualitative range of poor, fair, good, and excellent.

- *Prevention.* The probability that the critical material supply, if any, would be shut down to the would-be perpetrator or that the act would be uncovered (and therefore prevented) by intelligence during the planning stage.
- *Interdiction.* The probability that the perpetrators or their weapon would be discovered and/or caught while carrying out the act.
- *Mitigation.* The degree to which casualties or economic damage would be reduced by improved response actions.
- *Attribution.* The probability that the United States would be able to identify the perpetrators, their supporters, or their suppliers.
- *Retribution.* The probability that the United States, given proper attribution of the act, could deliver the desired degree of retribution in terms that struck at the heart of the adversary's value structure.

Each of the 14 scenarios was evaluated in this fashion, identifying specific opportunities to prevent, interdict, mitigate, attribute, and deliver appropriate retribution. The result was a rich set of capabilities and defensive and offensive options. To prioritize and identify the most

---

5. Volume 2 of this report contains a chapter presenting the detailed analysis conducted for each of the fourteen scenarios and the methodology used for identifying the most promising actions.

promising actions, the options were rated in terms of both impact and the degree of devastation that occurred in the scenario.

The options with the highest rating were those that had a major impact on most of the worst scenarios. A somewhat lower rating was assigned to those options that had a major impact on many less severe scenarios. Still lower were those options that had a minor impact on several scenarios. Those options rated the lowest had only a minor impact on only a few scenarios that resulted in only a small amount of damage.

The summary results of this evaluation are shown in table 2. The first column describes the scenario, followed by the potential unmitigated damage incurred from each—damage in terms of “equivalent” casualties, which combined the effects of people killed, people injured, and economic damage.<sup>6</sup> Of the many options evaluated, the top recommendations, which will be discussed in the following chapters, are summarized in the remaining columns, with a rating of the impact of those actions on each scenario.

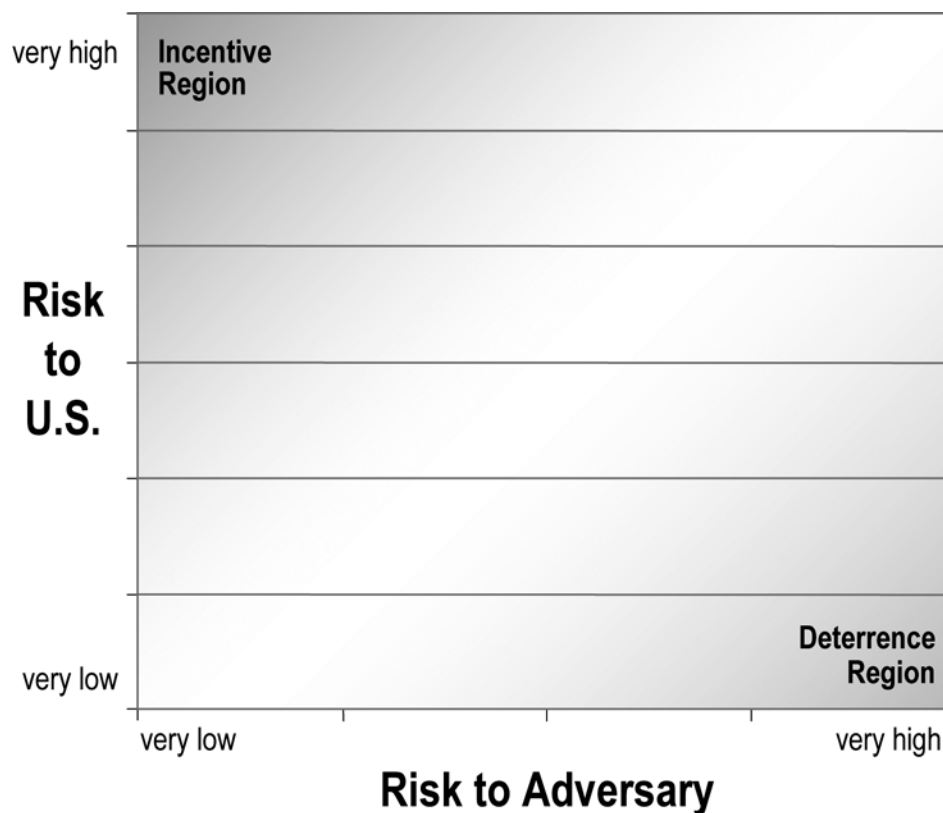
**Table 2.** Impact of Primary Study Recommendations on Scenarios

Scenario	Damage (equivalent casualties)	#1 Intelligence Improvements	#2 Material Control Actions	#3 Retaliation Plans	#4 National Readiness Improvements	#5 DOD Catastrophe Response
Nuclear blackmail	850,000	Major	Minor		Major	Minor
CM nuke	700,000	Major	Minor	Major	Major	Major
Improvise nuke	650,000	Major	Major	Major	Major	Major
Aerosol anthrax	130,000	Major	Minor	Major	Major	Major
Chlorine tank	45,000	Major	Major	Minor	Major	Major
RDD in 3 cities	26,000	Major	Major	Major	Major	Major
Sarin in building	8,000	Major	Minor	Major	Major	Minor
Blister agent in stadium	7,400	Major		Major	Major	Minor
Plague in arena	3,200	Major	Major	Minor	Major	
TIC at refinery/port	3,000	Major	Major	Major	Major	
Flu human spread	1,300	Major	Minor	Minor	Major	
Foot and mouth	1,000	Major		Major	Minor	
Chemical in Mid -East U.S. Base	600	Major		Major		Major
Food contamination	600	Major	Minor	Major	Minor	

6. Further explanation of how this calculation was made can be found in volume 2.



Figure 1 offers another view of the impact of these top five recommendations. What is plotted in this figure is the risk of each scenario to the United States in terms of how likely it is that the attack will succeed and the level of casualties that will result after mitigation. It is, in effect, a casualty expectation. The risk to the adversary represents the degree to which he will be caught or identified and whether the United States will be able to retaliate effectively against either the adversary or his suppliers and helpers.



**Figure 1.** Scenario Assessment

Figure 1 shows a visualization of risks for both red and blue (which, in the classified report, includes data for the 14 scenarios). Note that the upper left hand area of the chart is the region in which a potential adversary can inflict major damage on the United States with little risk to himself—a dangerous and unstable region of high incentive to a

potential attacker. In contrast, the lower right hand area on the chart is that region in which a potential attacker achieves low impact on the United States while exposing himself to a high likelihood of receiving an unacceptable level of retribution—a region of credible deterrence.

In addition to the quantitative and qualitative assessments that resulted from these analyses, the work also highlighted a number of general observations, including the following:

- Nuclear terrorism is in a class by itself, particularly for single events. Even if the combination of prevention, interdiction, and mitigation were to reduce damage expectation by 100X, it would still be unacceptable. This expectation underscores the need to do everything possible to deter both the use of nuclear weapons as well as the supply of critical materials. Since that supply is largely available only from nation-states, deterrence of supply should be a major objective.
- All scenarios are characterized by complex attacker workflow. This characteristic provides many opportunities for intelligence interaction. The three most common signatures are acquisition of specialized chemical, biological, radiological, and nuclear (CBRN) materials; convergence of technical specialists at unusual places (such as a farmhouse); and the repeated presence of unaffiliated persons at critical U.S. urban or industrial infrastructure sites.
- The easiest way for terrorists to acquire hazardous chemical material is to purchase/steal/use existing material in unsecured sites in the United States. Securing the most serious of these sites is an obvious option which is being pursued, albeit with inadequate urgency.
- The DHS scenarios underestimate the potential impact of WMD attacks. The damage estimates, particularly economic damage, tend to be low, the impact of repetition is not fully exploited, and delivery mechanisms are often far less than optimum from the viewpoint of a potential terrorist attacker.
- The type of analysis described in this chapter, done more completely and supported with an ongoing red-team activity can

provide a useful basis for readiness assessment across the entire federal, state, and local enterprise. It should include and be supported by outside expertise within the enterprise management structure of the U.S. counter-WMD effort.

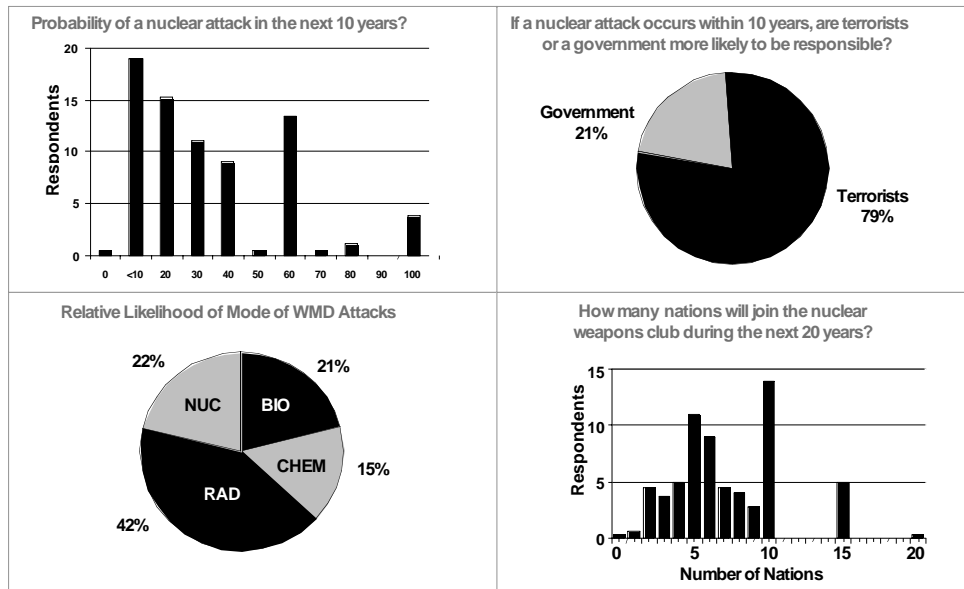
This overall assessment is indicative of the challenge posed by the threat: the task force found no easy solutions to this broad range of threats and broad range of weapon choices. Still, there are steps that the United States can take to reduce its vulnerability, as the chapters that follow will illustrate.

## Chapter 3. The Threat

Combating terrorist use of WMD requires foresight and action. Today, the nation faces a different kind of threat. It is not possible to observe the equivalent of nuclear testing. There aren't submarines slipping quietly below the surface of the ocean. The equivalent of nuclear silos is not under construction. Thus, this is a tough challenge to address, but one with disastrous consequences if the nation fails to do so.

Figure 2 portrays some interesting survey results—opinions of more than 100 national security and nonproliferation experts—that serve to highlight the changing nature of today's threat. The results are somewhat surprising, in fact—at least in terms of the severity of the threat and how it is characterized. The top left quadrant addresses the probability of a nuclear attack in the next ten years. Over half of those responding believe the probability will be greater than 30 percent over the next decade. That response is 10 or 100 times what we used to think the likelihood of a nuclear event might be (often described as “high consequence, low probability” a few years ago).

Nearly 80 percent of those responding believe that terrorists would most likely be responsible if a nuclear attack were to occur in the next 10 years (top right); only 21 percent believe that the government of a nation-state would be responsible. Over half of the respondents thought that there would be an average of 7 or 8 more nations joining the nuclear club during the next two decades (bottom left). And nearly half of those responding believed that a dirty weapon would be the weapon of choice, were an attack to occur—twice that of any other mode of attack (bottom right). This last result most likely reflects the relative ease with which a terrorist could acquire a dirty weapon as compared to chemical, biological, or nuclear. Thus, securing radiological material everywhere in the world should be a high priority if one agrees with these experts.



Source: The Lugar Survey on Proliferation Threats and Responses, June 2005

Note: Data shown are responses of 132 national security and nonproliferation experts.

**Figure 2.** Responses from the Lugar Survey

Our examination of the threat highlighted one very important fact: more relevant information than we currently collect is available and must be assimilated. Further, we have far less information on terrorists as compared to nation-states and the information that is available is far less detailed and specific. What we do know is that there is an increasing number of potential perpetrators and proliferators due in large measure to the increasing availability of materials, “know how,” and weapons. Furthermore, the likelihood of an attack is estimated to be substantial in the view of today’s leaders and well-informed experts in national security.

Not only is the threat far more complex than in the past, but the ability of the United States to respond is not as straightforward. The nation’s cold war WMD strategy was based on deterrence through mutual assured destruction. The threat was characterized by an established government, monolithic control, clear motivations and objectives, a large structured military, a substantial industrial and

economic base, and geographic clarity. That characterization reflects little of what the United States faces today. Instead the threat has no established government; different agendas, motivations, and objectives; far less structure; no clear economic base that could be held at risk; and even the geography is uncertain. We must refine our strategies to assure appropriate response to this threat.

Despite its complexity and danger, however, this threat is taken with varying degrees of seriousness. By our view, the most senior leadership is taking this threat very seriously—it is discussed in speeches and is identified as the number one threat in national security strategy and guidance. However, the sense of urgency at lower levels is less palpable. While preliminary steps are evident, and positive steps have been taken, far more is needed to turn these actions into a comprehensive capability. Our findings and recommendations will address this need.

## Chapter 4. Intelligence

Improving intelligence is a necessary enabler for all other steps to reduce WMD vulnerability. It is beyond the scope of any one country or organization to solve alone. Still, DOD can help create a truly integrated WMD intelligence community focused on improving strategic “knowledge” through innovative collection, dramatically revitalized analysis, and a “war room” mentality for attacking the problem and influencing the plans and perspectives of relevant actors.

The task force is aware that this topic enjoys high priority in the U.S. Intelligence Community and that considerable effort is being exerted to satisfy WMD intelligence needs. There have been impressive successes in collection, analysis, covert action, and support to the policy community. The task force is also aware, however, that many of the successes have been resource intensive and cannot be easily scaled across the breadth of the WMD challenges that the United States faces. Further, there are competing requirements for available resources and a number of programs confronting difficulties and in need of additional funds either to achieve operational status or to build upon prior successes. Our government’s resources are not infinite and these matters of target development, resource allocation, and collection strategy demand immediate redress.

This study had neither the intention nor resources to duplicate the work of the many commissions, Congressional inquiries, and studies that have offered important findings and recommendations related to intelligence. We instead viewed these findings and recommendations within the context of our own study and offer the following additional observations and recommendations from that more limited perspective.

The remainder of this chapter discusses, more specifically, the major concerns of the task force. First, there is a need for much more information. Second, there is a need for an accessible data base that is comprehensive—including both domestic and foreign information. Analysis of this information needs to be carried out in the context of the

best understanding of the adversary that we can achieve. Finally, the lines of authority and responsibility must ensure that there are no seams.

## **Improving Collection—The “Dots”**

The major intelligence challenge posed by terrorist or covert use of WMD is a lack of information. Analysts interviewed by the task force reported that there is decidedly less information today on this topic than there was five years ago. If the analysts are correct, it is unclear why the volume of information is declining. Whatever the reason, important decisions about the WMD threat are being made based on limited amounts of information.

The task force agrees with the observations of the WMD Commission that “the collection of information is the foundation for everything that the Intelligence Community does.” There is good work underway to enhance the community’s collection capabilities. This work needs to continue and success reinforced across a broad range of collection methods. It must also be adequately resourced in order to satisfy the nation’s urgent information needs against terrorism and WMD.

Detailed discussion of collection issues is classified and outlined in Volumes 1 and 2 of the classified report for this study.

The task force is aware that considerable effort is being expended in this area. Some of the approaches use existing and traditional collection means, while others require entirely new concepts in information systems intelligence. The limited review conducted for this study suggests that the traditional approaches continue to receive the highest level of funding and priority in resources. At the same time the most important, actionable, and insightful knowledge is being obtained by other techniques.



## **Improving Analysis and Information Management—“Connecting The Dots”**

The nature of conflict has changed. Where intelligence once focused on fixed installations as the target, there is now equal, if not more, concern with individuals and groups of individuals. Individuals are the new “high value targets.” It is thus useful to update the 20<sup>th</sup> century’s approaches to recognize this change. It is equally useful to view defense operations from an information perspective—a “data-centric” view of the enterprise.

### ***Federated Intelligence Data Base***

Two vestiges of the Cold War offer important constructs that can be adapted to today’s challenge. The first, the Modernized Integrated Data Base (MIDB), is a database of fixed (adversary) installations of potential strike interest—a “bomb encyclopedia”, in which every potential target has an entry and a bomb encyclopedia number. The second, the Joint Strategic Target Planning Staff (JSTPS), was formed to optimize nuclear targeting across the services and delivery systems. The JSTPS developed nuclear targeting policies and strategies and were premier users of the MIDB. The task force recommends adapting these two concepts to the terrorist WMD challenge.<sup>7</sup>

Accountability for the integrated data and data structures—the updated MIDB—will rest with both the Secretary of Defense and the Director of National Intelligence (DNI). The role of provisioning the database is clearly the responsibility of the DNI. Oversight of the database as a whole should rest with the Secretary of Defense, as the principal user. The role as overseer must take into account the various stakeholders of interest, which include U.S. Northern Command, U.S. Strategic Command, the Departments of Homeland Security and Justice, the President’s newly appointed principal for information

---

7. The analogy is that MIDB was a collection of “everything” that was known about each target. JSTPS was a user-dominated analysis and planning organization with full access to everything in the MIDB. In the modern case, the targets will largely be people (or groups of people) and things that are either mobile or fixed.

sharing, the chief information officers of the respective departments and agencies, and the Defense Information Systems Agency.

Operation of the database will require much collaboration. While the collective set of information must act as a single database, it is unlikely to be implemented that way. “Owners” of the component databases have legitimate responsibility for data assurance and for protecting the sources and methods by which data have been acquired. Modern ideas of federation and common-services architecture, coupled with data assurance methods such as public key infrastructure, should be utilized. The challenge is further exacerbated by the essential need to include both foreign and domestic information. Indeed, this is a challenge that the Director of National Intelligence and the President’s principal for information sharing must manage.

We thus recommend that the Secretary of Defense, through his Under Secretaries for Policy and Intelligence, and through the Chairman of the Joint Chiefs of Staff, assign responsibilities for the immediate push to unify such relevant data within the Department of Defense, and to prepare for a more global integration across other designated departments and agencies.<sup>8</sup>

Concomitant with the database efforts must be creation of and funding for the new doctrine, organization, and forces structure associated with the “new JSTPS.” This organization would provide the intellectual stimulus for designing response options to a WMD assault on the U.S. homeland. Deterrence is the most difficult, but most satisfying, answer to the WMD conundrum. It rests on the bedrock of attribution and retribution—credibly holding at risk something a potential adversary holds of value. With nation-states, there is generally a rich set of things to hold at risk; for nonstate actors this set may be sparse. The Intelligence Community must harness the intellectual horsepower required to address this challenge—at a level equivalent to that employed throughout the Cold War.

---

8. Volume 2 of this report contains a more detailed chapter on the intelligence challenge related to the WMD threat. It specifies additional actions to be undertaken in support of these recommendations.

The task force thus recommends that the Secretary of Defense assign his Under Secretary of Defense for Policy (USD [P]) responsibility for overseeing and, through the Chairman and the Commander of U.S. Strategic Command, accomplishing the formation of a joint strategic WMD operations response organization. This group should work closely with and support an equivalent organization under the National Security Council.

### ***Understanding the Adversary***

The 21<sup>st</sup> century presented the nation with a new genre of adversary—the rise of communities and societies significantly different than the nation-state. The United States is not yet well equipped to deal with this new adversary, in terms of institutions or processes. Without deep understanding of an adversary, there is no context for gathering intelligence information and little ability to hold his values at risk.

An understanding is needed of local, communal, and societal views; cultural norms and values; historic experience and ethos; and contemporary political context. In addition, an understanding of the perceived impact on these groups of western culture and U.S. policy is also useful when contemplating engagement with or actions against them.

While increased attention is being placed on understanding nonstate actors, the task force is concerned that much of this effort is focused on tactical information for tactical objectives that are focused on near-term problems and threats facing the United States. Instead, a deeper, more strategic understanding of emerging global trends with respect to nonstate actors and their desire for increased legitimacy will better inform the formation of more enduring policies, planning, and actions.

Today, the Intelligence Community does not have the resources to support the type of in-depth, strategic intelligence needed. The task force therefore recommends that the Secretary of Defense work with the Director of National Intelligence to establish a small cell of subject matter experts, drawn from a variety of organizations, both inside and outside of government, to focus on emerging trends and groups posing a threat to U.S. interests. This initiative could be limited in both size and time to avoid establishing a new bureaucracy and should be

replenished on a periodic basis to avoid stagnation. They should set up a forum to draw on all available cultural resources with an aim toward creating the best possible understanding of motivations, values, objectives, and weaknesses of individual, groups, clans, and ethnic and religious groups and members.

The goal of such a group would be to develop in-depth intelligence and knowledge of emerging adversaries to inform strategic and tactical intelligence gathering efforts as well as policy and military decision making. The group could also serve as a red team and a source of analysis alternative to institutional efforts and sensitivities. Intelligence analysts who serve in this cell would return to their respective organizations with greater expertise, understanding, and knowledge of adversaries.

The results of the deliberations of this cell should be channeled to intelligence analysts as well as those responsible for planning potential response options in case of a WMD event. Volume 2 of this report offers the provocative views of one leading expert on nonstate actors and alternative societies. The paper outlines some of the themes that such a forum of experts should explore.

## **Enabling More Effective Collection and Analysis**

Integrating activities across the Intelligence Community to support both national, battlefield, homeland security, and law enforcement missions is a significant challenge. Integration must reach across a matrix of intelligence departments and agencies as well as orthogonal institutions such as the National Intelligence Council, intelligence centers, mission managers, task forces, and other related groups.

Of particular relevance is addressing the challenge of simultaneously acquiring and protecting new and effective sources and methods while maximizing information sharing. A new Information Sharing Executive has been assigned by the President to focus on this task. Furthermore, an environment of risk-taking must be allowed and even encouraged within a restructured and transformed intelligence apparatus. Today's class of WMD threats require proactive, preventative, and even preemptive and provocative intelligence activities, which require a

community that is forward-leaning in the areas discussed previously in this chapter—an approach that is strongly supported by this study.

Coordinating and integrating the nation's resources against terrorist acquisition and unconventional use of WMD—including intelligence resources—must be a priority. The recent creation of a National Counterterrorism Center and a smaller National Counterproliferation Center has potentially introduced simultaneously disconnected and duplicative missions. The task force is concerned about whether these organizations have been unambiguously tasked with the specific responsibility to oversee, coordinate, and direct the Intelligence Community's efforts at the intersection of counterterrorism and counterproliferation—efforts that include collection, analysis, operational planning, and policy development.

As a result, the task force believes there is a need to explicitly assign responsibility for this coordination role to a WMD mission manager, under the Director of National Intelligence. The mission manager would be assigned responsibility to coordinate and integrate the Intelligence Community's efforts—including coordination with domestic law enforcement—with respect to terrorist acquisition and unconventional use of WMD.

In the past, the Intelligence Community has achieved success in such endeavors only when it recognized the imperative to mount a coordinated intelligence campaign. Thus, a comprehensive collection and analytic strategy for protecting the United States and its allies from covert or terrorist use of WMD is necessary.

These conclusions are not new. But in the view of the task force, the need to continue with the effective implementation of these and related recommendations from prior studies is imperative. The Intelligence Community has an excellent understanding of what needs to be done and, in the aggregate, the resources to do so. It needs, in our judgment, to advance with a greater sense of urgency, coordination, accountability, and leadership.

***Recommendation 1***

---

Recommendation #1 summarizes principal task force recommendations related to **Intelligence**.

The Under Secretary of Defense for Intelligence (USD [I]) and the Director of National Intelligence should implement and go beyond the recommendations of the 9/11 and WMD commissions in the following areas:

- Collection and analysis
  - Three recommendations under collection and analysis are classified.
  - Create on-going forum and tools to better understand potential adversaries and their motives, objectives, and values (USD [P])
- Federated data base, analysis, and exploitation built on MIDB concept (USD[I] and DNI, coordinate with all equities)
  - Single person responsible for development, including architecture (President's Program Manager for Information Sharing Environment)
  - Domestic and foreign intelligence
- Customer support and management (USD [I] and DNI)
  - Appoint a mission manager for terrorist pursuit of WMD
  - Revise security policies to rebalance need-to-share/protect

## **Chapter 5. Prevent Attack—The First Priority**

The first priority for the nation is to prevent an attack. Toward this end, we need to make the adversary's job as difficult and dangerous as possible and to minimize the likelihood that he will achieve his goals. This chapter covers three topics on which the task force concentrated in the area of prevention:

1. Deny weapon acquisition
2. Aggressive policies for attribution and response
3. Detection and interdiction in transit.

### **Deny Weapon Acquisition**

#### ***International***

The worst forms of WMD—nuclear and in some cases biological—would likely be acquired by terrorists from nation-state proliferators. So there is much to gain by reducing the stockpiles of these weapons worldwide and securing weapons materials. Material resources that should be protected include assembled nuclear weapons, special nuclear materials (SNM), and highly pathogenic biological agents. “Know how” is another key ingredient. Thus, tracking expertise in critical areas is important.

There is a lot of work going on in the nonproliferation arena: cooperative threat reduction programs, Nunn-Lugar, the Proliferation Security Initiative, special diplomatic efforts and other initiatives. These efforts should be increased to the highest extent possible. One way to extend these programs is to broaden the groups of countries involved. National efforts tend to have focused on Russia, but serious efforts should be underway to control proliferation in other countries. Certainly candidate nations of interest must be willing to cooperate, but it should be that willingness that limits our efforts—not funding or

initiative on the part of the United States. The objective should be to make acquiring weapons material as difficult as possible.

Furthermore, we should extend nonproliferation efforts beyond the traditional nuclear realm, to include the biological arena. International protection of those materials will always be imperfect, which results in an unwillingness in some quarters to continue the investment. The study concluded, however, that we, as a nation, should do everything possible to make access as difficult as possible, while at the same time recognizing that leakage will remain likely.

### ***Domestic***

While it is particularly important to prevent terrorist access to nuclear materials and the worst forms biological materials in the international arena, other forms of WMD (chemical, biological, radiological) are available in the United States. The infrastructure to develop these forms of WMD exists and is relatively accessible.

Why is it so easy to develop weapons inside the United States? First, the United States has the best infrastructure for scientific and technological development. It is difficult to find better, accessible equipment than in American universities. Toxic industrial chemicals can be used as weapons in situ, either at storage sites in populous areas or in transit. Materials to develop chemical weapons are generally available. Considerable radiological material is also accessible with limited security. The infrastructure to develop biological weapons is also accessible.

There is general recognition of this problem, but the action to secure these sources is not proceeding at a pace consistent with the deserved urgency. We must at least make it much more difficult for the adversary to use these sources and doing so is not difficult. If we were to take only one action toward prevention of a WMD attack, this is probably the one with the greatest payoff.

Until such time as we secure and protect all of these sources of materials within the United States, there is little reason for a terrorist to import these materials. Why take that added risk?



## ***Recommendation 2***

---

Recommendation #2 summarizes the actions recommended by the task force to **Deny Weapons Acquisition**.

- Strengthen and broaden international cooperative efforts in nonproliferation (DHS, Department of State [DOS], DNI)
  - Examples include treaties, PSI, Nunn-Lugar, special diplomatic efforts (such as Libya)
  - “Broaden” these efforts to include other countries, biological materials, “loose expertise”
- Remove easy access to WMD material in the United States, particularly radiological and chemical (DHS)
  - Increase physical security around sites near major population centers
  - Use transportation routes away from major population centers
  - Substitute materials to those that are less easily weaponized

## **Credible U.S. Policies**

The President has made clear the nation’s intent to punish anyone who uses WMD against the United States or its interests abroad or in any way aids and abets this use. The task force believes this to be the right policy. Terrorists must recognize that their values are at risk or their objectives will be denied. Supporters and suppliers, individuals, group, or nations must understand that their values are at risk. Those who do not provide adequate security for materials in their custody must also recognize the risks.

The most important foundations for this policy are attribution and retaliation.

### ***Attribution***

The credibility of declaratory policies to punish anyone who uses WMD against the U.S. or its interests abroad depends upon our ability

to attribute the source of the attack. Technical forensics, laboratory impurity analysis, and intelligence are combined to provide this capability and must be supported by databases and samples that can link findings to sources

For biological attacks, laboratory analyses can identify differences in genetic signatures and unique components of the culture medium that can point to the source of the organism. A major DHS program, the National Biodefense Analysis and Countermeasures Center, is constructing operational facilities that can perform the large volume of assays that would be required following a major attack and is pursuing underlying research to develop new assays and diagnostics.

Another pressing need is to accelerate development of international databases that assemble agent information from known repositories to provide clues regarding the source of an organism used in an attack. This effort faces both technical problems and policy issues.

For nuclear attacks, laboratory analyses that examine the residue from an explosion can yield insight regarding the design and source of the weapon. A program executed by the Defense Threat Reduction Agency (DTRA) has developed an initial sample collection capability and has reconstituted U.S. national laboratory capabilities first developed in the Cold War era to address this mission. Databases are also needed to link these results with a priori baseline knowledge. To ensure broad sharing of data that might contribute to attribution, prior coordination among the technical and intelligence communities regarding future collection priorities and joint activities following a nuclear burst is essential.

Attribution analyses also make use of data generated by national technical means, and the requirements on these capabilities must reflect the importance of that mission. The needs associated with nuclear attribution have received much less national attention and support than those for biological attribution. High level policy attention is needed to clarify interagency roles and responsibilities and to assure adequate support of the critical technical capabilities that provide the foundation for nuclear attribution.

In both the biological and nuclear cases, a broader assessment should be undertaken to address the likely effectiveness of technical attribution measures and the implications for national decision processes following an attack. In many cases, large uncertainties could remain even after the best available technical attribution analyses are completed. These inherent uncertainties should be identified and their impact on decision making understood. A net assessment of attribution capabilities for scenarios of interest, followed by exercises that consider the impact of attribution uncertainties, should be a part of the planning for U.S. response operations.

### ***Credible Response***

Response options are the other essential ingredient for effective deterrence policies. If a major WMD attack against U.S. interests occurred, and experts were rapidly able to determine who played what part in the attack, it is important that the United States be prepared to respond rapidly and appropriately. Furthermore, to be credible, the United States must advertise that these capabilities exist and that the nation is willing to use them. Credibility and a national willingness, together, will serve as a deterrent to many would-be attackers or supporters.

Now is the time to develop a spectrum of response options for all potential scenarios. The range of options available must include diplomatic, economic, and military responses. Until we can consider possible U.S. reactions in a disciplined and comprehensive process, the nation could be faced with ad hoc retaliation plans developed in the midst of chaos and urgent demands to “do something.”

The applicable cold war analog was the Joint Strategic Target Planning Staff and the Single Integrated Operational Plan (SIOP). These, of course, dealt with military options against fairly well defined and largely fixed targets. The current situation is much more complicated. However, it is important to apply the rigor and discipline of these cold war approaches and to understand the entire complex subject well in advance.

An important input to this type of planning is an understanding of the values and objectives of adversaries and others who support them.

This understanding is fairly straightforward for states but both complex and ambiguous for nonstate players. As discussed in chapter 4 (on intelligence), it is essential that we do everything possible to gain a detailed understanding of our potential adversaries at the religious, ethnic, tribal, group, organization, and even individual levels. Chapter 4 discusses creation of an institutional process to seek this understanding.

The National Security Council (NSC) must orchestrate this planning to consider and apply all of the organs of national power—economic, diplomatic, military, and other nonmilitary. This process should involve multinational partners where possible.

Developing military options need the rigor and discipline of the cold war SIOP process and should result in detailed plans for each option. The Under Secretary of Defense for Policy should lead the development of such a structure with the U.S. Strategic Command (STRATCOM) responsible for execution.

Planning cells must develop detailed response options to appropriately punish all participants to include perpetrators, organizers, enablers, hosts, and sympathizers. Options must account for the possible involvement of multiple organizations, countries, or regions. Alternatives should be identified and debated before an attack to provide the intellectual foundations for retaliation and deterrence and to allow for detailed planning. Furthermore, these plans should be subjected to simulations, gaming, exercises, and red teaming to gain insight into options and enhance effectiveness should execution be required.

### ***Recommendation 3***

---

Recommendation #3 summarizes the actions recommended by the task force to develop **Credible Policies for Attribution and Retaliation**.

- Continue to articulate clear policies for retaliation (Secretary of Defense, NSC, DOS, U.S. President)
- Improve support to these policies
  - Improve technical forensics capabilities as much as possible to improve attribution (USD [ATL])

- Task intelligence community to provide the corresponding data bases (USD [I])
- Develop and plan detailed retaliation options that could punish potential attackers and their supporters, suppliers (USD [P])
- Create a WMD retaliation-planning structure to develop military options (USD [P], STRATCOM) and the equivalent at the national level to bring to bear all organs of national power (NSC)

## **Detection and Interdiction in Transit**

Preventing terrorist acquisition and use of a nuclear weapon against a U.S. city must be one of the nation's highest security priorities. Extensive international efforts have been focused on the protection of the special nuclear materials critical to the manufacture of weapons and on the security of finished weapons, particularly in the United States and Russia. Programs initiated by the United States, such as the Cooperative Threat Reduction Program, and multilateral treaties have made significant contributions to the security of weapons and SNM worldwide.

However, their overall cost effectiveness and the level to which they can assure the security of foreign nuclear weapons and SNM have been controversial. The uncertainty in the performance of foreign safeguards, coupled with the lack of effective mitigation options against nuclear explosions, has caused a fresh look at systems that can intercept weapons or nuclear materials in transit.

Thus, this task force took a fresh look, in the broader context of the overall problem, at current national efforts with the goal of providing an updated assessment and recommendations concerning detection-based defenses of nuclear weapons in transit. Discussion of the current, planned, and recommended capabilities for interdiction and neutralization of nuclear materials is classified and covered in the classified version of this report.

## Chapter 6. Mitigation and Recovery

In case prevention fails, the next priority is to minimize the impact of attack on the United States. Mitigation and recovery is a national responsibility that involves many federal, state, and local organizations. This chapter addresses the national challenge first and then turns to DOD's responsibilities in mitigation and recovery.

### National Preparedness

Despite the many efforts and programs in progress, the nation is still poorly prepared to mitigate the impact of a WMD attack. Certainly the nation could survive all but the most devastating attacks, but likely experiencing many deaths and widespread destruction. In fact, the nation could recover from most of the less-violent scenarios evaluated by the task force during this study (described in chapter 2), even with little preparation—although the lack of preparation will equate to additional loss of lives. However, detonation of a stolen nuclear weapon of modest yield or a series of distributed biological attacks could well be devastating.

This lack of preparation appears to result from several key factors. First, the nature of our Constitution creates a division of responsibilities among local, state, regional, and federal governments that is compounded by fuzzy lines of demarcation. Preparation and implementation demand crisp, clear lines of authority and responsibility. Without unprecedented cooperation, planning, and exercising by all organizations and levels of government involved, including joint agreement subordinating responsibility and authority to a single chain of command, preparation and mitigation are likely to remain poor.

Second, the nation's preparedness appears to be lacking a sense of urgency—a need to remedy the nation's vulnerabilities appears largely missing except at the most senior levels of government. This sense is inconsistent with the potential devastation of the threat. Third, we, as a nation, tend to focus on or over emphasize the physical rather than psychological effects of an attack. But fear, panic, a loss of confidence in government, or erosion of national will could well result from a WMD

attack and may have been its ultimate goal. Thus, maintaining public support and understanding must be an element of national preparedness.

Reducing the nation's vulnerability to WMD requires a comprehensive approach across the spectrum from intelligence and prevention to mitigation, recovery, and response. No one or a few preparations are sufficient. A coherent, collaborative approach must overcome the challenges of coordinating among federal, state, and local governments and of sorting through myriad shared responsibilities. It must involve the private sector as well. Today's piecemeal, ad hoc approaches—that have become the norm—must be replaced by comprehensive, integrated, and systematic risk-based approaches.

The task force identified several high-payoff countermeasures among the many possibilities evaluated. First are planning, exercises, and command, control, and communications (C3)—relatively inexpensive and perhaps the highest payoff of all. These countermeasures must include fully interoperable communications and information systems across and among all organizations involved. Second is medical surge, which is widely recognized as a deficiency. We simply do not have the medical surge required to respond to a major WMD attack. Finally, while our analysis focused primarily on efforts common across the modalities, through this process emerged a number of modality-unique efforts that could significantly contribute to mitigation or recovery.

### ***Planning, Exercises, and Command, Control and Communications***

Planning, exercises, and C3—including shared situational awareness—are the foundation of effective mitigation and recovery. But truly effective action in this area seems to be limited. The Catastrophic Incident Supplement to the National Response Plan reflects thoughtful work. It is an excellent summary of all that needs to be done. But it falls short of being executable, depending on other agencies and state and local authorities to interpret and implement the document.

There must be one national plan with subordinate regional plans—all at sufficient level of detail that they can be executed. The regional plans must respond to single points of attack and the national plan

must seamlessly integrate all regional responses and responses to multiple attacks. All organizations and levels of government must “buy into” the plan.

Interoperable communications and information systems are essential, based on widely accepted standards, protocols, and data definitions. Fragmented systems should lead to an overall system design that provides both interoperability and robustness, with minimal replacement of existing hardware. In this design, it is important to consider the likelihood of adversary active disruption of communication and information systems as a part of a WMD attack.

Communications and information systems designed specifically and only for use following an attack, are likely to be ineffective. It is important to make these capabilities valuable to all users in the course of their regular and routine activities. If the systems are used every day, they will be well understood and useful in crisis.

The best of planning and C3 will be ineffective without regular exercises. Exercises will uncover deficiencies in the planning or C3. More importantly, they will create personal working relationships among the key players and decision makers. Under no circumstances should people “meet” for the first time in the chaos following an attack.

### ***Medical Surge***

A medical surge capability is critical. All high-casualty events will overwhelm nearby medical services. This outcome is probably the limiting factor in dealing with even moderate WMD attacks. The inability to provide medical services quickly will lead to unnecessary additional loss of life. It can also have a damaging impact on public perception of the government’s ability to function effectively and do its most basic job during a time of critical need. Thus the development of a national medical surge capability should be a very high priority.

There is widespread recognition that municipal and regional health care systems will be overwhelmed in even a minor WMD attack by casualties, the injured, and the “worried well.” An attack involving 10,000 victims with 10 times the number of “worried well” (a



conservative multiple based on experience) would require 20,000 trained medical personnel (as estimated by the Department of Homeland Security). The National Response Plan estimates that less than 4,500 trained medical personnel can be brought to bear within 72 hours. So the gap in capability is obvious.

Though the problem is widely recognized, progress to date has been slow. The Health and Human Services Cities Readiness Initiative has produced a single, 250-bed deployable hospital and has plans for three more without a firm schedule. The Office of the Surgeon General Medical Reserve Corps has 30,000 local volunteers from 237 communities, and is expected to double in size in the next year. In contrast, the Department of Defense has deployable assets—far larger than any domestic capability currently planned. These assets include expert medical personnel, infrastructure, personnel, and equipment from mobile Army surgical hospitals, combat support hospitals, and field hospitals.<sup>9</sup>

The task force believes that there are unexploited opportunities to enhance medical surge capabilities. In a crisis, the immediate need is to stabilize the victims until professional medical personnel can treat them. Some of this immediate need can be met by rudimentary first aid, inoculations, and the type of treatment offered by emergency medical technicians (EMTs).

One opportunity for creating a medical surge capability and expanding the nation's capability for a stabilizing strategy is to train the DOD civilian workforce of approximately 650,000 personnel in emergency medical training. We recommend a 2-week EMT course be mandatory for all DOD civilians, completed by 2007, at a cost of approximately \$650 per person.<sup>10</sup> This initial surge capability could be expanded to the rest of the federal work force, focusing on widely-dispersed populations such as the National Guard and U.S. Postal Service workers—both well represented throughout thousands of

---

9. DOD has 10s of combat support hospital units with 100s of beds each.

10. Annual training, of a shorter duration of perhaps a few days, will likely have to follow this initial training regime to maintain current capabilities.

communities across America.<sup>11</sup> This concept has precedence in CPR training that is provided throughout the federal workforce or, looking back to World War II, training for civil defense personnel.

In conjunction with this training, the task force recommends recruiting 10,000 medical doctor volunteers to serve as remote crisis responders. Further, telemedicine and automated medical data base networks should be extended to WMD response. Trained federal employees and remote physicians should participate in exercises using these databases and networks to test concepts of operations and readiness.

There are broader challenges involved in creating a medical surge capability, including the ability to get supplies and personnel to victims, transportation to the affected area, and communications between medical providers and facilities. The task force believes that planning and analysis, based on the reference scenarios, should be undertaken to understand in advance what problems are likely to arise in each circumstance. Gaming and simulation are needed to examine response plans and issues and to quantify necessary preparations.

### ***Modality-Unique Countermeasures***

The task force identified a number of modality-unique countermeasures where research and development efforts would have high leverage. These countermeasures include the following:

- Advanced medical countermeasures such as therapeutics, vaccines, diagnostics (biological)
- Advanced decontamination technology and techniques (each modality)
- Effective detect-to-warn or detect-to-treat capabilities (biological)
- Automated detection and air-flow control for facilities (chemical, biological, radiological)

---

11. The total federal civilian workforce comprises 2.7 million employees. DOD represents 24 percent of that workforce; the U.S. Postal Service, 30 percent; and the Department of Homeland Security, 5 percent. Source: Office of Personnel Management, November 2004.

In addition to these modality-unique research and development efforts, there are also a number of non-R&D areas. For example, mitigation of a nuclear attack could benefit significantly from “shelter-in-place” and well thought out evacuation strategies. The task force did not attempt to prioritize these near term, modality-unique countermeasures.

**Advanced Medical Countermeasures**

The biological terrorism threat is currently viewed as a long list of pathogens—bacterial and viral, contagious and not contagious. These pathogens are the “conventional threats.” This spectrum of potential threats poses serious problems today so there may be limited motivation for adversaries to seek more pernicious threats. However, the Soviet Union devoted a lot of effort to developing more “advanced threats” and it is reasonable to anticipate that some states (and possibly nonstate actors) are developing or will develop antibiotic resistant strains, genetically modified pathogens, or integrated “cocktails” of multiple pathogens. These threats are within the current state of the art and would complicate defense efforts immensely.

Today, countermeasures are available for only a limited set of the “conventional” biological threats. In order to cope with the wide range of threats and the potential for modified pathogens, the goal of some current advanced research is to create broad spectrum therapeutics, diagnostics, and vaccines. These would address the generic rather than the specific properties of pathogens and, if goals are achieved, would be effective against classes of pathogens rather than individual ones. They would provide countermeasures against the current (conventional) threats and against advanced threats. The applicability is illustrated in table 3.

**Table 3.** Applicability of Alternative Medical Countermeasures

Threat	Countermeasure	
	Specific	Generic
Conventional	X	X
Advanced		X

It is clear therefore, that such advanced research should be encouraged along with the more short-term efforts aimed at specific conventional threats.

There are currently three significant centers of investment for developing biological countermeasures. The National Institute of Allergy and Infectious Diseases, at the National Institutes of Health (NIH), is spending about \$1.5 billion per year. The Department of Defense's Office of the Assistant Secretary of Defense for Nuclear and Chemical and Biological Defense Programs (OASD [NCB]) and the Defense Advanced Research Projects Agency (DARPA) are each spending on the order of \$200 million per year. Each of these programs is addressing both specific and generic responses to biological attack. The task force recommends pursuing these efforts as vigorously as possible, to the level limited by good ideas. Whether there are enough good ideas to justify a major infusion of additional funds is a question beyond the scope of this study.

It is important that the separate development efforts be coordinated effectively, recognizing that each organization has strengths that can be brought to bear in developing advanced countermeasure capabilities. NIH operates largely with grants for research and with a peer review system that tends to make investment broad-based but conservative; however, there are obvious public health implications for developing broad-spectrum, generic countermeasures, which NIH can best exploit. The OASD (NCB) can create focused efforts and DARPA does and should concentrate on the high-risk, high-payoff areas.

Full success in the development of these advanced countermeasures, a long term goal, would negate the biological threat, both conventional and advanced and would have many positive effects on public health.

### **Advanced Decontamination**

Attack by any of the modalities (chemical, biological, radiological, or nuclear) is likely to leave a residual contamination of facilities and large areas. The contaminated areas can be unusable and uninhabitable for extended periods (years or decades in the case of radiological weapons) unless effective decontamination technology and techniques

are available and applied. Current capabilities for decontamination are limited, especially for radiological or biological residue.

An aggressive research and development program to develop these capabilities is warranted to mitigate the potential for huge economic costs.

### **Detect-to-Warn or Detect-to-Treat Biological Attack**

It would be highly desirable to detect and characterize a biological attack early enough to avoid human exposure. This capability is known as detect-to-warn (DTW). In principle, people could be moved out of the path of the biological agent or buildings could be sealed. However, current and currently projected technology is unlikely to provide this capability in open air—for example, upwind of a city. In the foreseeable future, DTW is likely to be useful only in constrained situations such as outlined in the next section.

However, early detection is still very important. Typically today, we anticipate that detection and characterization of a biological attack will result from clinical diagnosis of symptoms of infected people. Generally, the earlier the detection and treatment, the more likely the patient can be saved. Moving that detection timeline to the left is a goal of current research and development programs and should be funded to the limit of good ideas.

### **Automated Detection and Air-Flow Control**

The previous section discussed DTW and concluded that it was not applicable in open air. However, DTW can be applied to more constrained situations. For example, it could be applied to a modern building with sophisticated heating, ventilation, and air conditioning systems and generally well-controlled air intakes. Filters at the intakes can serve as “concentrators” of air samples and sensitive (that is, high false alarm) detectors placed there. These detectors then can be used to control air flow throughout the building—the “cost” of false alarms is generally tolerable with little impact on operations.

Another example, closer to the open air case, might be to protect a controlled area such as a military base. In this example a ring of detectors

at the protected perimeter could be set for high false alarms (and therefore high sensitivity). The false alarms in this case will impose a greater cost than the building air flow, but these may be tolerable. Examples of the reaction to an alarm might be to move personnel to sanctuaries (closed buildings), to use individual protection, or to administer medical prophylaxis.

#### ***Recommendation 4***

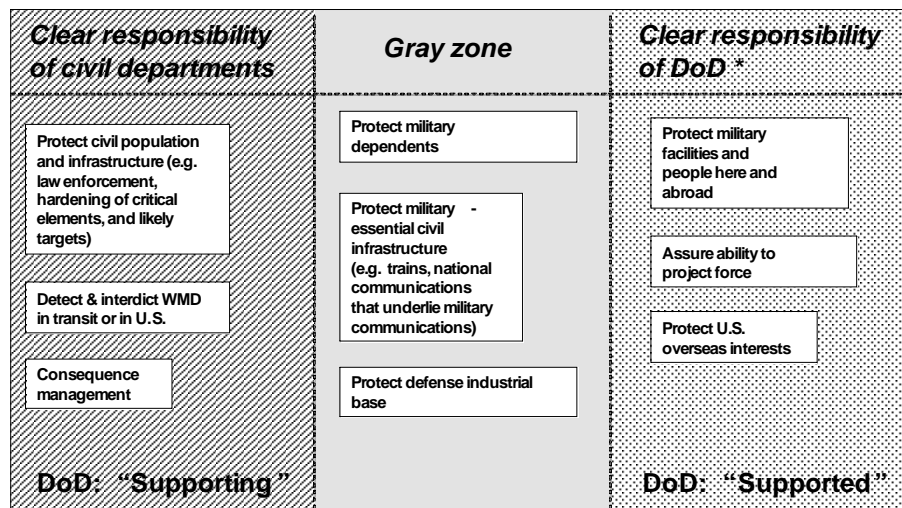
---

Recommendation #4 summarizes the most important actions recommended by the task force in **National Mitigation and Recovery**.

- Focus on the highest payoff mitigation and recovery efforts
  - Executable planning, exercises, and C3 (DHS)
  - Radically increased medical surge capabilities
    - EMT training for all DOD civilian employees (Assistant Secretary of Defense for Health Affairs and DHS for non-DOD)
    - Develop and implement telemedicine support for EMTs and medical doctors (DHS)
    - Initiate detailed analysis of surge issues (DHS)
  - Research and development on specific, modality-unique, high-payoff countermeasures (Director, Defense Research and Engineering; DHS)
    - Advanced medical countermeasures (diagnostics, therapeutics, vaccines) [bio]
    - Advanced decontamination technology and techniques [each]
    - Effective detect-to-warn or detect-to-treat [bio]
    - Automated detection and air-flow control for facilities [chemical, biological, radiological]
- Publicly articulate the situation regarding terrorist use of WMD clearly and honestly, with realistic assessment and guidance, to gain and maintain public support and to increase the sense of urgency (Secretary of Defense, DHS, U.S. President)

## DOD Responsibilities

As shown in figure 3, responsibilities for mitigation and recovery fall on both civil departments and the Department of Defense. The left side of the chart lists responsibilities that fall clearly in the purview of civilian departments and where DOD may play a supporting role. On the right are areas of clear responsibility for DOD. These areas include protecting its forces at home and abroad and assuring the ability to project force. But it is important to remember that DOD depends heavily on civil infrastructure to accomplish its mission—thus creating a gray zone. It is the view of the task force that DOD should lean into that gray zone—but we recognize that this is a notion subject to debate.



\* Strategy for Homeland Defense & Civil Support: "DOD is lead in force protection including family members, resources, facilities, and critical information." Includes mission assurance. Page 18 defines critical infrastructure.

**Figure 3.** Responsibilities in Mitigation and Recovery

In addition to clear responsibilities in mitigation and recovery, DOD has unique capabilities that could contribute to the national architecture. Examples of such capabilities include the following::

- Unparalleled capabilities for planning, exercising, and conducting that mission
- Extensive experience with C3 and information systems operating in adversarial conditions
- Ability to provide the extensive resources and discipline that would be required in the event of a truly catastrophic attack
- Proven technologies and response assets that could be effectively used by civilian responders in diverse domestic scenarios

The task force believes that the nation should draw on DOD's expertise and experience in these areas, in advance of an attack, to stimulate the environment and help lead and train a national capability while, at the same time, supporting DOD's accomplishment of its own mission. We are therefore recommending two areas that would serve as a useful beginning—to help create both a set of capabilities and a sense of urgency to motivate further action. These two initial actions are: 1) base protection and 2) planning for a truly catastrophic attack. Each will be discussed in turn below.

### ***Base Protection Pilot Program***

Today, base protection is being addressed in a number of limited pilot programs. Some of the programs underway include portal monitors created under the Unconventional Nuclear Warfare Defense Program, the Joint Service Installation Pilot Project, BioNet, and Guardian. Although built on the experiences of prior programs, each of these initiatives was undertaken relatively independently. The more recent and most comprehensive is Guardian. Originally intended to use available technology to provide base-protection capabilities to 200 DOD facilities, it was constrained to work entirely within the base perimeters, an overly restrictive concept. Guardian provides a level of off-the-shelf technology for the foundation of base protection.



However, the task force concluded that base protection and local community protection need to be addressed in a more comprehensive manner—an approach based on a systematic look across all modalities that is informed by risk assessment and implemented with standards and best practices. Base and local community protection are inevitably connected because of the need to protect military family members living off base and the essential dependence of the base on local infrastructure. In addition, it is clear that some measures of base protection require a “defended perimeter” which may well be outside the base confines and the authority of DOD. Thus, without the complete cooperation of the local authorities, base protection is likely to be ineffective.

The task force recommends that DOD initiate a base protection pilot program, led by the Defense Threat Reduction Agency, with support from U.S. Northern Command (NORTHCOM). This program would focus on reducing WMD vulnerability in DOD facilities and on establishing interoperability between civil and military C3 in those communities. The recommended program would provide the basis for a comprehensive base protection program that can be extended throughout DOD facilities and, through a partnership with DHS, serve as a model for civilian communities as well.

Specifically, the task force recommends that a careful analysis identify four bases to participate in the pilot—three in the continental United States and one overseas. The selection should be based on a number of criteria, but the most important is that the bases have a strong presence in the local community. Some of the candidate bases and regions discussed included the National Capitol Region and Andrews AFB; Fayetteville, North Carolina and Fort Bragg; Tampa, Florida and McDill AFB; and San Diego, California and the Coronado Naval facilities. There are certainly other possibilities and the task force came to no conclusion on which were preferable.

Each of the pilots should be designed carefully with a comprehensive, integrated, systematic approach for defense against WMD attack. The first selected base should be assigned to a small team (6–12 members plus support) with expertise in system design and engineering. The most

logical source of that team appears to be DTRA since that organization has the experience in all the relevant disciplines.

The team would carefully examine the base and environs and the potential risks to population, infrastructure, and facilities. Based on this assessment, the team would design the elements of the protection system and, after appropriate approval, guide the implementation. Prior to implementation, an independent red team should be called on to critique the design in depth. To the extent possible, the design should build on the lessons and experiences of previous programs mentioned above but should not be constrained by them in any way.

Table 4 identifies some (by no means all) of the many factors that need to be considered in the design of protective measures appropriate to each facility. These factors pertain both to the conduct of the site's military mission and its links to the local community.

**Table 4.** Example Elements of a Pilot Program in Base Protection

Base Concerns	Links to the Civilian Community
Define protected perimeter	Public education and information
Monitor principal portals, external choke points (NR)	Medical surge plans
Provide for automated detection and characterization of attack (BC)	Evacuation, sanctuary, and quarantine plans
Protecting water, sewer, power, food supplies, etc	Protection of critical infrastructure
Secure hazardous material in region (CR)	Support to local community
Cameras to detect suspicious activity	Sanctuary bastions in situ
Airspace monitor	C3; situation awareness
Automated detection and air-flow control systems for selected facilities (BC)	Information access as needed
Staging areas	Development of large-scale gaming to train and exercise

After the first pilot is underway, the team would design base protection systems for the other three bases in sequence, taking advantage of the experience gained in each case. This sequential approach would be lengthy in duration; forming four design teams to operate in parallel could be considered to implement the program more rapidly.

An essential element of the process is design critique conducted by red teams. Red teams should also “attack” the protected base and city realistically to verify not only that the capabilities implemented are appropriate and adequate but that the people using them have been trained to make them effective.

The task force believes that DOD should solicit participation from the Department of Homeland Security in conducting these pilots. The role for DHS is to apply what is learned from the pilots to civil protection systems and to propagate these systems across the country as appropriate. As well, DOD’s responsibility will be to extend the capabilities to other bases as the concepts are effectively demonstrated.

One additional element that is important to the pilot programs is to design, develop, and implement a prototype C3 capability that is robust and includes situational awareness. This prototype system should provide for each of the four pilot installations and link these to each other and to appropriate state and national elements. These C3 and information systems must be designed for every day use, but have properties that will withstand an attack—including cyber attacks. DOD has unique experience in the design and operation of such systems under adversarial conditions and should take the lead. The task force recommends that DOD approach DHS and negotiate to take the lead in developing and prototyping this system for use as the national homeland security system.

In summary, the concept is to take on several sites of manageable size as a learning tool, develop a comprehensive plan for WMD defense that includes particular emphasis on situation awareness and C3, and then extend this to sites throughout DOD and, eventually, the civilian community. The task force recognizes that transfer to civilian cities is not automatic, as a military base is certainly a more protected, “hardened” environment as compared to the softer target of civilian

cities. This concern is at least partially mitigated by inclusion of the surrounding civil community in the integrated design of the whole. In any case, the task force believes that relevant applications exist and taking the first step of conducting a comprehensive design in a few areas will be instructive for national planning.

### ***Planning for a Catastrophe***

The task force notion of mitigation and recovery planning for a catastrophic attack is intended to push the nation's thinking beyond that of September 11—a scale of attack that many viewed at the time, and still do so today, as catastrophic. But the concept here is far beyond that case, intending to focus on planning for an event such as a large-scale nuclear attack, a campaign of biological attacks that roll across the nation, or an attack that combines multiple modalities. Our definition of “truly catastrophic” is that the magnitude of the event completely overwhelms state, local, and federal civil capabilities and, in fact, that these capabilities may be effectively eliminated, at least in the region affected.

Management of the consequences of such an attack cannot tolerate divided responsibilities or ad hoc response without greatly increased loss of life and panic. There must be clear command and control and clear lines of communication. It must be recognized that, under such circumstances, the President may decide to call on DOD to take control of the affected region. This decision obviously would apply only in extreme situations. However, DOD should be prepared to provide all needed capabilities to surviving civil authorities of a region.

The time for detailed planning is now. Doing so ad hoc, in the chaos of attack, will almost certainly cost more lives and result in public loss of confidence and panic. The task force likens this type of planning to classic “war planning” in which DOD is so effective. Catastrophe planning deserves the same level of attention and detail. It must include plans for providing resources, medical surge, logistics, forces to maintain order, burial capabilities, and other considerations specified in the National Response Plan Catastrophic Incident Supplement. The plans should incorporate commercial support such as the Civil Reserve Air Fleet and its application to trucks, rail, and buses; prearranged and organized medical surge; and standing logistics contracts.

The task force recommends that NORTHCOM take the lead in developing these detailed plans—a major undertaking since each major metropolitan area is different and will require a specific plan. In developing these plans, NORTHCOM should coordinate with DHS and the National Security Council because of the obvious collaboration that will be required should DOD be called upon to provide full support of an attacked region for mitigation and recovery operations.

### ***Recommendation 5***

---

Recommendation #5 summarizes the actions specifically recommended by the task force for execution of **DOD Responsibilities in Mitigation and Recovery**.

The Department of Defense should accelerate action on its responsibilities in mitigation and recovery and, at the same time, lead the way for the civil community (Secretary of Defense):

- Establish a comprehensive pilot program to protect four military installations (DTRA with NORTHCOM)
  - Build on prior pilot programs
- Design and develop robust situation awareness and C3 (USD [AT&L] or Assistant Secretary of Defense for Networks and Information Integration, with primary user NORTHCOM/National Guard)
  - Negotiate with DHS to lead in development, prototyping of national C3
- Develop detailed plans (modeled after “war plans” for execution of DOD responsibilities if directed to provide full support of an attacked region for mitigation and recovery operations (NORTHCOM)

## Chapter 7. Managing the Enterprise

Creating an effective counter-WMD effort will require coordination and integration of activities across many organizations, including federal, state, and local government agencies, as well as many private sector organizations—notably those involved in areas of U.S. critical infrastructure. This coordination and integration will require a new organizational approach with requisite staff and budget resources.

**We believe that one single individual must be charged with this responsibility—someone who is positioned to see the whole WMD picture. Today, no one has that visibility.** This individual should report to the Secretary of Homeland Security and should receive guidance and oversight from a subcommittee of the U.S. Homeland Security Council with appropriate representation from government and industry. Furthermore, every six months this individual should provide to the President an assessment of the nation's capabilities and readiness to address the threats from WMD.

To aid in the development of these regular assessments, we believe that cost and performance metrics—readiness metrics—must be established to help prioritize activities and measure progress. Regular simulation exercises with trained red teams should be performed in order to test U.S. readiness and to collect data from which these metrics can be evaluated.

This task requires broad visibility into programs and budgets with metrics and tools that link investment and capability. To this end, we support the efforts of the Congress and the administration to improve the efficiency of our national investments in information technology. The leadership of the Office of Management and Budget, the Federal Chief Information Officers Council, and the Office of the Assistant Secretary of Defense for Networks and Information Infrastructure in developing enterprise technology and processes for integrating information systems will help provide the necessary visibility into programs and budgets and in collecting and evaluating the readiness

metrics described below. We recommend that current technology and processes be expanded specifically to address the WMD threats.

## **DOD Organization**

Assigning to U.S. Strategic Command the mission of combating WMD has created a military advocate that will drive WMD planning in the combatant commands, the military services, and the Joint Staff. This assignment was a positive step toward coordinating DOD activities. However, within the Office of the Secretary of Defense (OSD), there is no single individual or organization below the level of the Deputy Secretary of Defense that sees the WMD problem as a whole.

The OSD organization for combating WMD has evolved on an ad hoc basis for 15 years. There is no *de facto* clear line of authority and responsibility. Roles are distributed across many parts of the organization to include the assistant secretaries for homeland defense, health affairs, special operations and low intensity conflict, and the assistant to the secretary for nuclear, chemical, and biological matters. To address this situation, we recommend that a single individual within OSD have the responsibility, with appropriate staff and budget authority, to provide the necessary leadership in areas of DOD responsibility in addressing the WMD threats.

Currently, DTRA is the single organization in DOD with a coherent mission in WMD across all modalities—and it is important to maintain that cohesiveness. While DOD undergoes many organizational changes to meet evolving threats and missions, we believe that DTRA has an enduring mission for WMD issues and should continue as a unified DOD agency.

## **Metrics: Readiness**

The task force is concerned that top management in the Department of Defense may be led to believe that there is more capability than really exists. While there are many ongoing efforts and investments, many power point presentations and “strategies,” all too frequently it is assumed that investments will in fact lead to planned capabilities.

However, developing a capability requires active management based on well-defined performance metrics—in other words a “readiness” system for reducing the vulnerability to WMD.

The analysis described in chapter 2, and used during the course of this study to identify high-payoff recommendations, done more completely and supported by an on-going red team activity, could provide a useful basis for readiness assessment across the DOD or national enterprise. The level of effort contributing to the analysis for this study was about two man-months of effort. Accordingly, we believe that the necessary readiness assessments can be accomplished with a modest and highly cost-effective investment. Whether the methods used in this study are adopted by the department or others are used, the task force recommends that the DHS and DOD develop an enterprise readiness process and system that can provide assessment of each of the major capabilities required to reduce U.S. vulnerability to WMD and to overall national preparedness.

To begin, we recommend creating a small cell in the Office of the Secretary of Defense, Program Analysis and Evaluation (OSD [PA&E]) to provide an objective review and analysis (including metrics) of government-wide efforts to reduce vulnerability to WMD. PA&E has the capability and the culture to conduct such assessments and would therefore be an appropriate organization to initially take on this task. It is equally important to create red teams to challenge the assessments. This exercise should be repeated annually within DOD so that the Secretary of Defense is regularly apprised of DOD activities and progress in this area. Ultimately, we believe that a small group needs to be chartered and empowered to conduct these assessments on a national level, reporting to the Secretary of Homeland Security or the White House.



***Recommendation 6***

---

Recommendation #6 summarizes suggested action in **Managing the Enterprise** regarding WMD.

Develop an enterprise readiness process and system that can provide assessment of each of the major capabilities required to reduce U.S. vulnerability to WMD, and overall national preparedness

- Create a small group chartered and empowered to do this, reporting to Secretary of Homeland Security or the White House (DHS)
- Initially create a special cell in OSD (PA&E) to provide an objective review and analysis (including metrics) of government-wide efforts to reduce vulnerability to WMD (OSD [PA&E])
- Create red teams to challenge the assessments

## **Chapter 8. Summary of Recommendations**

In summary, the task force has identified six high-payoff recommendations that will greatly reduce U.S. vulnerabilities to weapons of mass destruction. At the highest level those recommendations are as follows:

- Improve intelligence collection, analysis, and management in ways specific to unique aspects of the WMD threat
- Deny weapon acquisition to the adversary through international cooperative efforts and increased emphasis on tracking and protecting hazardous materials in the United States
- Articulate aggressive policies regarding the use of WMD, backed by improved attribution and response capabilities
- Improve national mitigation and recovery capabilities by focusing on the highest payoff efforts—planning, exercising, C3, and medical surge
- In DOD, establish pilot programs in base protection and undertake planning for catastrophe response
- Develop and use readiness metrics as a basis for assessing major capabilities and national preparedness to reduce U.S. vulnerability to WMD

### **Investment in Reducing the Threat**

To put the investments needed to implement these recommendations in some context, the task force first gathered data on the current federal investments in reducing the threat from WMD. This estimate was not straightforward to create, as most federal expenditures are not described in directly relevant terms. Even the simple availability of data varies widely across the federal government.

To establish some consistency, fiscal year 2005 was chosen as a baseline, as it is the most recent year for which nearly complete data were available. For some of the funding within the Department of Homeland Security, data from fiscal year 2004 was used. The reason for this adjustment, the sources for all the data, and the details of how the funding was then categorized, are described in the investment chapter of volume 2.

Significant uncertainties still remain in these estimates of federal funding. Some activities that are relevant to reducing the threat from WMD are but a small part of comparatively very large operating accounts. The use by customs inspectors of radiation detectors as part of their general inspection activity is one such example. The estimates here do not attempt to reflect the funding for such activities. Additionally, many activities are imperfectly described in the available sources, so errors in interpreting the purpose of some activities is likely. Some agencies with small investments were not included as the task force focused on understanding the larger efforts. Nonetheless, the task force believes that the general pattern and scale of the investments described here fairly represents the total federal investments.

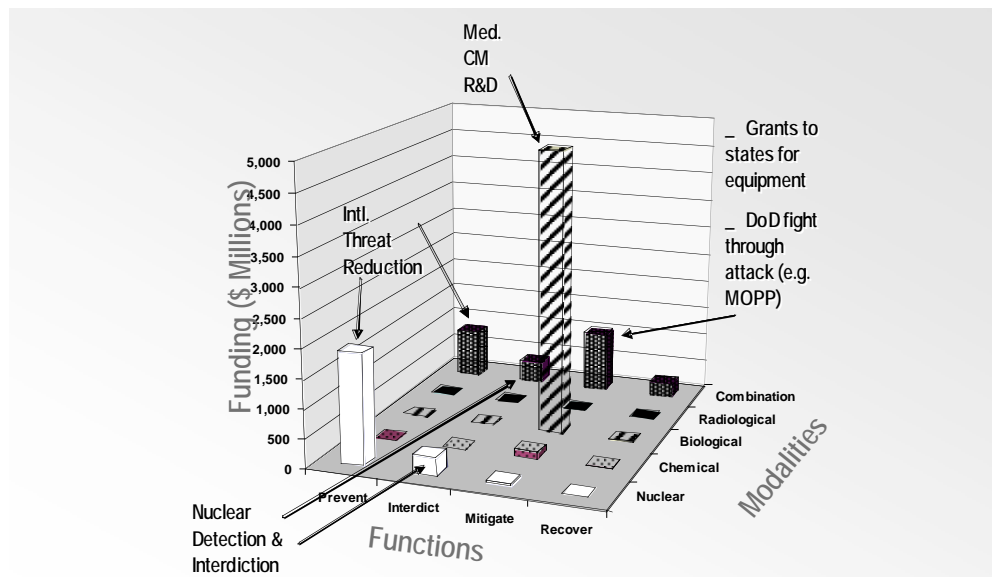
The federal investment examined and categorized by the task force totaled \$10.5 billion. The funding came from five departments, as shown in table 5. These data do not include funding for intelligence activities.

**Table 5.** Federal Investment in WMD-Related Activities

	<b>Billion</b>
Department of Defense	3.1
Department of Homeland Security	1.3
Department of Health and Human Services	4.1
Department of Energy	1.9
Department of State	0.1

For each agency and activity, the task force used available information to categorize the funding as some combination of function and modality. Results of this categorization are shown in figure 4.

The pattern of federal investment seen in the figure has several obvious features. First, investments tend to concentrate in just a few areas: mitigating biological attacks through either research and development for medical countermeasures or grants through the states for improving medical preparedness; preventing the acquisition of nuclear weapons through international threat reduction programs, largely in the former Soviet Union; mitigating a variety of attacks through investments such as personal protective suits for the military and first-responder equipment funded by grants; and interdicting nuclear attacks through improved detection. These areas of emphasis are not surprising.



**Figure 4.** Investment in Reducing the WMD Threat, Fiscal Year 2005

Second, there are a large number of areas with very little investment. Some of these areas—such as prevention of radiological attacks (through securing sources), forensics after an attack of any modality, and recovery—suggest to the task force missed opportunities.

Finally, political attention is currently focused on increasing funding for one of the already emphasized areas, nuclear detection and interdiction within the Domestic Nuclear Detection Office in DHS—an investment we question, and which was discussed earlier in this report.

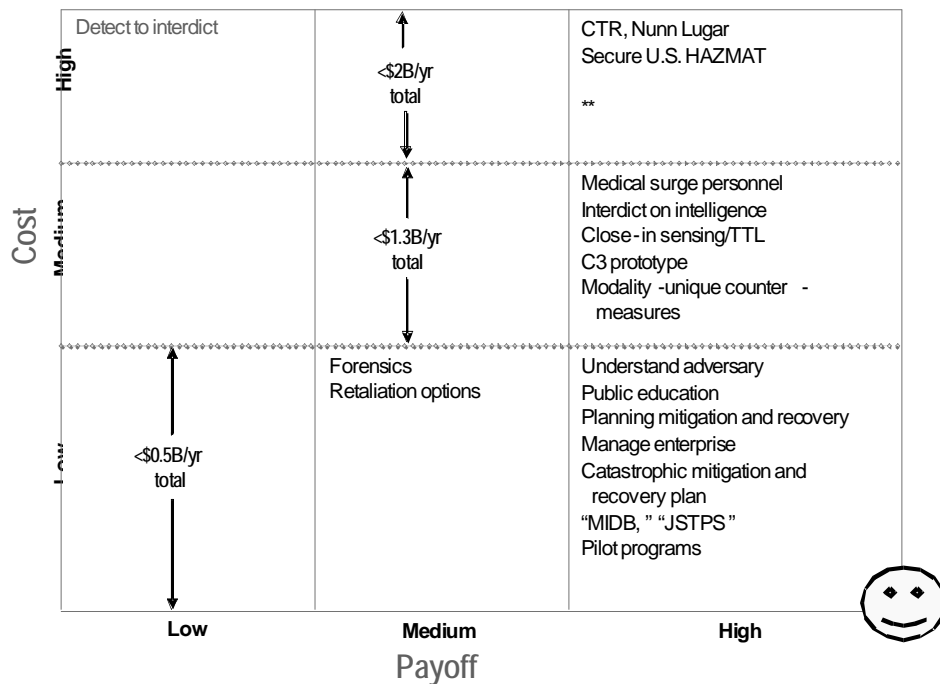
With this pattern of existing federal investment for context, we now turn to the additional investments required to implement the task force recommendations. Table 6 shows the estimates, made by the task force, this additional investment. These estimates, made consciously conservative, total only \$4.0 billion per year—a manageable level of additional investment for the federal government

**Table 6.** Additional Cost of Task Force Recommendations

<b>Recommendation</b>	<b>~ Billion Dollars Per Year</b>
1. Improve intelligence in specific ways	0.7
2. Deny weapon acquisition	2.0
3. Improve support to aggressive policies	0.2
4. Enhance national mitigation and recovery	0.6
5. Establish DOD pilot programs and catastrophic planning	0.3
6. Develop and use readiness metrics	~0.0
<b>TOTAL</b>	<b>~\$4.0 B</b>

To generate the cost estimates presented in table 6, the task force assessed the requirements for the detailed recommendations presented in the earlier chapters of this report and used the expert judgment of its members to generate first-order estimates of the annual, recurring costs associated with implementation. In all cases, we rounded up to add some measure of conservatism to the estimates, although it is important

to caveat the assumption that the programs be well managed and well run. Using criteria of less than \$100 million per year as low cost, \$100 to \$500 million per year as medium, and greater than \$500 million per year as high, the individual recommendations were arrayed on a cost/payoff grid as shown in figure 5. The payoff rating is a qualitative effectiveness assessment that reflects the task force's analyses of its detailed recommendations within the six areas identified in table 6.



\*\* Note: Full implementation of mitigation and recovery plans and National C3 in not included.

**Figure 5.** Opportunities versus Investment

Examining the six broad recommendation areas and the required investments produces an important observation. Many of the individual recommendations offer very high payoff at relatively low cost, as the number of actions in the bottom right box of figure 5 illustrates. Yet, despite the high payoff and low cost, the task force found no evidence that these efforts are being aggressively pursued. Consequently, the task



## Bottom Line

**Effective implementation of all six recommendations would, in our assessment, significantly reduce the impact of most forms of WMD**—chemical, biological, radiological—as represented by the DHS scenarios evaluated in this study. A nuclear attack is in a class by itself and remains a serious threat, depending heavily on prevention. Campaign attacks also remain potentially catastrophic due to the potential for widespread destruction. To implement these initial recommendations would require about \$4 billion of additional investment annually. It is an investment that the country must be willing to make.



## **Appendix A. Terms of Reference**



ACQUISITION,  
TECHNOLOGY  
AND LOGISTICS

THE UNDER SECRETARY OF DEFENSE  
3010 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-3010

JAN 10 2005

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference -- Defense Science Board 2005 Summer Study on Reducing Vulnerabilities to Weapons of Mass Destruction

You are requested to form a Defense Science Board (DSB) Summer Study on Reducing Vulnerabilities to Weapons of Mass Destruction (WMD). The 2005 Summer Study should concentrate on a State's clandestine employment of WMD or the use of such capability by a terrorist.

Much of the dialogue and activity concerning the reduction of vulnerability to WMD effects focus on limited aspects (e.g. detection, defeat, consequence management) of a single modality – whether it be biological, chemical, or nuclear/radiological. While single modality approaches are useful, they do not lend themselves to the development of an integrated system. In addition, by focusing on separate aspects of the overall defense outside of an end-to-end architecture, the proper balance of requirements and resource allocations across architectural components cannot and has not been made. WMD defense must be able to handle the different modalities singularly or in combination across the spectrum of WMD from preemption to consequence management. The current segmented approach begs the question whether coverage gaps exist in this spectrum and if there are misplaced priorities in the programs designed to protect the US from WMD attacks. In addition, the current approach does not provide any mechanism to rationalize the effort and likely lends itself to suboptimal resource allocation, especially with the “sharp” lines being drawn between national security and homeland security.

The Summer Study should develop national enterprise architecture to reduce vulnerabilities to WMD. The architecture should identify those areas where integration across modalities would pay off, as well as the issues that are uniquely tied to a single modality. Ideally, the architecture should be able to adapt to shifting priorities in WMD defense which may arise from new intelligence or other sources and adapt to different generations of WMD defensive systems which will probably be procured under a spiral development model. An integrated WMD system would be able to assess from end to end the state of affairs in WMD defense.

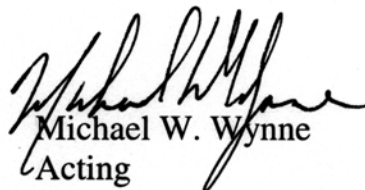
The Summer Study should develop an enterprise architecture which covers the entire range of U.S. government capabilities and responsibilities. Using this architecture, the Summer Study should assess:



- Which WMD modalities are the U.S. most vulnerable to? What factors might change the vulnerability over time?
- Functional "requirements" of envisioned WMD defense capability – quantified to maximum extent possible.
- Develop an overall architecture including distributed characteristics, interfaces, and commonalities.
- Examine current and planned U.S. investments in WMD defense. Recommend a prioritized and comprehensive investment strategy.
- Which organizational construct best serves the implementation of an integrated WMD defense, both nationally and within DoD?

The Summer Study will be co-sponsored by me as the acting USD(AT&L) and the Assistant to the Secretary of Defense (Nuclear, Chemical and Biological Defense Programs). Mr. Larry Lynn and Mr. Bob Nesbit will serve as chairmen of the Summer Study. Mr. Mike Evenson, DTRA, will serve as Executive Secretary. LTC Scott Dolgoff, USA will serve as the Defense Science Board Secretariat representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of section 208 of Title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.

  
Michael W. Wynne  
Acting

## Appendix B. Task Force Membership

### CHAIRMEN

Name	Affiliation
Mr. Larry Lynn	Private Consultant
Mr. Bob Nesbit	MITRE

### STEERING GROUP

Mr. Irv Blickstein	RAND
Dr. Regina Dugan	Private Consultant
Dr. Matt Ganz	HRL Laboratories, LLC
Dr. William Graham	National Security Research, Inc.
Dr. Mim John	Sandia National Laboratories
Mr. John Lauder	Areté Associates
Dr. Ann Skalka	Fox Chase Cancer Center
Mr. Bob Stein	Private Consultant
Dr. Michael Vlahos	John Hopkins University, Applied Physics Laboratory

### TASK FORCE MEMBERS

Dr. Steve Balut	Institute for Defense Analyses
Dr. James Bonomo	RAND
Dr. Bob Brammer	Northrop Grumman
Dr. Larry Brandt	Sandia National Laboratories
Mr. Peter Breier	National Security Research, Inc.
Dr. Julie Casani	Department of Health, State of Maryland
Dr. Delores Etter	U.S. Naval Academy
Dr. Craig Fields	Private Consultant
Gen John Gordon, USAF (Ret)	Private Consultant
Mr. Richard Haver	Northrop Grumman
Dr. Robert Hermann	Private Consultant
Maj Gen Ken Isarel, USAF (Ret)	Lockheed Martin

Mr. Alan Marcus	CNA
Dr. Joe Markowitz	Private Consultant
Dr. Susan Marquis	LMI
Dr. Thom Mayer	Best Practices, Inc.
ADM Donald Pilling, USN (Ret)	LMI
Dr. Brad Roberts	Institute for Defense Analyses
Mr. Jim Shields	Draper Laboratory
Mr. Vince Vitto	Draper Laboratory
Mr. Mark Wagner	Batelle
Mr. Steve Weiner	MIT Lincoln Laboratory
Dr. Obaid Younossi	RAND

**EXECUTIVE SECRETARY**

Mr. Mike Evenson	Defense Threat Reduction Agency
------------------	---------------------------------

**DSB REPRESENTATIVE**

LTC Scott Dolgoff, USA	Defense Science Board
------------------------	-----------------------

**GOVERNMENT ADVISORS**

Col Don Ahern	NGB J-5
Dr. Parney Albright	Department of Homeland Security, Science and Technology, Programs
Ms. Lisa Bronson	Office of the Deputy Under Secretary of Defense (Technology Security Policy & Counterproliferation)
Col Mason Carpenter	USAF, J-5
Dr. Michael Carter	Department of Homeland Security
Dr. David Cooper	Office of the Secretary of Defense, ISP/NPP
CAPT John Fraiser	U.S. Special Operations Command
Dr. Richard Gault	Defense Intelligence Agency
Ms. Laura Gross	Office of the Under Secretary of Defense for Policy, International Security Policy
Dr. Clifford Hansen	U.S. Northern Command
LTC Mark Holloway	U.S. Northern Command
LTC Thomas Hook	NGB J-3

Mr. Wade Ishimoto	Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict
Dr. Randy Long	Department of Homeland Security
COL Richard Marchant	Office of Force Transformation
Dr. Maureen McCarthy	Department of Homeland Security, Science and Technology, Office of Research and Development
Col Mike McGauvran	U.S. Strategic Command
Col Don McGonigle	Office of the Assistant Secretary of Defense for International Security Policy
Ms. Cathy Montie	Defense Threat Reduction Agency
Dr. Maruice Mizrahi	Office of the Secretary of Defense, Program Analysis and Evaluation
Mr. Thomas Pagan	U.S. Army Space and Missile Defense Command
Dr. Lisa Rotz	Center for Disease Control
Dr. Scott Steele	Federal Bureau of Investigation
LTC Robert vonTersch, USA	Office of the Assistant Secretary of Defense for Health Affairs
Mr. Paul Wolfe	Defense Intelligence Agency
Mr. John Wood	Office of the Assistant Secretary of Defense for Homeland Defense

**STAFF**

Ms. Barbara Bicksler	Strategic Analysis, Inc.
Ms. Julie Evans	Strategic Analysis, Inc.
Ms. Amy Cauffman	Strategic Analysis, Inc.

## Appendix C. Presentations to the Task Force

Name	Topic
------	-------

### JANUARY 31 – FEBRUARY 1, 2005

Dr. Brad Roberts <i>Institute for Defense Analyses</i>	DOD's Implementation of the National Strategy to Combat WMD: A Progress Report on Work by a Panel of the Threat Reduction Advisory Committee
---	--

### MARCH 8–9, 2005

Col Mason Carpenter <i>Joint Staff, J-5</i>	Joint Staff Combating WMD Efforts
Dr. Len Connell <i>Sandia National Laboratories</i>	Analysis of the RDD Threat: A Risk-Based Approach
Dr. Randy Long <i>Department of Homeland Security</i>	Chemical Countermeasures Science and Technology Program
Dr. Maurice Mizrahi <i>Office of the Secretary of Defense, Program Analysis and Evaluation</i>	Combating Weapons of Mass Destruction: An Investment Strategy
Dr. Vayl Oxford <i>Department of Homeland Security</i>	Overview of the Domestic Nuclear Detection Office
Mr. Scott Rowell and LtCol Don Leathem <i>Office of the Assistant Secretary of Defense for Homeland Defense</i>	DOD's Strategy for Homeland Defense and Civil Support
Dr. John Vitko <i>Department of Homeland Security</i>	An Overview of the Biodefense RDT&E

### APRIL 4–5, 2005

Bill Bryan <i>Director, Critical Infrastructure Protection</i>	Defense Critical Infrastructure Program (DCIP)
Dr. Julie Casani, <i>Director, Office of Public Health Preparedness and Response, State of Maryland</i>	Public Health Preparedness
Dr. David Cullen <i>Office of the Under Secretary of Defense for Policy, Chemical and Biological Defense</i>	Chemical Biological Defense Program and Biological Standoff Detection Program

Dr. Thom Mayer, <i>Best Practices, Inc.</i> Dr. Dan Hanfling, <i>Medical Director for Disaster Management, Inova</i>	Healthcare Facility Preparedness for WMD Response: The Current State of Affairs
<i>Various Intelligence Agencies</i>	Status of Terrorist Threat

**MAY 3–4, 2005**

Dr. Seth Carus <i>Center for the Study of WMD, National Defense University</i>	What are Weapons of Mass Destruction? Historical and Legal Perspectives
Ms. Ellen Embrey <i>Deputy Assistant Secretary of Defense for Force Health Protection and Readiness</i>	Medical Emergency Preparedness Programs and Initiatives: Overview and Status Update
Dr. Dale Klein <i>Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs</i>	Department of Defense: Combating Weapons of Mass Destruction
Mr. Brad Roberts <i>Institute for Defense Analyses</i>	Calibrating Adversary Intent: State and Non-State
Ms. Nancy Suski <i>Department of Homeland Security</i>	National Incident Management System and National Response Plan
<i>Various Intelligence Agencies</i>	Counterproliferation and Counterterrorism

**JUNE 1–2, 2005**

Dr. Jay Albanese <i>Chief, International Center, National Institute of Justice</i>	Criminal Motivation and Crime Prevention
Mr. Rudy Cohen and LtCol Perry Helton	TOPOFF III After Action Comments
Mr. Mike Evenson <i>Defense Threat Reduction Agency</i>	DTRA Programs Related to WMD Defense
Anthony S. Fauci, MD <i>Director, National Institute of Allergy and Infectious Diseases, National Institutes of Health</i>	NIH Biodefense Research: Progress and Priorities
Col Joseph Palma, USAF, MD <i>Medical Director, Office of the Deputy Assistant to the Secretary of Defense for Chemical and Biological Defense Programs</i>	Biodefense Transformation
Roy Godson and Richard Shultz <i>Consortium for the Study of Intelligence</i>	Requirements for Effective Intelligence Against Non-State Armed Groups
ADM Bill Studeman, USN (Ret) <i>Presidential Commission on Intelligence Capabilities of the United States Regarding WMD</i>	Intelligence Community Transformation: Issues and Challenges



**JUNE 28-29, 2005**

COL Neal Anderson, USA <i>U.S. Northern Command</i>	NORTHCOM's Plans and Capabilities for CBRNE Response
CAPT Jim Burans <i>Director, National Bioforensic Analysis Center</i>	Overview of the National Bioforensic Analysis Center
Mike Evanson <i>Defense Threat Reduction Agency</i>	Pilot Program in Base Protection
CDR Andrew Kuepper, USN <i>Office of the Assistant Secretary of Defense, Homeland Defense</i>	CBRNE Consequence Management Executive Order
COL Michael McNeely, USAF <i>Joint Staff, J-5</i>	Proliferation Security Initiative
Dr. William Raub <i>U.S. Department of Health and Human Services</i>	Office of Public Health Emergency Preparedness
David Wilson <i>Federal Bureau of Investigation</i>	FBI Laboratory, Chemical Biological Sciences Unit

## Appendix D. Glossary

C3	Command, Control, and Communications
CBRN	Chemical, Biological, Radiological, and Nuclear
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOS	U.S. Department of State
DSB	Defense Science Board
DTRA	Defense Threat Reduction Agency
DTW	Detect-to-Warn
EMT	Emergency Medical Technician
JSTPS	Joint Strategic Target Planning Staff
MIDB	Modernized Integrated Data Base
NIH	National Institutes of Health
NORTHCOM	U.S. Northern Command
NSC	National Security Council
OSD	Office of the Secretary of Defense
OSD (PA&E)	Office of the Secretary of Defense, Program Analysis and Evaluation
SIOP	Single Integrated Operational Plan
SNM	Special Nuclear Materials
STRATCOM	U.S. Strategic Command
TIC	Toxic Industrial Chemical
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USD (I)	Under Secretary of Defense for Intelligence
USD (P)	Under Secretary of Defense for Policy
WMD	Weapons of Mass Destruction