The Science and Technology of Combating Terrorism

About the President's Council of Advisors on Science and Technology

President Bush established the President's Council of Advisors on Science and Technology (PCAST) by Executive Order 13226 in September 2001. Under this Executive Order, PCAST "shall advise the President ... on matters involving science and technology policy," and "shall assist the National Science and Technology Council (NSTC) in securing private sector involvement in its activities." The NSTC is a cabinet-level council that coordinates interagency research and development activities and science and technology policy making processes across federal departments and agencies.

PCAST enables the President to receive advice from the private sector, including the academic community, on important issues relative to technology, scientific research, math and science education, and other topics of national concern. The PCAST-NSTC link provides a mechanism to enable the public-private exchange of ideas that inform the federal science and technology policy making processes.

PCAST follows a tradition of Presidential advisory panels on science and technology dating back to Presidents Eisenhower and Truman. The Council's 23 members, appointed by the President, are drawn from industry, education, and research institutions, and other nongovernmental organizations. In addition, the Director of the Office of Science and Technology Policy serves as PCAST's Co-Chair.

The Science and Technology of Combating Terrorism

President's Council of Advisors on Science and Technology

July 2003

July 21, 2003

The Honorable John H. Marburger, III
Director, Office of Science and Technology Policy
The Executive Office of the President
Washington, DC 20502

The Honorable E. Floyd Kvamme
Co-Chair, President's Council of Advisors on Science and Technology
Washington, DC 20502

Dear Dr. Marburger and Mr. Kvamme:

The Panel on the Science and Technology of Combating Terrorism of the President's Council of Advisors on Science and Technology (PCAST) has prepared the enclosed report to assist in the nation's efforts in the war on terrorism. This document serves as a companion to the earlier PCAST report on how science and technology capabilities might best be structured to contribute to the newly formed Department of Homeland Security.

This report documents the work of the PCAST during 2002 and 2003 in the area of combating terrorism. The findings have in large part been discussed with the appropriate individuals in government throughout this time period, and many of the recommendations are already being implemented in one form or another.

The report expresses the views of the Panel members on a select set of key issues that are illuminated by science and technology and that we feel can improve America's efforts to counter terrorism. The action by the Congress to enact the President's proposal to establish the Department of Homeland Security, including an Undersecretary for Science and Technology, has importantly enhanced the nation's ability to call on its science and technology expertise in this regard.

In addition, the National Strategy for Homeland Security, published in July 2002, set the stage for creation of the Department of Homeland Security. This Strategy—together with two other key documents: The National Security Strategy of the United States of America, released in September 2002; and the National Strategy to Combat Weapons of Mass Destruction, published in December 2002—establishes the framework for our nation's efforts to combat global terrorism. Complementing these major planning documents, the President has announced Project BioShield, The National Strategy to Secure Cyberspace and The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.

Since there are a number of science- and technology-related initiatives already underway that address many aspects of the war on terrorism, we have not tried to be all-inclusive; rather we have sought to address a few key issues that we believe warrant particular attention.

Our recommendations focus on protecting citizen health through the creation of a comprehensive national readiness strategy, helping first responders, helping businesses protect our nation and improving the technology of personal identification. We also offer suggestions on cyberterrorism, and other matters involving threat detection, assessment and response. We would note that the report's appendices present an important part of the basis for our findings.

We hope our work and recommendations can contribute to helping make our nation safer from the terrorist threats it unfortunately confronts.

Sincerely,

Norman R. Augustine

President's Council of Advisors on Science and Technology

CHAIRS

John H. Marburger, III, Ph.D.
Director, Office of Science Technology Policy

E. Floyd Kvamme
Partner, Kleiner Perkins Caufield & Byers

MEMBERS

Charles J. Arntzen, Ph.D.
Director, Arizona Biomedical Institute and
The Florence Ely Nelson Presidential Chair,
Department of Plant Biology,
Arizona State University

Norman R. Augustine
Former Chairman and CEO,
Lockheed Martin Corporation

Carol Bartz
Chairman of the Board,
President, and CEO, Autodesk, Inc.

M. Kathleen Behrens, Ph.D.
Managing Director, RS Investments

Erich Bloch
Corporate R&D Management Consultant,
The Washington Advisory Group

Stephen B. Burke
President, Comcast Cable Communications

G. Wayne Clough, Ph.D.
President, Georgia Institute of Technology

Michael S. Dell
Chairman and CEO, Dell Computer Corporation

Raul J. Fernandez
CEO, Dimension Data of North America

Marye Anne Fox, Ph.D.
Chancellor, North Carolina State University

Martha Gilliland, Ph.D.
Chancellor, University of Missouri-Kansas City

Ralph Gomory, Ph.D.
President, Alfred P. Sloan Foundation

Bernadine Healy, M.D.
Medical Senior Writer and Columnist for U.S. News and World Report; Former President of the American Red Cross; Former Director of NIH; Cleveland Clinic Foundation

Robert J. Herbold, Ph.D.
Herbold Group, LLC

Bobbie Kilberg
President, Northern Virginia Technology Council

Walter E. Massey, Ph.D.
President, Morehouse College

Gordon E. Moore, Ph.D.
Chairman Emeritus, Intel Corporation

E. Kenneth Nwabueze
CEO/CTO Corporation, SageMetrics

Steven G. Papermaster
Chairman, Powershift Ventures

Luis M. Proenza, Ph.D.
President, University of Akron

George Scalise
President, Semiconductor Industry Association

Charles M. Vest, Ph.D.
President, Massachusetts Institute of Technology

EXECUTIVE DIRECTOR

Stanley S. Sokul

Panel on Anti-Terrorism Technology

CHAIR

Norman R. Augustine
Former Chairman and CEO,
Lockheed Martin Corporation

MEMBERS

Charles J. Arntzen, Ph.D.
Director, Arizona Biomedical Institute and The Florence Ely Nelson Presidential Chair, Department of Plant Biology, Arizona State University

M. Kathleen Behrens, Ph.D.
Managing Director, RS Investments

G. Wayne Clough, Ph.D.
President, Georgia Institute of Technology

Ralph Gomory, Ph.D.
President, Alfred P. Sloan Foundation

Bernadine Healy, M.D.
Medical Senior Writer and Columnist for U.S. News and World Report; Former President of the American Red Cross; Former Director of NIH; Cleveland Clinic Foundation

Bobbie Kilberg
President, Northern Virginia Technology Council

E. Kenneth Nwabueze
CEO/CTO Corporation, SageMetrics

Steven G. Papermaster
Chairman, Powershift Ventures

OSTP STAFF LIASION

C.E. Hildebrand, Ph.D.

Table of Contents

Executive Summary

This report documents the work during 2002 and early 2003 of the President's Council of Advisors on Science and Technology (PCAST) Panel on the Science and Technology of Combating Terrorism. Because of the urgency of our nation's efforts to rally scientific, engineering and technological resources in the war on terrorism, the findings of the Panel have, in large part, already been shared with the appropriate individuals in government throughout this time period, and many of the recommendations are currently being implemented in one form or another.

The Panel's recommendations focus on protecting citizen health through the creation of a comprehensive national readiness strategy, helping first responders, helping businesses protect our nation and improving the technology of personal identification. Importantly, the actions proposed emphasize helping citizens help themselves. We also offer suggestions on cyberterrorism and other matters involving threat detection, assessment and response. In each instance we attempt to acknowledge the activities that already exist in the private sector (citizen and corporate), and to suggest the appropriate governmental tools that could be applied to achieve the desired objectives in the particular situation addressed. As already noted, in a number of instances the Panel's recommendations are intended to confirm, augment or refocus efforts that are currently under way or under consideration.

Primary Recommendations

1. Protecting Citizen Health and Safety—A National Readiness Strategy

The White House, in conjunction with the Department of Homeland Security (DHS) and the Department of Health and Human Services (DHHS), should lead the creation of a coordinated national strategy for protecting citizen health and safety against terrorist actions. Such a strategy should organize and guide our public health and safety efforts and identify investments in science and technology that require long lead times. That strategy would be analogous to the strategy or doctrine that guided our national security efforts during the Cold War with the Soviet Union. This national readiness strategy would have many components, all of which need to be carefully developed and integrated. Four of the most vital components include:

a. Biodefense. Particular urgency exists in addressing procurement for biodefense measures because of the long lead times for drug and vaccine development. The first step is to produce, stockpile and maintain critical assets for biodefense, including diagnostics, antibiotics, antivirals and vaccines. Producing these items has traditionally involved a partnership between the government and industry. The Panel recommends that government's role in this partnership should be to develop a prioritized list of needed vaccines and to create—through specific guaranteed government purchases—a market for these products, a distribution plan, appropriate FDA protocols for the assessment of such products and a realistic indemnification plan.

b. Food and Water Security. While the biodefense efforts outlined above would govern the pharmaceutical response (inoculation or treatment in the event of human exposure), the means by which enemies might deliver harmful agents must also be addressed. Our food and water supply systems present potential vectors for delivering biological or chemical attacks aimed at citizen health, but we presently lack adequate knowledge and detailed planning needed to protect these systems and to respond to attacks against them. The Panel recommends enhanced and sustained federal investment in research to ensure continued discovery of the scientific and technological knowledge necessary to address this inadequacy.

c. *Self-Help*. The Panel strongly supports and encourages sustained efforts of DHS to mount a "citizen preparedness" campaign. Self-help at the individual level represents the first line of defense against many forms of terrorist attack. But most Americans today simply do not know the proper things to do in the event of a chemical or biological crisis, or a radiological or nuclear weapons attack. Nor do they have a family disaster plan involving preparation, communication, response and recovery formulated. Citizens can be helped in protecting themselves by widely distributing a fact-based and user-friendly pamphlet that describes what they can do before, during and after a terrorist attack to improve their survivability. The information provided in this pamphlet should also be made available through the Internet and by other means of public communication. Although initial steps are now being taken to alert the public through electronic means (for example via the comprehensive preparedness website *www.ready.gov*) and the media, much of the public remains largely uniformed and unprepared.

d. *A National Readiness Strategy*. The Panel recommends enhancing the campaign to increase civilian institutional awareness. For example, if DHS publishes recommendations that schools and workplaces should be prepared, it must also be ready to provide schools and workplaces with a blueprint for what readiness means and to provide appropriate information resources. Furthermore, many of the homeland security products that already exist—and the many more that are likely to come on the market—need standards and testing.

2. Public Health Preparedness

a. *Public Health Systems.* In addition to organizing and integrating biodefense, protection of food and water systems, and citizen self-help efforts, the nation needs a public health workforce knowledgeable in the science and technology of combating terrorism. Health professionals generally agree that the readiness and capacity of the nation's healthcare system to handle a major terrorist attack can be significantly improved. The Panel recommends several approaches to respond to this need:

- *Research and Education Centers of Knowledge* — establish several Centers of Knowledge devoted to aspects of terrorist threats as they relate to public health and safety.
- *Emergency Medical Supplies* — establish more extensive stockpiles of medical supplies and therapeutics for major emergencies.
- *Health Reserve Corps* — establish a civilian corps of trained and paid health reservists analogous to the National Guard. Plans should be in place to backfill these individuals in their day-to-day responsibilities in the event that they are activated to deal with a national emergency.
- *Advisory Group* — establish a scientific advisory panel backed by a robust communication system to provide advice and counsel to federal agencies when important public health decisions must be made, especially when time for considering alternatives is limited and consequences are great.
- *Psychosocial Effects* — establish a research program to help guide public response and policy development, and to sustain and augment research into the psychosocial implications of terrorist incidents.

b. Communications. The Panel recommends that the national readiness strategy should include a component for communicating with the public that incorporates lessons learned from previous terrorist incidents, especially communicating the risks and benefits of countermeasures such as vaccines and antibiotics. Above all, whatever information the government provides must be timely and accurate.

3. Helping First Responders

The Panel recommends that the federal government expand its program to help first responders. The program should include conducting research and development (R&D) specifically aimed at improving equipment for first responder protection (including equipment for situation assessment, personal protection and communication). It should also establish national technical standards that will help ensure the effectiveness and safety of first-on-scene personnel by reducing the likelihood that the units representing these individuals will purchase equipment that does not work as advertised, that requires exceptionally high levels of training or that is incompatible with equipment that may be shared with other organizations.

4.Helping Business Protect Our Nation

a. Security Standards and Recovery Plans. Action should be taken to substantially reinforce the existing standard-setting processes governing certain businesses to include consideration of the consequences of terrorist threats. Standards changes could, for example, address air filtration, fire resistance, detection and warning in buildings used by the public. It is important to coordinate physical protection and cybersecurity efforts to ensure efficient integration of activities common to both.

b. Small- and Medium-Sized Businesses. The Panel strongly endorses the establishment of the Office of Private Sector Liaison in the Department of Homeland Security. This Office will provide America's business community a direct line of communication with DHS and coordinated state and local agencies. The Panel recommends that this new office seek appropriate private-sector advice on working effectively with individual businesses, trade associations and other nongovernmental organizations to foster a dialogue between the private sector and DHS on the full range of issues and challenges faced by American businesses in the post-September 11 world. The Panel recommends that membership of the Homeland Security Science and Technology Advisory Committee in the Office of the Undersecretary for Science and Technology include experts who can address key industry sectors affected by homeland security.

5. Identity Authentication

A substantially expanded research and development program should be initiated to create and test reliable national individual authentication mechanisms. An expanded research and development effort in this area can lay the groundwork for whatever application of biometrics may be warranted in the future.

6. Cybersecurity

The Panel makes recommendations in several areas of cyberspace security that could be pursued as a complement to the National Strategy. These include extending the efforts contained in the National Strategy to the international level and placing responsibility for cybersecurity in the Department of Homeland Security. Physical attacks by terrorists may be accompanied by cyber attacks, and our response to this threat should be a coordinated one.

7. Detecting Nuclear Weapons

Significant efforts are underway to control access to nuclear materials, weapons and means of delivery. Nonetheless, there remain a number of opportunities for government, academia and the private sector to enhance the nation's capability to counter nuclear and radiological threats. There is a critical need to aggressively pursue an R&D program that will improve the ability to detect the presence of nuclear materials and weapons. Because of the enormous implications of the nuclear weapon threat, this effort deserves a mini-Manhattan Project type of effort.

Additional Recommendations on Threat Detection, Assessment and Response

1. Threat Assessment

The initial PCAST Report on Maximizing the Contribution of Science and Technology in the Department of Homeland Security recommended establishing a Red Team function within DHS. A Red Team would include experts in technology and operations related to terrorism who could identify likely threats and their consequences. It is further noted that it will be essential to coordinate Red Team exercises with private-sector entities.

This threat assessment function should not neglect a technique that is often referred to as "Blue Teaming." A Blue Team considers the responses that could be applied to a terrorist action identified by the Red Team, and helps provide a more realistic threat assessment.

2. List of Experts

The Panel recommends that high priority be given to the creation of a national registry of experts capable of dealing with the broad spectrum of issues that are likely to emerge in the immediate aftermath of terrorist acts. These experts should be available to deploy to the sites of terrorist incidents just as Federal Emergency Management Agency (FEMA) teams of structural and civil engineering experts deploy to hurricanes, earthquakes and other natural disasters in support of local authorities.

3. Data Mining and Information Fusion

The Panel recommends significantly increased funding for data mining and information fusion techniques that offer the potential of identifying terrorist actions before they occur. Although commercial firms already have access to an astonishing amount of personal information through marketing activities and credit card verification, and broad scale information is already publicly available on the Internet, the processes involved in countering terrorists must nonetheless protect personal privacy and confidentiality to the maximum practicable extent.

I. Introduction

In 2001 the President's Council of Advisors on Science and Technology established a subcommittee to address the science and technology of combating terrorism. In mid-2002 the panel provided a report to the President recommending a *structure* for the conduct of research and development within the Department of Homeland Security. The present report provides the views of the panel on a broader set of issues affecting the science and technology *content* of the nation's activities to combat terrorism.

The PCAST panel focused its efforts related to homeland security primarily on actions relating to science and technology that can have a significant impact in the "mid-term" time frame (one to five years), and that deal with the interface between the public and private sectors, including individual citizens. However, the Panel has noted a few potentially high payoff actions that could have a significant impact outside this focus. The recommendations include actions that can enhance the ability of the private sector and private citizens to contribute to the war against terrorism. Because of the urgency of the matters involved, the various issues and findings have been discussed continually with appropriate federal agencies as this report was prepared, rather than waiting for formal approval of this document.

Because of the extraordinarily broad nature of the role of science and technology in countering terrorism, no attempt has been made in this review to survey the entire field. Rather, the Panel has selected specific topics that relate to the general guidelines noted above and that appear to be worthy of special emphasis.

This focus means that some weighty topics considered by the PCAST Panel on the Science and Technology of Combating Terrorism are not addressed in this report. These issues are, however, important to the nation and should still be carefully considered. Among these are such matters as protecting large crowds from terrorist attack, countering terrorist acts of a widely diffuse nature such as attacks on the food supply or on individuals, and protecting commercial aircraft from shoulder-fired surface-to-air missiles. *Such "free-lance" terrorism could become a preferred means of attack in an environment where terrorist networks have been "decapitated" and their ability to communicate and raise funds significantly diminished.*

II. Mobilizing Our Science and Technology Resources

An underlying characteristic of modern terrorism is that individuals or small groups, not acting on behalf of enemy nations, can threaten the lives of very large numbers of people and profoundly alter the day-to-day functioning of a free society. Although it is not possible for these groups to exert control over that society, they can significantly disrupt the ability of established institutions to preserve a stable order. This disproportionate impact is due in part to the open nature of our society, the ability of enemies to live among us, their willingness to sacrifice their lives, and our reliance on complex and finely balanced systems of governance and commerce—which in turn depend on sophisticated technology to function efficiently.

Our vulnerability to terrorist threats stems in part from the asymmetric nature of that threat which seeks to exploit our openness with any weapon at hand. Such threats range from low-tech suicide bombs to high-tech weapons of mass destruction—regardless of the consequences to innocent people. Some of our most effective countermeasures to defend against these threats will draw on new science and technology applications. Fortunately, there is an exceptionally wide range of these applications: from threat detection (reliable identification systems, bioagent detection), to protection measures (new vaccines and effective personal protective equipment), to response systems (communications and

emergency medical care). Mobilizing our science and technology resources for this effort has three major dimensions: engaging the private sector (including businesses and individual citizens), pursuing an effective federal leadership role and strengthening the ability of state and local governments to act.

III. Engaging Private Citizens and Businesses

It has been estimated that over eighty percent of the physical assets that might be targeted by terrorists are owned by the private sector. Similarly, much of the nation's science and technology capacity for dealing with terrorism resides in the private sector—that is, in the nation's corporations, academic institutions, and the scientists, engineers and technicians who work there. This is true not only for countering the low-tech threats most commonly used by terrorists—such as conventional explosives—but also for developing innovative ways to use science and technology to counter many of the more sophisticated and destructive weapons that are of increasing concern. Nonetheless, because of the differentiated, competitive, market—driven character of the private sector, the task of harnessing its considerable capabilities in this battle falls to a large degree upon government—particularly the federal government—insofar as leadership is concerned. State and local governments, given their primacy in providing local security, also play a key role, particularly as far as implementation is concerned.

Many of the fundamental characteristics that underpin America's civilian enterprises tend to be at variance with the requirements for homeland security. Prominent among these inherent tensions are those associated with efficiency vs. resilience and individual freedom vs. security. Considerations of efficiency often argue for maintaining small inventories and using streamlined (single string) system architectures. In contrast, resilience often demands large stockpiles of parts and products and redundant architectures. This intrinsic stress became evident in the automotive industry immediately after September 11, when highly regarded "just-in-time" inventory practices proved very brittle when the nation's borders were closed unexpectedly and the flow of components was thereby curtailed. Additionally, the trend of U.S. industry to locate component and assembly operations overseas in low labor-cost areas can affect supply and inventory considerations, particularly when borders are sealed. Similarly, efforts to control medical costs dictate nearly full occupancy of beds in hospitals during "normal" times, leaving little cushion available in case of emergency.

These considerations point to the potential need for difficult compromises when drawing on science and technology to combat terrorism. This led the PCAST Panel to propose selected actions suitable for immediate implementation (e.g., guidance for citizen personal preparedness) and programs to bring the nation's capabilities to a level of readiness permitting introduction either in steps or, alternatively, full implementation "just in case" (e.g., an integrated personal identification system based on drivers' licenses as one important step towards the ability to field a robust and more widely applicable identification system were the latter ever to be deemed necessary).

Individual Citizens

Leadership in response to terrorism must originate with government. However, in this war—as in others where civilians have become targets (e.g., the London bombing blitz during World War II)—there is much that individual civilians can do to protect themselves, working hand-in-hand with federal, state and local governments. However, except for the recent and highly localized activities stemming from the declaration of a high (orange) threat level alert, there has been little involvement in self-defense on the part of the general public to date. This is not likely to change unless something happens to increase general awareness of the nature of the danger we face from potential terrorist use of weapons of mass destruction, and unless people are informed and motivated to take steps to improve the chances of survival for themselves and their families.

If informed civilian awareness for self-protection can be stimulated, it will help activate normal free-market forces. For example, it may lead to the purchase of civil defense items by individuals, such as filter masks, safe rooms and convenient emergency kits. Increased civilian awareness will also create a demand for protection in the workplace and through these demands, provide an incentive for further improvements through R&D conducted in the industrial sector and academia. In order to stimulate public demand, however, people need to have confidence that there are *meaningful* things that they can do for themselves. They also need to have confidence that they are not wasting their resources on alarmist advice or ineffectual measures. *Furthermore, they require a means of being warned of impending danger and of the nature of the danger once an attack is underway*. Citizen confidence in self-help measures—based on scientifically and technologically sound information—can also serve to alleviate the fear and anxiety that terrorists seek to instill. Erroneous, vague or conflicting guidance can have exactly the opposite effect.

This calls for a campaign aimed at training and empowering citizens. It should be based on the fundamental message that you *can* help yourself and that doing so is your duty to yourself, your family and your country. In addition to that fundamental message, the campaign should tell people where to find help. For example, phone numbers to be called, brochures that are available and distributed through post offices, web sites and other means. The information through these sources should emphasize practical actions based on scientific facts and empirical evidence. The goal must be training and empowering citizens, not frightening them with menaces to which they cannot respond or suggesting measures that are impractical, unaffordable, faddish, ineffective or simply wrong. Citizen response to high (orange) threat alerts suggests that not only will those citizens act in the market for self-defense, but also that the government must drive the information provided so that sensationalized media reports do not undermine credibility.

Such information should include answers to specific questions, in a "Q&A" format—especially those questions that continue to perplex the public—for example: "If I tape myself into a 'plastic safe room' am I in danger of asphyxiation? If I select a special filter to install in my air conditioner or heater, what size particle must it stop? What will that do to my power bills? Should my safe room be above ground to protect against chemical agents or below ground to protect against blast? In case of a smallpox attack, should I go to the hospital to be vaccinated or stay away from all those sick people?" The absence of credible and practical guidelines that deal with these and many other questions confuses and frustrates many people, who then may take no action at all.

Private Enterprise

The ability of private enterprise to engage in the war on terrorism is shaped in part by the fact that there are few free market incentives to motivate or justify its participation. Firms, of course, have an interest in surviving natural disasters or other disruptive events, much as it is in a firm's interest to take steps that assure survival of its employees and facilities in the face of terrorist actions. But the efficacy of such steps must be assessed in the context of the competitive environment of the free, global marketplace. Therefore, automotive firms generally cannot afford to maintain stockpiles that are substantially greater than those of their (international as well as domestic) competitors; telecommunications firms cannot afford to maintain excessively redundant switching centers and power sources; and pharmaceutical companies cannot underwrite research for which there is a highly uncertain demand.

On the other hand—as evidenced by the effort devoted to avoiding the Y2K problem and by the willingness of firms to participate voluntarily in ameliorating the immediate aftermath of the September 11 events—the private sector can and must play a key role in countering terrorism. To bring this about requires that the nation's homeland security efforts harness the enormous power of the free enterprise

system. The challenge of protecting against biological warfare agents provides a case in point. America's pharmaceutical and biotechnology firms have demonstrated a remarkable ability to introduce new drugs and vaccines into the civilian market—all while rewarding their shareholders who invest the capital that, in part, enables those new advances to take place. This commercial market is characterized by large scale, relative predictability (e.g., any drug that proves an effective cancer therapy will be in demand) and can be expected to support significant financial margins when an effective drug is successfully developed through clinical trials and gains Food and Drug Administration (FDA) approval. In contrast, there has been little or no market for developing means of neutralizing agents associated with biological warfare. Those markets that do exist for such agents are highly unpredictable and, importantly, are fraught with financial liabilities.

This situation, however, is not unprecedented. There is, for example, no civilian market for many of the products of America's defense industry (such as tanks, fighter aircraft and nuclear submarines), yet our nation has built a defense industrial base unrivaled in the world in terms of the quality and capability of its products. But there are important differences between the pharmaceutical industry and the defense industry that must be considered when trying to apply scientific and technological capabilities to combat terrorism. Most of the nation's defense firms are highly concentrated in defense, do not enjoy significant alternative market opportunities, are highly indemnified by the government customer and have created a capital structure that, together with the government's policies towards that industry, permits them to remain financially viable. In contrast, pharmaceutical companies are generally accustomed to larger profit margins than defense companies, yet also invest far more of their own discretionary resources in research and development. They also face very high risks and uncertainties in moving potential products from the laboratory through the FDA approval process. Furthermore, they have alternative markets readily available wherein they can realize significant margins if the counterterrorism market does not offer attractive benefits.

In short, attempts to mobilize the scientific and technological capabilities of such industries will likely be unsuccessful if we seek simply to use the government-defense sector model—although some of the attributes of the model may be relevant. Since many of the markets for countering terrorism (personal protective equipment, for example) are characterized by large numbers of small buyers—such as local fire departments—policies designed to enable large individual purchases may have little, if any, effect in encouraging the innovative involvement of the private sector. This raises the question of the most effective government role in mobilizing the nation's entire base of technological and scientific resources to counter terrorism.

The President's announcement of Project BioShield is an important step in the right direction and sets the stage for implementation of a national framework that will enable the development of relationships between government and some firms in the private sector by providing appropriate measures for incentives and indemnification. The challenge will be to refine and sustain this effort over the long period of time required to introduce the necessary new products.

IV. The Government Role

The federal government itself supports a substantial science and technology enterprise that exceeds $110 billion in annual expenditures. The institutional platforms and skilled human capital associated with this enterprise include agencies such as the National Science Foundation (NSF), National Institutes of Health (NIH), National Aeronautics and Space Administration (NASA), National Research Council (NRC), Environmental Protection Agency (EPA), Defense Advanced Research Projects Agency (DARPA), United States Department of Agriculture (USDA), FDA, National Institute of Standards and Technology

(NIST), Department of Energy (DOE) and the newly established DHS, with its R&D segment. These agencies provide a reservoir for the nation's science and technology efforts in countering terrorism. Their capabilities, however, will need to be focused on challenges that may not conform to past experience and practice, requiring the reallocation of resources (both funding and people) and the development of special research guidance and coordination.

In addition to mobilizing its own substantial science and technology capabilities, the federal government will need to play a central and continuing role in engaging industry and academia as partners in the nation's counterterrorism efforts. This role will require consideration of a range of measures to shape markets and innovation systems to address the nation's specific needs. In spite of the absence of an existing free market with regard to many of the elements of the counterterrorism effort, there is much that the federal government, working in concert with states and localities, can do to ensure that market forces encourage science- and technology-based innovation and subsequent development of affordable and useful equipment.

While the federal government always retains the ability to directly impose security-related mandates upon business, it also possesses other less intrusive tools to encourage desired actions in a manner that stimulates a high degree of innovation and flexibility. These include:

- Working with state and local governments and other germane organizations to establish codes and standards, thus permitting first responders (as well as commercial suppliers) to enjoy the benefits of scale, to have increased assurance of product quality and, importantly, interoperability. The benefits of establishing uniform codes and standards include:
  - Performance standards and testing allow local fire departments and law enforcement organizations to make informed acquisition decisions based on empirical evidence that products perform as claimed.
  - Interoperability standards allow local emergency organizations to operate together or in concert with neighboring departments.
  - Standardized equipment buttresses the formation of acquisition pools that allow the fractionated market power of state and local agencies to take advantage of economies of scale.
  - Standards and certification will—presumably as by-products—result in lowered insurance rates.

By taking the actions described above, exposure to natural threats would also be reduced.

- Guaranteeing a market for pre-specified products meeting national needs for counterterrorist capabilities where markets do not otherwise exist—for example, for vaccines and therapeutics to counter biological agents. Where performance warrants, profit margins should be allowed that are competitive in the marketplace. Although by guaranteeing future procurement, government might lose some of its flexibility to revise its plans—and in doing so could potentially challenge existing procurement law—such an approach appears essential. Such guarantees could provide powerful tools to encourage firms to participate in endeavors for which there is no civilian market, especially in the biodefense arena where the diseases in question do not manifest themselves in peacetime situations.

- Offering incentives to induce desired actions—for example, tax credits for research having direct application to homeland security, or for the construction of physical plants offering properties specifically applicable to countering terrorist threats.

- Providing indemnification for business risks that go well beyond the normal hazards of the commercial marketplace. This may be especially important in biodefense where liabilities for biopharmaceutical

entities may have to be limited to enable investments in therapeutic or prophylactic products that could have unanticipated consequences when administered on a large scale to civilian populations in the event of a bioterrorist attack.

Finally, the government always retains the choice of establishing internal capabilities to fill unique needs, much as the arsenal system was established to fulfill certain defense needs.

The selection of particular tools to deal with specific needs will inevitably depend on the circumstances being addressed. For example, directly underwriting research could prove a powerful incentive for universities (with no interest in production) or for makers of protective clothing (with a limited market for their products), but would be much less appealing to pharmaceutical firms (where research talent is at a premium and commercial markets are large and potentially lucrative).

V. Primary Recommendations

Based on these considerations, the PCAST Panel on the Science and Technology of Combating Terrorism offers a number of recommendations. In each instance we attempt to acknowledge the issues and capabilities that exist in the private arena (citizen and corporate), and to suggest the appropriate governmental tools that could be applied to achieve the desired objectives in the particular situation. In a number of instances, steps are already underway in the federal government that relate to the actions proposed, in which case these recommendations are intended to confirm, augment or refocus these efforts.

1. Protecting Citizen Health and Safety—A National Readiness Strategy

The White House, in conjunction with DHS and DHHS, should lead the creation of a national strategy for protecting citizen health and safety that will organize and guide our public health and safety efforts and identify science and technology investments that require long lead times. This "national readiness strategy" would have many components, all of which need to be carefully developed and integrated. Four of the most vital aspects include:

a. Biodefense. Due to the lengthy process inherent in drug and vaccine development, immediate attention must be paid to the procurement of biodefense measures. The first step is to produce and stockpile critical assets for biodefense, including diagnostics, antibiotics, antivirals and vaccines. Producing these items has traditionally involved a partnership between government and industry. Now the government's role in this partnership should be expanded to include developing a prioritized list of needed vaccines, diagnostics and therapeutics; as well as creating a market for these products through specific guaranteed government purchases, a distribution plan, appropriate FDA protocols for the evaluation of such products and a realistic indemnification plan. These steps are particularly important because many of the specific diseases involved in bioterrorism do not exist in a peacetime environment.

b. Food and Water Security. While the biodefense efforts outlined above would govern the pharmaceutical response to direct human exposure (preventive inoculations and post-exposure treatment), the means by which terrorists could deliver harmful agents must also be addressed. Our food and water supply systems present an opportunity to conduct a biological or chemical attack aimed at citizen health, but we lack the full knowledge necessary to protect those systems. This circumstance affects our ability to accurately assess potential risks to the food and water supply, and to adequately develop an effective and affordable defense. Sustained federal investment in research is necessary to address gaps between terrorist threats and existing capabilities, as well as the ability to detect emerging threats. The appropriate federal agencies should evaluate the

applicability, in the context of biological or chemical terrorism, of existing technologies for assessing microbial or chemical contamination of food or water. Furthermore, as new research findings provide scientists with a better understanding of the factors that affect the safety of the U.S. food and water supplies, policymakers will need to revise laws and regulations in response to the new knowledge. Finally, a plan must be put in place specifying how we will respond to any attack on the food or water supply.

c. Self-Help. Citizen self-help presents the first line of defense against many forms of terrorist attack, but most citizens today are unaware of appropriate actions to take in the event of a chemical, biological, radiological or nuclear attack. Most do not have a family disaster plan that includes the necessary elements of preparation, communication, response and recovery. While developments over the next several years will provide citizens with new tools to help themselves, they must begin to use the information and products currently available and become comfortable with the notion that self-help plays an important role in protecting themselves and their families from terrorist attacks. Credible self-help information—by enabling citizens to feel that they, themselves, are in fact taking action to the extent practicable—will also help alleviate the fear and anxiety that terrorists seek to create. Widely distributing a fact-based and user-friendly pamphlet that describes what citizens can do before, during and after a terrorist attack can increase citizens' chances of survival. This pamphlet should include an understandable and credible explanation of the different kinds of threats and their consequences, as well as measures citizens can take to protect themselves. The latter should include ensuring a safe and sustainable personal supply of food, water and air. Since very different actions may be appropriate depending on the nature of an attack, scientifically based information should be provided to every citizen *before it is needed*. Other media, including the Internet, television, videotapes, inserts in Social Security and tax mailings, etc., should augment the information in the pamphlet. The Panel strongly supports the recent initial efforts of DHS to mount a citizen preparedness campaign.

d. A National Readiness Strategy. However, such a campaign is only a beginning. DHS must be organized to respond to the issues that will be raised as a result of increasing civilian awareness, even ultimately tying recommended *citizen* actions to some derivative of the color-coded threat level. Many of the homeland security products that already exist, and the many more that are likely to reach the market in the future, need standards and testing. Special attention should be given to particular needs of certain types of facilities that provide daycare for children or individuals requiring institutional care (disabled, mentally ill, etc.), as well as facilities and communities of predominantly senior citizens. Again, there is an important role for DHS in this area. Civilian defense must become an ongoing activity, not just a one-time endeavor. Furthermore, better methods of civilian defense should have a prominent place in the research and development conducted by DHS (e.g., better air filters for buildings, citizen emergency warning systems and standards for masks suitable for use by the public).

2. Public Health Preparedness

a. Public Health Systems. In addition to organizing and integrating biodefense, food and water systems, and citizen self-help efforts, the nation needs a public health workforce that is knowledgeable in science and technology and that is equipped with resources developed in the environment of fast-changing medical science and technology. The process should be highly innovative in order to generate the new science and technology needed as biological and other threats change over time. Health professionals largely agree that the readiness and capacity of the

nation's healthcare system to handle a major terrorist attack can and should be significantly improved. We suggest several basic activities to address this situation:

- *Research and Education Centers of Knowledge* — the establishment of several Centers of Knowledge devoted to different aspects of terrorist threats as they relate to public health and safety.
- *Emergency Medical Supplies* — establishment of more extensive stockpiles of medical supplies and therapeutics to be available in times of crisis.
- *Health Reserve Corps* — establishment of a civilian corps of trained and paid healthcare reservists whose skills and the situations they may be called upon to manage should be evaluated to ensure compatibility with the prepared operational plan.
- *Advisory Group* — the establishment of a scientific advisory panel to provide advice and counsel to federal agencies when important public health decisions must be made, especially when time for considering alternatives is limited.
- *Psychosocial Effects* — augmentation of research into the psychosocial implications of terrorist incidents in order to help guide public and policy responses.

b. Communications. The national readiness strategy should include a component for communicating with the public that incorporates lessons learned—such as those stemming from the anthrax incidents of 2001—as well as addresses and communicates the risks and benefits of countermeasures, such as vaccines and antibiotics. (Five individuals died as a result of the 2001 anthrax attack. It was reported that ciprofloxacin was prescribed for as many as 40,000 individuals and an unknown number began taking it independently.) A mechanism should be created to ensure that those involved in communicating with the public during crises are current on the lessons learned from the psychosocial and/or medical research recommended above.

3. Helping First Responders

The federal government should expand its program to help first responders. The program should include conducting research and development to improve equipment for first responder protection (including equipment for situation assessment, personal protection and communication), as well as establishing national technical standards that will help ensure the effectiveness and safety of first-on-scene personnel (by reducing the likelihood that these units will purchase equipment that does not work as claimed, that requires exceptionally high levels of training or that is incompatible with equipment that may be shared with other organizations). First responders function in a highly fragmented organizational environment with very limited means to undertake independent research, development and testing on their own. While advancements in the technological capabilities of equipment for first responders are important, research and development aimed at lowering the cost of adequate and useable equipment will probably have the greatest near-term impact on response capabilities. Similarly, while developing more sophisticated new standards can be valuable, verification of even basic technical standards will be of immediate value to local first responders.

4. Helping Business Protect Our Nation

a. Security Standards and Recovery Plans. Action should be taken to substantially reinforce the existing standard-setting processes governing certain lines of business to include consideration of the consequences of terrorist threats. Standards changes could, for example, address air filtration, fire resistance and protective clothing. As occurred during the response to the Y2K threat, businesses in a wide range of essential infrastructure sectors (such as food, electricity, telephone service, etc.) should be encouraged to develop plans for business continuity and recovery. The Panel is aware of the Executive Branch's ongoing development of a comprehensive strategy for

critical infrastructure protection and assurance, which is included in The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Close coordination between physical protection and cybersecurity efforts will ensure efficient integration of activities where it is appropriate. The Panel recommends the establishment of mechanisms to ensure continuing involvement of the private sector in developing and updating contingency plans and strategies, as well as in research and development planning to support continuing operations.

b. ***Small- and Medium-Sized Businesses***. The Panel strongly endorses the establishment of the Office of Private Sector Liaison in DHS. This Office will provide America's business community a direct line of communication with DHS, as well as with state and local agencies. The Panel further recommends that this new office seek the advice of the private sector on working effectively with individual businesses, trade associations and other nongovernmental organizations to foster a dialogue between the private sector and DHS on the full range of issues and challenges faced by America's business sector in the post-September 11 world. Particular attention should be given to the unique challenges faced by small- and medium-sized businesses as contrasted with those of larger businesses.

The Panel also supports the advisory functions of the Homeland Security Science and Technology Advisory Committee (in the Office of the Undersecretary for Science and Technology) and recommends that its membership include experts capable of addressing issues affecting specific industry sectors that may contribute to scientific and technological solutions to homeland security challenges.

5. Identity Authentication

A major research and development project to create and test reliable means of robust individual identity authentication on a large scale should be initiated. Such an identification system could build upon the access control and biometrics research currently underway in several government agencies (National Institute of Standards and Technology; Defense Advanced Research Projects Agency; and the Departments of Defense, Homeland Security, and Justice). Congress has already mandated the deployment of an entry-exit biometric system on our borders. The Panel is aware of the lead that the Office of Science and Technology Policy (OSTP) and DHS, as well as other interested agencies, are taking in assessing biometric technology, and the Panel recognizes it as a platform for addressing the broader issues that have been identified in numerous earlier studies.

6. Cybersecurity

The Panel notes the February 2003 release of the National Strategy to Secure Cyberspace. Four aspects of cyberspace security that could be pursued as complements to the National Strategy are: (1) establishment of a mechanism to ensure inter-agency coordination of relevant research and development programs (possibly through the National Science and Technology Council); (2) consideration of a broad test bed to assess the scalability of particular security measures; (3) expansion of efforts contained in the National Strategy to the international level, with particular emphasis on research to develop cooperation among American industry and foreign governments that will achieve a more robust Internet architecture; and (4) assignment of responsibility for cybersecurity to the Department of Homeland Security.

7. Detecting Nuclear Weapons

Recognizing that significant efforts are underway to control access to nuclear materials, weapons and their means of delivery, a number of additional efforts by the government, academia and the private sector are needed to enhance the nation's capability to counter nuclear and radiological threats. The Panel recommends communicating to the public the nature of these threats in a clear and timely manner. The information should inform and stimulate public awareness, but avoid inducing unwarranted

alarm. Additionally, there is a critical need to aggressively pursue an R&D program that will improve the ability to detect the presence of nuclear weapons. Because of the enormous potential consequences of the nuclear weapon threat, this effort deserves a comprehensive systems approach. Although this is a daunting task, its potential importance in the decades ahead can hardly be overstated.

VI. Additional Recommendations on Threat Detection, Assessment and Response

The PCAST Panel on the Science and Technology of Combating Terrorism makes the following additional recommendations, which are further discussed in the appendices.

1. Threat Assessment

The initial PCAST Report on Maximizing the Contribution of Science and Technology in the Department of Homeland Security recommended the establishment of a Red Team function within DHS. A Red Team would include experts in technology and in terrorism to identify likely threats and their consequences. The Red Team should make assessments that include the perspective of a terrorist organization and consider the various strategies and tactics a terrorist might choose (targets, weapons, etc.). Such a perspective will be necessary to avoid the mirror-imaging of adversaries that can lead to strategic surprises and unanticipated types of attack.

As the Department of Homeland Security organizes itself, the Panel is pleased that such a Red Teaming function is under active consideration. We further note that in organizing this threat assessment function, what is sometimes referred to as "Blue Teaming," should also be considered. A Blue Team identifies possible responses to the terrorist actions identified during the Red Team activity. Blue Teaming not only helps to improve response capabilities, but also allows for more realistic threat assessments by preventing the Red Team activity from being assessed on a "worst case scenario" basis. The Red Teaming activity should anticipate appropriate Blue Team responses and an iterative process established.

2. List of Experts

High priority should be given to the creation of a national registry of experts capable of dealing with the issues that are likely to arise in the immediate aftermath of terrorist acts of all types. The experts in the registry should be supported with an effective means of communicating with national leaders, local response managers and, when appropriate, the general public—all under emergency conditions. These individuals should be available to deploy to terrorist incidents in a manner patterned after FEMA's teams of structural and civil engineering experts who respond to hurricanes, earthquakes and other natural disasters in support of local authorities. The National Academies and other scientific and engineering associations are currently seeking to engage the nation's vast scientific and technological talent base in the effort to combat terrorism, but these efforts must be developed in a logical and integrated way to support the needs of decision makers.

3. Data Mining and Information Fusion

The Panel's deliberations and briefings have reaffirmed the enormous need for effective integration of multiple data sources and types of data for countering terrorism—for example, the integration of data acquired by threat-agent sensor arrays or tracking and fusion of financial transaction data.[1] A significant increase is needed in funding the development of advanced data mining techniques that have the potential to identify terrorist actions before they occur. An important aspect of this effort would be determining methods of assuring appropriate degrees of privacy, while recognizing the extent to which such mining systems are already available to commercial firms through credit card verification technologies and market research and to the general public through Internet searches.

Appendix 1. A National Readiness Strategy: Health and Safety

A national strategy for health and safety readiness to combat terrorism is an essential ingredient in focusing our overall readiness efforts and especially in defining science and technology priorities and investments that require long lead times. The framework developed for a national readiness strategy should address the full spectrum of threats—conventional explosives, biological, chemical, radiological, nuclear and psychological. This discussion is focused on attacks which involve weapons of mass destruction because of their potentially devastating impact and on bioterrorism in particular because of the uniqueness of the demands it places upon the nation's defenses, its consequences and its potential availability to terrorists.

Bioterrorism involves human intervention to promote the spread of disease. Deliberate release of natural or engineered biothreat agents directed at humans represents one of the relatively few terrorism threats with the potential to rupture our national fabric. Widespread fear and profound economic disruption would amplify the medical consequences of an attack involving dangerous agents transmissible from person to person. An attack on one of our major trading partners could also have a severe negative impact on the U.S. economy as well as on the lives of the citizens of that nation and other nations.

Public health readiness to combat major acts of terrorism is a massive undertaking that requires leadership at the national level. It involves both the private and public sectors, is a local as well as a federal effort and is multidisciplinary—requiring expertise in science related to air, water, veterinary medicine, agriculture, general medicine and public health. There has been a focus on improving the public health at the state and local level for many years. This new and potentially overwhelming public health threat demands the increased attention of the federal government.

The national readiness strategy at the federal level should be based on a formal risk/benefit analysis to allow the identification of priorities incorporating scientific methods of technology evaluation. The strategy would prioritize the focus on specific infectious agents and countermeasures which are currently understood and would look into the future to clarify the spectrum of required materiel and operational capability to sustain an effective biodefense. It should include measures that prevent pathogens and toxins from being spread through food and water systems, contagious pathogen transmission and it should identify vaccines and antibiotics that help the body fight pathogens once they have entered the body. The status of our health system to respond to a large-scale attack on citizen health should be evaluated and a means to communicate with the public before, during and after an attack should be designed. Lessons learned from the 2001 anthrax emergency and the 2003 Sever Acute Respiratory Syndrome (SARS) epidemic should contribute to developing an effective communications system that would convey the risk/benefit considerations of biological attack countermeasures. There should be a plan for the proper deployment of such measures—including the steps individuals should take in their own behalf.

Because of its special access to information about our enemies' capabilities, the federal government is uniquely qualified to design a biodefense strategy and to determine the priorities for bioterrorism countermeasures. To engage the private sector effectively, the government must speak with a clear and consistent voice. It must also understand the research and development system and market mechanisms that govern the biodefense arena, since they are different from the more traditional national defense and healthcare environments.

To create an integrated nationwide public health response capability under the leadership of a federal agency, certain specific cultural issues must be addressed. The life sciences and medical communities are not accustomed to considering intentional enemy threats related to their areas of research interest. Further, their research culture is, in most cases, averse to top-down direction with regard to research goals and timetables. A mechanism to harmonize the required research and the mechanisms for the integration of needed work and existing cultures needs to be developed. This could be achieved through extramural centers of excellence, which should demand interdisciplinary team efforts from the outset.

The Panel suggests five key areas that a national readiness strategy should encompass: biodefense, food and water safety, individual self-help, the public health system and communications. Ultimately, if it is to be successful, the national readiness strategy will require coordinated efforts by the nation's public and private sectors. DHS, in collaboration with the Department of Defense (DoD) and DHHS, should be tasked with development of a strategic national health readiness doctrine.

1.1 Biodefense—Beyond BioShield

Particular urgency exists in addressing procurement of biodefense products and services, especially because the development of new drugs and vaccines takes a long time and America's pharmaceutical and biotechnology industries, where a great deal of our biomedical innovation capability resides, are not yet significantly engaged in this effort.

Public-Private Cooperation for Biodefense

After the formulation of a biodefense strategy with its priorities set, a critical need exists to produce and stockpile vital tools for biodefense, including protective gear, antibiotics, antivirals, vaccines and other countermeasures against biological threat agents. Producing such tools has always involved cooperation between the government and industry. Typically, the government's predominant role is in the earliest research stages—with private-sector investments and activities dominating in the evaluation, manufacture and wholesale distribution of antibiotics and vaccines.

It is probably not an exaggeration to say that in the past 30 years, every important antimicrobial drug and vaccine discovery has benefited in some way from the research conducted under the sponsorship of NIH. Through its intramural and extramural programs, NIH has funded discoveries that have provided a foundation for the expansion of new knowledge about how infectious agents spread and cause disease and how the human body fights back. In addition to its unique mission to develop basic scientific knowledge, NIH has facilitated moving scientific discoveries out of the laboratory and into clinical trials where safety and efficacy can be evaluated. Other federal programs at the Centers for Disease Control and Prevention (CDC) and in other departments within DHHS, DoD and Veterans Affairs (VA), have also made important contributions. For example, VA makes a valuable contribution by conducting clinical trials.

The government, and particularly FDA, establishes minimum standards for healthcare product safety and efficacy. This regulatory role extends to manufacturing practices. The extent to which regulation of manufacturing drives the costs and development times of vaccines and other products is an important consideration in establishing biodefense procurement policy.

Finally, the government has successfully created large and inviting markets for biologic innovations by serving directly as a customer (via Medicare, Medicaid and VA's healthcare programs), as well as by the regulatory and tax provisions that are important to the large, private health insurance industry.

As important as the government's role is, it can be said that all of the important vaccines and therapeutics for disease prevention and treatment in the United States have become available only after substantial effort and investment by private-sector companies in the pharmaceutical and biotechnology

industries. Some of these programs began as early-stage discovery programs in industrial laboratories. Often these programs benefited from technology licensed from the nation's research universities, where discoveries were typically funded by government grants. Still others were the result of technology transferred by NIH or other agencies to a committed industrial partner under licenses and Cooperative Research and Development Agreements (CRADAs). Regardless of how industry became involved, every successful product has required private investment ranging from tens to many hundreds of millions of dollars.

The incentive for the private sector to make these huge investments has been the size of the market for successful innovations, which can generate hundreds of millions or even billions in annual sales with substantial profit margins. This is in striking contrast to the smaller margins typically seen in the defense industry and the maximum margins allowed in typical federal procurement programs. As a result, the biodefense (pharmaceutical and biotechnology) sector has a different innovation system, reinvestment policy and market structure from the national defense sector. While American companies can be counted on to respond to a crisis in the short term, efforts to attract the best people and companies to work for many years on high-risk bioterrorism countermeasure projects will fail if the reward structure is not aligned with the prevailing incentives in that industry sector. Not only do investments in new pharmaceutical and biotechnology products entail large, long-term commitments, but also the FDA approval process is very demanding and introduces considerable uncertainty.

Pharmaceutical and Biotechnology Firms

With regard to pharmaceutical and biotechnology firms, the most important missing ingredient for attracting investment capital into bioterrorism R&D is the lack of a large, predictable market with appropriate profit margins and defined risks. If investors believe that a company is developing a drug to improve treatment of breast cancer, they know how to assess the likelihood that Medicare, managed care and other health insurance plans will reimburse such an innovation. Today, the market for highly innovative and effective means to protect against potential bioterror agents is altogether uncertain. Cost-plus manufacturing contracts with rates-of-return typical in the defense industry are not economically viable for companies with the ability to target important peacetime human pharmaceutical and vaccine markets in the commercial arena.

One procurement innovation that should be explored for high-priority countermeasures is the use of "purchase orders" for products that would only have a market demand in preparation for or after the occurrence of a particular type of terrorist attack. With such an approach DHS, in collaboration with DHHS, as mandated in the Homeland Security Act of 2002, would define specifications for new drugs and vaccines required to address foreseeable threats. These specifications would need to encompass safety, efficacy, shelf-life and other pragmatic requirements. If a company could deliver a drug or vaccine meeting the specifications, it would be assured of a supply contract with an opportunity to earn a competitive profit. For targets with high enough priority, the opportunity should compare to major products developed elsewhere in the industry. This will require the government to define relatively specific commitments to complement the pool of money made available through Project BioShield.

In this model, market forces would guide private-sector efforts and risk-taking towards well-defined objectives, rather than depending entirely on government experts to select winning strategies. As is the case today, companies could license technology from university or government laboratories or depend on internal R&D, or all three. For such incentives to work over the time frame of drug and vaccine development, they must be credible, predictable and relatively immune to the vagaries of political influence. By consulting leading pharmaceutical and biotechnology innovators and their investors the government can develop a realistic understanding of how procurement innovation, such as a guaranteed purchase program, can result in the long-term engagement of such firms in bioterrorism research.

Concern regarding product liability risk in an environment as unfamiliar as bioterrorism is another important factor that deters investment in products that could be used to counter terrorism. These concerns are most deeply held by the companies with the most to lose, namely, the largest and most successful innovators and the handful of large, healthy companies with substantial sales. If the private sector is to engage in this battle, the liability issue cannot be ignored—and this observation applies to firms working in a broad variety of markets extending well beyond the biosciences.

Physical Approaches to Defense Against Bioterrorism

While the discussion thus far has dealt with medical or biological defenses against bioterrorism, there is also an important role for other approaches involving the physical sciences. To be harmful, a biological agent must reach its intended victim; however, in today's world, many of the most attractive targets for bioterrorism are cities with their large concentrated populations spending much of the time indoors. Many buildings already provide their occupants with filtered air since filters are a part of every heating, ventilating and air conditioning system. These filters can be upgraded to greatly reduce the level of airborne biological contaminants. Upgrading to the highest commercial grade provides a concomitantly high degree of protection. Similar measures are possible for individual homes, and more advanced filtering capabilities can be developed.

Filtering and other physical methods—such as safe rooms—have an important strategic advantage over purely biological defenses. Filtering methods can be devised which will stop almost all particles larger than a specified size. If the particle is, for example, an anthrax spore or similar particle, the same filter will stop all such particles; however, each may require a different medical approach, and as the characteristics of the agent may not be known in advance, that medical approach may not be available. In addition, if filters are always in use, they provide automatic protection in advance of detection.

1.2 Food and Water Security

A national readiness strategy must account for food and water security issues since these systems present avenues through which biological or other attacks on citizen health can occur. Further, such attacks may not require the high level of coordination and investment demanded of terrorists instigating many other types of attack. As such, the vulnerabilities in the U.S. food and water systems, including the "gaps" in existing scientific knowledge of the many biological and chemical "agents-of-concern," need to be addressed. In particular, the need exists for an in-depth, research-based understanding of the biological and chemical agents that could potentially be introduced into the food or drinking water supplies to harm Americans, create chaos in distribution and severely damage the U.S. economy. Plans for responding to the advent of such an occurrence also need to be put in place prior to such an event becoming a reality.

The Potential Agents

While some agents-of-concern are well characterized in isolated form and their behaviors and effects understood under certain conditions, a dearth of knowledge exists about their effects on human health and about the effects of existing production technologies on these agents in food systems. For example, while the retort process successfully inactivates certain agents, it is uncertain whether the traditional pasteurization process will be adequate to neutralize certain other agents and, if not, what measures would be needed to eliminate the related biothreats.

Relevant Assets

The Food System

Because of the vastness of the U.S. food production and distribution system, the potential exists for a massive food-borne disease outbreak to occur. The American consumer's penchant for minimally processed, ready-to-eat foods, such as packaged fresh-cut lettuce, and the increasing availability of these products, poses a growing challenge—especially when intentional and widespread contamination by terrorists is a possibility. In addition, the food supply is increasingly being imported. Rapid, near real-time methods for sampling and testing for microbes, toxins and poisons are essential.

Agriculture

The supply chain for food products introduces yet another set of vulnerabilities. The insertion of a plant or animal pathogen into our food supply could greatly increase the costs of certain food products and severely disrupt the food supply. For example, a foot-and-mouth disease (FMD) outbreak or widespread *Actinobacillus pleuropneumoniae* (APP) infection in pigs could dramatically reduce the supply of animals for processing. The presence of a toxic substance integrated into the edible portion of a single field or fruit crop not only eliminates that site as a near-term food source, but also casts doubt upon the safety of the entire supply and requisite control measures.

The Water System

There have been public reports of attempts to contaminate water reservoirs with agents-of-concern, including pesticides. In addition to enhanced physical security systems, rapid real-time analytical systems need to be introduced on a much wider basis. The advanced technological capabilities of industries that depend on highly purified water should be assessed and leveraged to help address the security of public water systems. Fortunately, the sheer volume of the water supply provides some degree of inherent protection, making it difficult for an attacker to introduce sufficient quantities of an agent to mount an effective attack on any given system or to attack multiple water systems simultaneously.

Research to Build the Necessary Knowledge Base

The overarching goal of comprehensive food and water safety research must be to prevent the entry of pathogens and toxins/poisons into food and drinking water supplies and to control hazards by inactivation or removal as necessary. Given the current status of scientific knowledge, the following areas of research should be given high priority:

- Development of novel processing technologies to inactivate pathogens and toxins, particularly for "fresh-like" ready-to-eat foods. Research shows potential for irradiation, high-pressure processing and pulsed-electric-field (PEF) treatment.
- Development of rapid/real-time methods to detect known and emerging human pathogens, toxic substances and other biological and chemical agents-of-concern throughout the food and water chain. Applications of biosensors and nanotechnology have great potential for this purpose.
- Development of predictive models for risk assessment and response to agent/food combinations with a "high" vulnerability. This would require collecting and assessing information from sites throughout the food distribution chain all the way to the consumer.
- Development of new or improved technologies to create plants and animals that are resistant to agents-of-concern, utilizing where appropriate genetic modification methods that provide cost-effective, sustainable varieties. In parallel, technologies to protect animals from agents-of-concern should be developed, including the creation of strategic reserves of effective vaccines that can be mobilized for protection of the food supply.
- Development of probiotics or "positive control organisms" that have antagonistic or neutralizing effects against agents-of-concern. A probiotic agent would operate naturally to counter or neutralize a given threat agent but must be carefully utilized as it would introduce a new biological agent into the host system.

- Development of a better understanding of the oral exposure (versus inhalation or ingestion) infectious dose and human health effects of agents-of-concern. In these cases, allergens should be evaluated as well as the agents more commonly addressed in this context.
- Development of a better understanding of the microbial ecology and stability characteristics of known and emerging human pathogens and hazardous substances in food ingredients and products in order to enable food processors to design product formulations and processing treatments which will inactivate pathogens and toxins.

1.3 Helping People Protect Themselves

As has been noted, leadership in response to terrorism must come largely from government. However, in this war, as in others where civilians become targets, there is a great deal that individual citizens can do to protect themselves. As one of its highest priorities, a national readiness strategy must include informing these individuals what to do—or to avoid doing.

The possibility that attacks could involve the use of weapons of mass destruction such as chemical and/or biological weapons, or some form of nuclear or radiological weapon, has been made clear to our nation's citizenry, and while there is much that individuals can do to improve their chances of survival, there has been little involvement in self-defense on the part of the general public to date. This is not likely to change unless something happens to increase substantially general awareness of:

- The nature of the danger we face from terrorist use of weapons of mass destruction, and
- The specific steps people can take to improve the chances of survival for themselves and their family.

If civilians can be made aware of the importance of self-protection, it will not only lead to the purchase by the public of civil defense items, such as filter masks, safe rooms or emergency kits, but also it will create a demand for protection in office buildings and in the workplace. These demands would provide an incentive for further improvements through research and development conducted in the private sector and academia.

However, in order to stimulate public demand, people must have confidence that there are meaningful things that they can do for themselves to improve their chances of surviving a terrorist attack. They also must believe that they are not wasting their resources on ineffectual measures based on alarmist advice. Citizens who do not expect fires in their homes nonetheless purchase fire extinguishers based on common-sense risk/benefit judgments. The same can be true of defenses against terrorist actions. Guidance needs to be provided on how various threat levels should prompt different individual self-protection responses.

In the following section examples are provided to illustrate that there is much that can in fact be done. Many of these preventive measures are similar to the preparations for natural disasters that are commonplace for people who reside in areas vulnerable to flood, windstorm, earthquake or wildfire. However, there are special features that distinguish terrorist attacks with weapons of mass destruction from natural disasters—such as the presence of nuclear radiation or pathogens.

Consequences of an Attack

One likely outcome of an attack with weapons of mass destruction is disruption of essential services for a substantial period of time. If many people are injured or killed, if they stay home instead of going to work, if they are unable to get to work, or if they leave an affected area, many essential jobs will not be performed. In addition, large areas may become contaminated or damaged, leaving them inaccessible for significant periods of time. It may not be safe even to go outside. Such conditions could lead to widespread fear of pursuing normal routines. Thus, it becomes necessary to ensure that people have clean air, clean water, clean food, and credible information, in a timely way.

Planning and Access to Information

It is important to create plans for families, businesses and schools that specify what actions to take and how to communicate in the event of an attack. In order to do this, the public needs to know what to expect and how to respond at different threat levels and to various kinds of attacks. This is a key role of government, especially the federal government.

If the electricity supply has been interrupted, radios and computers that depend on central power will not run. Lights will go out. Many furnaces will cease to function. People need to be prepared at home and at work. One key measure is having battery-operated radios available to ensure information flow. Another is to have operating flashlights and extra batteries for the flashlights and for anything else that needs battery power to operate. Each family will need its own communications plan, including prescribing meeting locations and designating a third party contact point in a different, and perhaps remote, location.

Essential Supplies, Including Food and Water

Citizens should be provided with credible guidelines to ensure adequate preparedness. For example, the home and workplace should have a supply of water, food and other ordinary items to last at least several days. In addition, more specialized items such as medicines, antibiotics and foods for infants need to be provided. Having these and other items at home makes it possible to feed and preserve a family, even in the face of a stoppage of many public services. In addition, in the event a contagious pathogen is involved, this preparation makes possible a "stay-at-home" strategy. This strategy of providing emergency supplies for one's family, when widely adopted by the general public, reduces the need to make panic trips to the super market and gas stations, thereby reducing the likelihood of contagious contact if biological agents are part of the emergency.

Protection from Airborne Pathogens

Personal biodefense measures often require applying common sense to uncommon situations. It is a very important and largely neglected point that, in the long term, physical methods aimed at barring pathogens from entering the body must play a major role in both home and workplace bio-defense measures, in part because of the fundamental difficulty of applying medical procedures against an arbitrary pathogen once it has entered the body.

Much of the spread of pathogens is through the air. In any building where there is central air, the highest-grade commercial air filters consistent with the system's design should be installed. Possessing air-filtering devices, such as filter masks and portable filter fans, can be essential. Fans and masks reduce the chance of infection, and masks can limit the spread of a contagious pathogen. Citizens need to be told what devices are appropriate and when they should be used. They should be trained to wash their hands frequently in a biodefense emergency. Simply washing hands is a basic sanitation measure, but may save many lives.

Creating Civilian Demand

There are important and straightforward actions that individuals can undertake immediately that will affect their probability of survival—and they can be accomplished with currently available and generally affordable technology. In the long run, all these steps can become more sophisticated and rely on more advanced technologies—special materials for safe rooms, improved filters and masks and numerous other items. For example, filters that produce diminished pressure drops make them affordable for a wider range of buildings. Other examples include developing filters that protect against chemical as well as biological attack, utilizing ultraviolet light to kill airborne pathogens, etc.

Given that there are simple and effective steps that individuals can take, the question becomes how to create civilian demand that will bring market forces and individual judgment to bear. To motivate action by individuals, the greatest need is to convey the fact that there are things that individuals can and should do for themselves and their family. This calls for a continuing campaign that is aimed at training and empowering citizens. It should be centered on a high-level message that is short and to the point, that explains that you can help yourself and that it is your duty to yourself, your family and your country to take action. Additionally, the message should point to where more detailed instructions about what to do can be found. For example, phone numbers to call for information and assistance, brochures that are available and distributed through post offices, and web sites with information that is specific and useful. The emphasis should be on practical actions. The goal must be to train and empower citizens, and to avoid frightening them. In this regard, it is of the utmost importance that when the government refers citizens to a particular source of information, that the source be of high quality.

National Information Network

To keep responders and citizens informed, resources from federal agencies should be combined to create a national information network. The network should contain selected information on the various types of threats and infrastructure status. The information should first be catalogued, then filtered by private, public and government organizations, and then made available to the general public and to organizations that have a need to know. (See, for example, the comprehensive DHS web site at *www.ready.gov*.)

1.4 Public Health Systems

In terms of public health readiness, the federal government needs to work at two levels to combat the public health threat to our nation posed by certain kinds of terrorist activity. First, it must promote public and community readiness through specific programs and public awareness campaigns. Second, it must assure readiness and cohesive action in our private medical and public health systems throughout the country.

Terrorist weapons producing severe destruction or disruption (nuclear, radiological, chemical, biological and high yield explosives) present a public health threat and a unique medical pathology. Large-scale, purposefully visible acts designed to maim and kill civilians as well as engender fear, anger, insecurity and even despair in those watching from far and near is a concept heretofore largely outside the experience of most Americans. For the most part, research that would relate to bioterrorism has been the domain of the military or law enforcement agencies and their commercial contractors. The knowledge base and expertise in nuclear or radiological threats, biological weapons or chemical attacks have generally not been found within the life sciences community, universities or even the federal health science agencies.

Although for decades specialists in weapons of mass destruction, mostly within government, have worked extensively on countering biological, chemical, radiological and nuclear threats, the medical communities had little interest in these challenges prior to September 2001. Thinking beyond natural forces or human error as the agents of disaster is alien to the humanitarian temperament that drives most life scientists and medical researchers. Combating terrorism as a threat to public health therefore entails involving both medical and life sciences communities, as well as the public at large in an essentially new kind of activity.

Such involvement demands knowledge expansion. Since terrorism, using weapons of mass destruction, has simply not been part of medical thinking, there is, for example, little knowledge about how to deal with an immediate assault by a poison gas, the suspicious mindset to imagine that a mysterious emerging epidemic might be from an organism intentionally and clandestinely introduced into the population, or the understanding to handle the long-term fear instilled by extensive exposure to excess radiation from a dirty bomb that would impose its damage years later in the form of substantially higher cancer risk.

Our nation's senior government officials can provide the leadership and the inspiration for the public to take the practical initiatives to prepare itself for the adverse health consequences of attacks. High-level mobilization of scientific and medical resources of the nation on behalf of public health and well-being is a crucial message that will hopefully engage the public's own participation.

Developing Required Capabilities

Developing these special capabilities within the Public Health Service and the biomedical research and practice community at large must become a sustained priority and will require a kind of strategic analysis with planning and timetables that is not customary in the life science fields. Impediments may be as broad as cultural barriers or organizational constraints and as specific as lack of sensors or therapeutics. Only targeted, focused basic and applied research with urgency and bottom-line orientation to achieve specific goals and create an expert talent base will close the enormous gaps in our know-how in the required time frame.

Surge capacity for medical, technical and scientific help on the scale that would be required at the time of a major homeland attack is generally lacking in today's medical service and university systems. Privatization and market discipline have eliminated excess capacity. Moreover, knowledge is lacking in the care of victims of nefarious attack including decontamination, triggers for isolation or quarantine, or mass public health response with drugs or vaccinations. Peacetime scarcity of blood and other biologics, like immune globulins, forebode inadequate preparation for large numbers of civilian casualties. Moreover, we have little understanding of the psychological consequences of terrorism on our citizens—widespread fear, depression, anxiety and despair—and its impact on the individual segments of the population necessary to sustain a long-term war effort. The recent sniper attacks in the Washington, DC area are an example of how even highly limited terrorist-like acts can psychologically affect the citizenry.

Initiatives

1. Health and Life Sciences Research Centers and Education Programs

Strategic centers of knowledge development and education should become an accepted component of biomedical and life sciences research and development to counter weapons of large-scale destruction and disruption.

By establishing ten or twenty sites at strategic locations in existing institutions of research and education, funded by CDC and DHS, the federal agencies could tap into nationwide expertise to combat terrorism. This Centers of Excellence approach has been very successful at NIH and has fostered the dissemination of critical health know-how, as well as the establishment of institutional resources throughout communities nationwide.

These national preparedness centers would focus on basic and applied research linked to specific strategic goals relating to public health: response to and mitigation of adverse events, and eventual recovery. They would encompass multiple disciplines, including a full range of human needs—air, water, food, animals, plants, as well as general human health. Research proposals and projects would be peer reviewed and would rely on a DARPA-like research and development model of clear strategic goals, timelines and regular progress reports. This would involve contract research instead of the research grants now common in life sciences and medical research.

A public-private advisory board comprised of distinguished experts and public members would oversee the network of preparedness centers to assure coherence and avoid duplication of efforts. The advisory board and the centers would provide a readily accessible source of medical and scientific advice. The staff of the centers would be held to high standards of confidentiality, as needed, and have security clearances so they can contribute in sensitive areas.

A national public health and life sciences research and education program also needs to be developed to complement the proposed centers. The program should be structured to attract some of the nation's "best and brightest" to careers in public health and to assist in funding their education. The nation has long invested in the education of its military professionals because of the public service nature of their careers. A similar investment should be made to provide for the training and education of the individuals needed for defense against terrorist threats to our homeland and its citizens.

2. Strategic Public Health Stockpiles for Implementation of the Federal Response Plan
The Federal Response Plan, codified by the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law 93-288, as amended), lays out specific responsibilities for federal action across the government in the event of a catastrophic national emergency. The plan calls for functions that require materiel that may not be readily available in the event of massive civilian attacks.
[Note: Under the Homeland Security Act of 2002, Title V, Section 507 requires the Federal Emergency Management Agency, now part of DHS, to revise the Federal Response Plan.]

The Homeland Security Council, DHS, DHHS, the Public Health Service, Centers for Disease Control and Prevention, the Federal Emergency Management Agency (with its strong regional presence), the Veterans Administration, the Armed Services and the Federal Bureau of Investigation (FBI), must act in concert to assure that strategic public health assets are available to respond to a catastrophic terrorist event. The public expects that these assets will incorporate the latest technology appropriate and effective for any situation. First responders depend on access to these resources and the public will take comfort in knowing that these reserves, renewable and current, are available.

The government maintains a pharmaceutical stockpile part of which was deployed in the aftermath of the September 11 terrorist attack. Other critical therapeutics should be added or developed for the medical therapeutic stockpiles. These would generally include strategic reserves of frozen and liquid blood, frozen platelets (in development), bone marrow, supplies of intravenous immune globulin, and other biologics including a range of vaccines and diagnostic tests critical to a rapid response to major civilian attacks.

These biologic stockpiles present a unique challenge in that they must be regularly refreshed and should be upgraded to reflect the latest science and technology. Many of these products are already known to be in short supply—such as blood and immune globulin—and reserves must be created that do not deprive other patients seeking care from obtaining life-saving therapies. The means must be developed to maintain stability of supply so that a critical scarcity does not occur elsewhere. Applied research and collaboration with industry are critical to assure that necessary high technology public health stockpiles are available to professional healthcare workers and to those they serve.

3. A Public Health Reserve Corps

A nationwide civilian network of health and medical responders needs to be created and specifically trained to respond to massive terrorist attacks. They should be involved in performance of the applied research, the provision of scientific and technical advice and the conduct of modeling exercises. Important initial steps have already been taken in this regard. For example, a current network for disaster response exists under the guidance of DHHS. The Office of Emergency Preparedness at DHHS has set up the National Disaster Medical System and its Metropolitan Medical Response System. It functions as a cooperative effort among federal agencies, state and local governments, private organizations and civilian volunteers to help provide medical services after a major disaster that overwhelms local capabilities. If needed, the system is also intended to augment the Armed Services and the Veterans Administration medical systems in caring for casualties.

However, consideration should also be given to the creation of a volunteer corps of highly trained, civilian responders. Elements of that corps could be located in strategic locations throughout the country, be fully integrated into the local and federal response structure, and be compensated like other responders. The corps should accept the obligation to serve in a manner similar to the voluntary military reserve. Rigorous systems analysis, testing, scientifically-driven planning and protocol development would be part of this effort. It is unclear whether our current system has the capacity, the knowledge base or numbers of disciplined and well-trained personnel to serve as the rapid and early responders to major civilian or military casualties from massive terrorist attacks, particularly when highly contagious diseases are present.

4. A Public Health And Scientific Advisory Group

An "at-the-ready" public health and scientific advisory group is also needed to provide advice relating to major decisions that would have to be made by the President and other leaders when responding to situations that could dramatically affect the civilian population.

For example, one of the most visible and crucial decisions that the President might have to make in the event of a biological attack that poses a national threat would be quarantine of large segments of the population. By law, only the President of the United States can take this action. If the President imposed quarantine, it would be a historic Executive Order decision with far-reaching medical, scientific, psychological, legal, economic, ethical and social implications for those affected and for the nation as a whole. Even though quarantine is an inherent part of epidemic containment (as was the case in some countries during the recent SARS outbreak) and is referred to regularly in planning exercises, it remains highly controversial within the public health community. Currently, there is a lack of agreed on scientific guidelines for when to quarantine or who should be quarantined in a bioterrorist attack. Whatever the guidelines, they should be established based on scientific facts, be planned well ahead of time, and rely on an informed and understanding public.

5. The Psychological Effects of Terrorism

If one accepts the perspective that we are encountering a massive escalation of a new kind of prolonged warfare directed against Americans and our homeland, then the psychological impact of the threats must be confronted. CDC has studied one-time natural disasters and the military has examined post-combat battle stress. Both may result in post-traumatic stress disorders, increased levels of depression and alcoholism among both victims and rescue workers—ills that can persist for years after the event.

Studies suggest that the ongoing threats after September 11 have placed a non-negligible psychological burden on the nation. The RAND Corporation performed a national survey within a week of September 11 and identified substantial stress symptoms in 45 percent of Americans nationwide and some level of stress reactions in almost everyone surveyed. Children were affected as well as adults—most were concerned about their own safety and that of their families.[2]

The mental and spiritual impact of additional major attacks on our soil, especially if associated with extensive casualties, would likely carry with them an even more intense psychological response. Such events would solidify the notion that our nation is at war, is vulnerable, and would raise concerns as to its preparedness. America's determination and resolve will very much be a consequence of the way the majority of Americans handle the stress and anxiety that are part of an even more vivid reality of ongoing physical threats to their homeland.

Understanding and responding to the psychological impacts related to this kind of war on civilians is a medical and public health challenge that begs for research and clinical study to inform practice. In brief, the impact of mass stress and anxiety on a population that has generally been safe is one that cannot be ignored as a public health threat, and may have major implications for high-level policy decisions, including those made by the President and the Cabinet.

1.5 Communications

The need for credible and consistent communication of preparedness and readiness information (addressed in specific contexts in previous sections) is being given increased attention by both federal and state agencies and by nongovernmental organizations. In particular, the coordination of readiness and response communications is being addressed by DHS, which has established a website at *http://www.dhs.gov/dhspublic/* that provides detailed threat-specific information. It is noteworthy that the American Red Cross has also launched a "Together We Prepare" campaign as a vehicle to provide practical disaster preparedness information to the general public. In addition to such preparatory communication, steps are needed to assure that citizens can be promptly warned of an actual radiological, chemical or airborne biological attack when minutes may count.

Appendix 2. Helping Protect First Responders

Local and state first responders, rather than federal emergency teams, will be the primary source of on-scene emergency aid for most terrorist incidents—even those incidents that require additional support from across the nation. The day-to-day business of these teams is conducted in a fragmented organizational environment with very limited means for evaluating acquisition alternatives, conducting research and development, or setting standards and testing equipment. Although their limited resources are sometimes augmented by federal funds, most of their acquisition decisions are made independently. As a result, the local response unit faces many obstacles with respect to equipment compatibility, performance and cost. For day-to-day operations these limitations have a modest impact, but in a major incident they can have a significant impact on first responder effectiveness and safety.

The Nature of Major Terrorist Incidents

Considerable effort has been devoted to assessing the risks and dangers to emergency personnel who are on the front lines in responding to terrorist attacks. Recent studies of the terrorist attacks on New York City and the Pentagon (2001), the Alfred P. Murrah Federal Building in Oklahoma City (1995), and the anthrax incidents occurring on the East Coast (2001), indicate that three characteristics of an incident significantly influence the adequacy of response and the risks to first responders.[3]

- **Scale**—The significant size of these disasters strained the resources available.
- **Duration**—The prolonged recovery from these attacks resulted in a broad range of demands. A two-phased process emerged, the first lasting several days involved urgent rescue activities, while the second comprised a multi-month, sustained recovery campaign.
- **Range of Hazards**—While the most urgent risks in many forms of conventional attacks are initially related to fire, in the above incidents they rapidly progressed to risks associated with massive structural debris and dangerous materials, hazards which frequently exceeded the training and equipment provided to responders.

In such situations the safety and effectiveness of local and state first-response personnel is directly related to prior training, incident management and the availability of suitable equipment. Because of the role of science and technology in providing effective and usable equipment, and because of the potential role that the federal government can play in applying science and technology to this challenge, the Panel has focused on the last of these three factors.

Shortcomings of Current First Responder Equipment

In the events mentioned above, personal protective equipment (PPE) technologies were generally found to be effective when applied to the specific hazardous conditions foreseen in the design and procurement of the equipment in question; however, significant shortcomings were evident when this was not the case. For example:

- Overall equipment suitability under unexpected conditions was poor. Reports of biological/chemical threats resulted in a wider range of potential hazards than responders were equipped to handle. In addition, law enforcement personnel found it particularly difficult to work effectively at crime scenes that were also hazardous disaster sites.
- Lack of "user-friendly" respirator gear severely limited protection. Responders could not assess what hazards were present, equip themselves with the proper gear, and interpret the complex procedures for use of their equipment, while still performing their jobs. Issues relating to filter type, weight, refill and replacement requirements, communication difficulties, physical discomfort, mobility and certification all reduced the likelihood of responders using any protection whatsoever.

- Logistical complications further diminished the use of proper equipment. Most departments ran out of equipment while that which was available frequently malfunctioned or did not have replacements for limited life components (such as filters). Although massive amounts of equipment were supplied on request or were sent voluntarily, use was often limited by a lack of organization, lack of training on the equipment supplied, or incompatibility among various equipment components.

Solution Approaches

The recent studies of the experiences of first responders in terrorist events suggest a number of approaches to providing more appropriate equipment. First responders have indicated that the highest priorities for equipment development should be assigned to respirators that offer both practicality and comfort for extended use, escape hoods with an air supply for emergency medical service personnel, and thinner, yet effective, thermal protection gloves for firefighters. In particular, research and development for future personal protective equipment should strive for higher levels of protection while placing much greater emphasis on making it possible for responders to perform their emergency response duties with a minimum of equipment-related interference.

In addition, techniques for faster and more accurate hazard monitoring should be developed to enable first responders to evaluate environments for themselves or to receive early hazard assessment information. Personal protective equipment selection decisions will require such information as long as equipment that is specific to a single hazard type continues to be used. Broader-spectrum personal protective equipment useful for a range of hazards needs to be developed, particularly for respiratory protection, which is obviously one of the most essential elements of protection. This might best be achieved in stages, with the initial stage being to develop and field equipment with an intermediate level of protection against a wider range of hazards than is now available while still meeting weight, flexibility and decontamination requirements at an affordable cost.

Emergency-response "caches" managed at regional and national levels are needed and can be used to promote standardization. Federal agencies should be required to purchase the same equipment, or equipment that, at a minimum, is compatible with other equipment—unless there are sound and specific reasons for doing otherwise. Cost and logistical considerations dictate that this activity be coordinated with the Federal Response Plan and the Strategic National Stockpile program.

Pre-disaster training should be conducted under more realistic, high-pressure conditions and should include the participation of engineering, construction and transportation personnel. Procedures are needed to permit the communication of accurate hazard information to responders as quickly as the nature of a hazard is determined. Finally, flexible and dynamic procedures need to be developed to insure an effective incident management authority that can quickly establish control at a disaster site, account for individuals working in dangerous environments and assure that the proper personal protective equipment is selected for use.

A Federal Research Role

The above considerations suggest two primary areas in which science and technology can contribute to improvements in protection of first responders: (1) developing equipment (for hazard identification, communication and protection) and (2) establishing technical standards for the equipment.

While advancements in the technological capabilities of equipment are important, research and development aimed at lowering the cost of adequate and useable equipment will probably have the greatest impact on national capabilities because of the large quantities of equipment needed and the budgetary constraints under which most first responders operate. Similarly, while the task of developing

sophisticated new standards can be complex and challenging, the research-based verification of even rudimentary technical standards will ultimately be of great value to local first responders.

Most local emergency response agencies have limited equipment acquisition budgets, since most of their resources are dedicated to meeting personnel costs. This makes it very difficult and inefficient for local or state agencies to conduct or even influence significant research and development efforts. At the same time, the relatively small and fragmented market for personal protective equipment and other emergency response products often does not justify significant R&D commitments by individual private-sector vendors. As a result, the majority of the technology in use by emergency responders today has been transferred from applications developed for other purposes, particularly military use, and technology transfer is believed to be the mechanism by which most future gains may well be made on behalf of this community. However, it is important to note that most defense equipment that could be relevant to operating in hazardous environments (such as a battlefield contaminated with chemical, biological, radiological or nuclear agents) has not been designed to comply with Occupational Safety and Health Administration (OSHA) standards.

DHS should work with NIST, NSA, OSHA and other federal agencies and civilian organizations with expertise in technical standards setting in order to establish programs to verify that products comply with such standards (e.g., ANSI, IEEE and NCSA). This initiative should identify areas where standards are needed and should design and institute a program capable of verifying product compliance that encourages innovation by suppliers, perhaps through the use of independent, objective, third-party, private-sector testing organizations.

Appendix 3. Helping Business Protect Our Nation

Most potential targets of terrorist attack reside in the private sector—the greatest portion of the nation's infrastructure, its commercial and economic endeavors, and most working citizens. Much of the capability to provide technology to counter terrorism is also found in the private sector. It is thus crucial to involve individual citizens, companies, universities and other private-sector institutions in the fight against terrorism. The PCAST Panel on the Science and Technology of Combating Terrorism believes that there is much that can be done in this regard.

The industrial sector can contribute in two important ways to counter terrorism. First, being prepared to maintain the supply of essential services such as food, communications, electricity and financial services following a terrorist attack. Second, providing improved antiterrorist products to local fire, police and other emergency organizations, as well as the federal government and individual citizens. In its first role, businesses will need to provide essential services, such as shipping food into retail markets, providing check-cashing services and, in general, assuring continuity of vital services after a terrorist attack. It is likely that this will involve additional "peacetime" costs, for there is an inherent conflict between the desire to do things at minimum cost and the desire to have resilient systems that have the ability to recover rapidly. These additional costs must be paid by businesses and by consumers, much as costs of greater airport security are paid today.

As noted, much of the nation's research and develoment capacity to counter terrorism resides in the private sector, particularly in industry and in academia. The marshalling of this capacity to provide improved capabilities to counter terrorism is hindered in many instances by the lack of adequate market incentives, by the diffuse character of that part of the market which depends on state and local governments, and by what is widely perceived to be an onerous and burdensome federal procurement

process. These factors particularly hinder pharmaceutical firms (because of their preference for established and profitable alternative markets). The federal procurement process also discourages small- and medium-sized firms, because it is difficult to compete with the economies of scale available to larger firms. While local police departments, fire departments and other first responders who purchase equipment directly from suppliers drive the majority of the homeland security market, the portion that is driven by federal government purchases is not insignificant. Finding new and effective ways for the federal government to engage pharmaceutical firms and small- and medium-sized businesses, such as has been suggested herein, may represent an important contribution in the war on terrorism.

3.1 Security Standards and Recovery Plans

Security standards, recovery plans and the requirements that could be fulfilled by the private sector have been discussed under the previous section on Helping to Protect First Responders. It will be necessary to obtain private-sector consultation and advice in the development and promulgation of security standards, development strategies and recovery plans at all stages to ensure effective implementation.

3.2 Small- and Medium-Sized Businesses

Smaller businesses face considerable challenges as they seek to participate in the nation's program for countering terrorism. In some instances these challenges do not differ from those of large firms; they are simply more difficult because economies of scale required in efficient government contracting are not available to smaller firms, nor do these firms typically have the capital resources and staying-power of larger firms.

One survey has indicated that three-fourths of all small- and medium-sized enterprises believe that they have products or services relevant to homeland defense. Despite this view, less than half of these firms are doing business with the federal government at all, and far fewer are participating in the homeland security initiatives. Of the small- and medium-sized enterprises that are involved in selling to the government, 42 percent report that the process is too bureaucratic, that the sales cycle is too long and that participating in the market is ultimately not sufficiently profitable to pursue.[4]

Smaller businesses are also concerned about the requirements of multiple agency security clearances. There are too many agency security clearances required, each with a separate investigative process. Applying and waiting for duplicative, multiple agency clearances limit the smaller enterprise's ability and willingness to respond to the immediate needs of homeland security.

Small- and medium-sized businesses often believe that current intellectual property laws and regulations are too restrictive and do not facilitate the development of new technologies for homeland security. These enterprises are concerned that if the government contributes funding, the government (or prime contractors) will appropriate ideas and technology or demand an inequitable share of ownership interest and license rights. In addition, many smaller firms consider the "bundling" of contract work to be detrimental to their ability to participate in the procurement process, although others see efficiencies in bundling. What is clear is that it is an approach that requires careful consideration on a case-by-case basis.

Appendix 4. Identity Authentication

Certain types of trustworthy identity authentication systems can be established relying on current technology. Some systems are specialized (for law enforcement officers or first responders at the scene of a terrorist incident; voluntary programs, such as a preferred traveler system; or a pervasive identification application, such as a system for all transportation system operators- pilots, drivers, railway engineers, and vessel captains-or even the general public). However, technological innovations are needed to improve cost efficiency, deployment speed, broader applicability, and reliability of such systems—particularly if they are to be applied on a large scale where even very low false alarm rates are unacceptable because of the large volume of transactions involved.

Because of the long lead time required, it is important to begin research and development now to establish a framework for a reliable large-scale identity authentication system if the nation is to be prepared to deploy such systems in the future. If we fail to explore the necessary science, technology and procedural prerequisites for such a system now, we will have dismissed even the possibility that such a system might be promptly deployed if it were ever concluded that it were in fact needed in the future.

Types of Trustworthy Identification Systems

Trustworthy identification (ID) systems come in many forms. Typically, they have three common components: (1) a register of individuals together with unique identifying information about those individuals; (2) tokens (e.g., ID cards) that carry an identification alphanumeric that can refer back to the register; and (3) a biometric identifier and sensor.

Needed Research

The R&D agenda for technologies that best enable or improve trustworthy identification systems will depend on how such systems are to be used. Critical factors include:

- The circumstances under which an ID card or an alphanumeric can be demanded,
- The extent to which use of the system assumes extensive networking, and
- The integration between trustworthy identification systems and other licensing/identification systems.

These issues can be illustrated by considering two types of trustworthy identification systems. The first is designed primarily to log the passage of people of interest past checkpoints (e.g., borders or airline gates), and to enforce targeted access control (e.g., keeping those on a watch list out of the country). This type of system would use an ID card that is read electronically and is not designed for casual inspection (e.g., by a street police officer). The second is designed for human readability and serves as a broad access control device (e.g., it might be used to detect visa violators).

The first type of trustworthy identification system puts a premium on R&D relating to one particular set of technologies:

- Cryptographic techniques (digital “signatures”) to link an individual with a specific registration transaction (e.g., we know the specific ID in question was issued by an authorized agency because no one else can generate a byte-string that encodes an individual’s alphanumeric code and that of the authorized issuing agency).
- The ability to encode and read enough digital information (a digitally signed alphanumeric) reliably and quickly (much as a proximity card is read in passing through transit turnstiles).
- Security techniques that underlie the chains of authenticity and custody over the cryptographic machinery (to ensure that the digital signatures are valid).

- Processes to make a sufficiently reliable match between the biometric features of the *de facto* holder and the recorded biometrics of the *authorized* card-holder (e.g., someone presents the card to an electronic card reader and a server returns the facial image of the authorized card-holder to a human inspector).
- Secure and reliable networking among the checkpoint acquisition devices (e.g., card readers), the trustworthy identification system data stores (i.e., to validate identity), and the transaction data stores (to record passage of the individual).
- Reliability and backup mechanisms to ensure that no checkpoint lacks functioning card-reading devices.
- Secure database management to ensure that data are not erased or tampered with and that access to data is properly controlled.

The second type of trustworthy identification system places emphasis on another set of R&D tasks. Reliable networking may not be as critical, but the requirement that the card can be authenticated upon inspection means that the authenticity of the card relies on ensuring that its features are easy to validate and difficult to duplicate (e.g., a laser hologram). Technology improvements are continually required to defeat those who would produce false ID documents.

Some issues apply to both types of systems. Biometrics, for instance, would be necessary to ensure that one person is not registered twice. Fingerprints are a proven method for verifying uniqueness, however their historical association with criminal registration may cause people to balk at providing them and they are not usable with a small segment of society which possesses no usable fingerprints. Automated methods of performing fingerprint matching and doing so in near real time have made significant advances but still warrant improvement if they are to be used in high-traffic applications where even low false alarm rates become intolerable.

Questions to be addressed include: Can fingerprint collection systems scale to where they can prove uniqueness within a database of one-half billion people without generating too many false results that a newly offered set of fingerprints is already in the system? If fingerprints are used, must ten prints be collected or would two or four prints suffice? What standards should be used to ensure sufficient print quality? How should the approximately 2 percent of the population that cannot produce a readable fingerprint be registered? Are other biometrics (e.g., iris scans, facial images) ready to be supplements or complements to fingerprints? To what extent can machine-aided techniques (and/or better imaging techniques) help ensure that, for example, facial photographs (or other soft biometrics) maintained in a registry can be matched with the faces of claimed authorized card-holders (as would be the case in situations where asking cardholders to provide fingerprints or other biometrics is not feasible).

Necessary Technical Standards

Standards raise other questions. What performance metrics should be specified for card-reading devices? To what extent should a trustworthy identification system be compatible with those of other countries? Although visas can be incorporated in a trustworthy identity system, what set of performance and design criteria should be negotiated with those countries currently part of the visa-waiver program (assuming their citizens are not to be registered *de novo*)? How will cases of identity mismatches be handled (e.g., when preparing to board an aircraft or enter the country)?

Finally, there are issues associated with the introduction of any new system. For example, what techniques can be used to reduce the costs and expedite the rollout of (1) identity cards, (2) card-reading devices, (3) secure reliable information networks, and (4) biometrics and transaction servers?

Now is the time to accelerate research into these areas to preserve the option to rapidly implement a robust system of personal identification in the future should circumstances require.

Appendix 5. Cyberterrorism Threats and Countermeasures

Cybersecurity, particularly that designed to counter cyberterrorism, is a critical but complex challenge. It touches all infrastructure sectors and spans national security, homeland security, law enforcement, civil rights and commercial and other private-sector interests. Any improvement in cybersecurity will require unprecedented cooperation between government and private entities. Additionally, the pace of technological advance in the cyber field compounds the problem. There are no easy solutions, and there is little historical precedent to guide our efforts to improve cybersecurity while balancing other interests and considerations. Further, cyber attacks might be initiated in conjunction with other forms of attack in order to complicate response and recovery.

The security and infrastructure assurance structure set up under DHS includes the National Infrastructure Protection Center (NIPC), the Critical Infrastructure Assurance Office (CIAO), and the industry-centered Information Sharing and Analysis Centers (ISACs), and has provided much of the organizational framework for cybersecurity to date. The approach for countering cyberterrorism is articulated in The National Strategy to Secure Cyberspace, released in February 2003.

Two efforts typify the work that has been conducted to provide an operational cybersecurity capability. The first centers on efforts to develop a cyber warning and information network (CWIN) envisioned to be a federal government program that would be available to selected private organizations. The second is the Computer Emergency Response Team (CERT) and its Coordination Center (CERT/CC), whose work focuses on protecting private, commercial and government cyber systems. It includes responding to computer security incidents, publishing security alerts, conducting research on vulnerabilities and developing the security changes needed in networked systems. CERT also publishes research and training materials on cybersecurity. The center is funded by the federal government and is managed by Carnegie Mellon University.

While it may be argued that these structures could improve warning capabilities to the extent that terrorist cyber attacks can be thwarted, many experts point out that the most important threats (sophisticated attacks by organized, well-funded adversaries such as nation states or major terrorist organizations) will most likely not be able to be detected until after they occur. In many or most instances warning systems are unlikely to be effective, even with a significant increase in intelligence collection efforts. This points to the need not only to develop a substantially increased capability to respond to attacks once they are taking place, such as provided by CWIN and CERT, but also to advance research into new tools and techniques, such as immune systems that would minimize the effects of an intrusion once it is detected.

It is important to note that reliable information concerning the cyber threat is very limited. While private-sector firms undertake internal assessments of attacks that threaten substantial business interests, the results are understandably rarely made public. In recent reports, even private-sector firms specializing in marketing such data have indicated that existing indicators have substantive limitations and that they are mainly “suggestive.”

With the enactment of the Cyber Security Research and Development Act (H.R. 3394), and the issuance of The National Strategy to Secure Cyberspace, the federal government has set forth a near-term course of action to organize cybersecurity efforts. The recommendations include:

(1) Establishing a mechanism to ensure inter-agency coordination of relevant research and development programs;
(2) Establishing a flexible test bed to assess the scalability of particular security measures;
(3) Expanding efforts recommended in the National Strategy on the international level, with an emphasis on cooperative research and development among governments and industry; and
(4) Developing a set of standards against which companies, as well as government, can be measured as an indicator of how secure their cyber systems are.

Since cybersecurity is intimately entwined in almost all forms of terrorism response as well as in many forms of terrorist attacks, it can be best addressed with the agency that oversees other forms of terrorist threats, namely, the Department of Homeland Security. This implies a massive coordination task on the part of DHS...but so too does the conduct of virtually all of its other responsibilities.

Appendix 6. Detecting Nuclear Weapons

The United States has made significant investments in research and development that support the prevention of nuclear proliferation and the management of nuclear emergencies involving complete weapons or nuclear materials (plutonium and enriched uranium). These investments have provided a technological infrastructure that supports national security needs in proliferation monitoring; nonproliferation assurance; nuclear weapons and special nuclear materials stewardship; as well as management of emergencies involving nuclear weapons or special nuclear materials.

The technical challenges arising from nuclear or radiologic terrorism share common foundations and scientific goals with global proliferation monitoring, surveillance of items crossing U.S. borders, and environmental monitoring of urban areas for the presence of nuclear materials and radiologic threats. Currently systems for proliferation detection and deterrence address goals such as identifying the origins of foreign nuclear materials, monitoring global fissile material production, monitoring both bilateral U.S./Russian warhead dismantling and cooperative threat reduction, countering nuclear smuggling, and enhancing international fissile material safeguards.

Nuclear Weapons

While the security of U.S. nuclear weapons is considered to be assured, the security of the growing number of nuclear weapons and nuclear materials in some foreign countries is much less certain. The possibility of a weapon falling into terrorist possession through theft or "sale" cannot be overlooked. Important initiatives to reduce the global nuclear threat (e.g., the ongoing U.S./Russian bilateral agreements) should result in consolidation of at least some weapon materials and device stockpiles into facilities with higher levels of security. The United States is working with other declared weapon states that have shared interests in security and safety and these joint efforts can be expected to have similarly positive effects. Nonetheless, the proliferation of nuclear weapons around the globe coupled with the potential impact of such weapons in the hands of terrorists makes this threat worthy of extremely high priority research and development efforts to detect the presence of such devices.

Improvised Nuclear Devices

The development and deployment of an improvised nuclear device requires expertise, appropriate materials, equipment and facilities, and a means of delivery. The Nonproliferation Treaty has been the international mechanism to safeguard nuclear material and to control the distribution and export of nuclear technology. Nevertheless, the possibility of terrorist organizations acquiring, *or claiming to have acquired,* these elements cannot be dismissed.

Radiological Dispersion Devices

The dispersion of quantities of radiological material (e.g., ^{60}Co) by detonation of high explosives constitutes a radiological dispersion device (a "dirty bomb"). It is also possible that a failed detonation of an improvised nuclear weapon may spread hazardous radioactive material over a relatively wide area. Although a radiological dispersion device could present a significant hazard, the likelihood of acute and immediate health impact on large populations is low. The fear of exposure to radiological materials, and the health and economic consequences engendered by that fear, will nonetheless exist. The dispersal of radiological materials in public places is likely to cause significant societal and economic disruption, and the affected public health and medical communities will be stressed to provide needed care. Procedures to monitor marginally exposed members of the public need to be put in place, as have already been discussed herein, to build confidence and to reduce concerns from this "invisible threat" to health and life.

Other Potential Radiological Incidents

Other incidents involving intentional dispersal of radiological materials into populated areas also must be addressed in planning the nation's overall counterterrorism program. These incidents could involve airliner attacks (possibly multiple attacks) on a nuclear facility or efforts to acquire nuclear or radiological material in storage or in transport. Radioactive materials are already widely used in our economy, are stored in many locations and are frequently moved.

Economic Impact and Challenges

The immense number of shipping containers entering the United States daily presents an enormous challenge. Approximately 6 million cargo containers enter United States ports each year and another 12 million cross by land. This results in approximately 16,000 containers coming into seaports each day and 33,000 per day by land. While it would be desirable to screen every container coming into the United States, less than 2 percent of incoming containers are presently inspected because of the time required to examine containers and the resultant increase in the cost of shipping and reduced throughput.

There are a number of challenges that must be faced: (1) the development of faster and more accurate inspection equipment (Containers currently inspected are subjected to x-ray image technology and the image must be interpreted by an inspector. No reliable computer software is currently available to automate this task. Suspicious containers must be opened and visually inspected.); (2) the provision of space to locate inspection equipment at seaports—space which is scarce and expensive; (3) the difficulty when using radiation detection techniques of finding nuclear materials that are shielded; and (4) the fact that, even if ideal screening equipment were available, it would take a number of years to install the equipment and train the necessary personnel.

The solution to these dilemmas will probably be a combination of a "trusted shipper" program, profiling of high-risk containers, installation of multiple-method inspection equipment and increased personnel at the point of origin as well as at the destination.

In order to reduce the nation's vulnerability to the possibility of imported nuclear materials or devices, the Panel recommends a major expansion in research and development on systems for detecting nuclear devices and materials.

Appendix 7. PCAST Panel and Support

Members of The PCAST Panel on Combating Terrorism

Norman Augustine	*Former Chairman and CEO, Lockheed Martin Corp. — Panel Chair*
Charles Arntzen	*Director, Arizona Biomedical Institute, Arizona State University*
Kathleen Behrens	*Managing Director, RS Investments*
G. Wayne Clough	*President, Georgia Institute of Technology*
Ralph Gomory	*President, Alfred P. Sloan Foundation*
Bernadine Healy	*Medical Senior Writer and Columnist, U.S. News and World Report, Former President and CEO, American Red Cross, Former Director, National Institutes of Health*
Bobbie Kilberg	*President, Northern Virginia Technology Council*
Kenneth Nwabueze	*CEO, Sagemetrics Corporation*
Steven Papermaster	*Chairman, Powershift Ventures*

Acknowledgements

The White House Office of Science and Technology Policy provided technical and administrative support in the preparation of this report.

The Science and Technology Policy Institute at RAND, a Federally Funded Research and Development Center sponsored by the National Science Foundation in support of the White House Office of Science and Technology Policy provided analytic support for this effort under the direction of Dr. Bruce Don.

The Panel benefited greatly from discussions with the leadership of the National Academies' Committee on the Science and Technology for Countering Terrorism and from their report, "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism."

As the Panel's deliberations were held during the formative stages of the development of the framework for the Department of Homeland Security, briefings by numerous government agencies provided background to help the Panel assess the status of ongoing and planned work relevant to combating terrorism and homeland security in the federal science and technology infrastructure.

The Panel is also grateful to the many nongovernmental organizations that provided reports on studies relating to terrorist threats and scientific and technological approaches to countering them.

All findings and recommendations are those of the Panel and of the PCAST.

References

[1] Committee on Science and Technology for Countering Terrorism, National Research Council of the National Academies, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington, DC: The National Academies Press, 2002).

[2] M.A. Schuster, B. D. Stein, L. H. Jaycox, R. L. Collins, G. N. Marshall, M. N. Elliott, A. J. Zhou, D. E. Kanouse, J. L. Morrison, S. H. Berry, "A National Survey of Stress Reactions After the September 11, 2001, Terrorist Attacks," *New England Journal of Medicine* 345, no. 20 (15 November 2001): 1507-1512, summarized in "After 9/11: Stress and Coping Across America," available from < http://www.rand.org/publications/RB/RB4546/>.

[3] This assessment is based on a number of sources. First, a conference held in New York City from December 9 to 11, 2001 that was sponsored by the National Institute of Occupational Safety and Health (part of the CDC) on behalf of the White House Office of Science and Technology Policy. Conducted by the Science and Technology Policy Institute at RAND, the workshop provided a comprehensive review of the experiences of emergency personnel regarding recent homeland terrorist attacks. Second, this assessment draws from a series of workshops conducted by RAND during the summer of 2001 for the Office of Homeland Security. This series of seven workshops examined critical infrastructure protection—including the protection of first responders and other emergency management personnel and functions.

[4] From a recent survey by the Northern Virginia Technology Council and The Potomac Tech Journal.

President's Council of Advisors on Science and Technology • July 2003

www.ostp.gov