

The Fourth Annual Report to the
President and the Congress of
the Advisory Panel to Assess
Domestic Response Capabilities
for Terrorism Involving
Weapons of Mass Destruction

IV. Implementing the



National Strategy

The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction was established by Section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105–261 (H.R. 3616, 105th Congress, 2nd Session) (October 17, 1998). That Act directed that a federally funded research and development center (FFRDC) provide research, analytical, and other support to the Advisory Panel during the course of its activities and deliberations. RAND has been providing that support under contract from the Department of Defense through one of its FFRDCs, the National Defense Research Institute, since the Advisory Panel's inception.

This Fourth Annual Report to the President and the Congress is a document of the Advisory Panel, not a RAND publication. It was prepared and edited by RAND professional staff and is being submitted for review and comment within the U.S. Government Interagency process. It is not copyrighted but does contain material from copyrighted sources. Copies of the report may also be obtained via the Internet at: <http://www.rand.org/nsrd/terrpanel>

About RAND

RAND's mission is to improve policy and decisionmaking through research and analysis. Though RAND confronts different policy challenges over time, its principles remain constant. RAND research and analysis aim to:

- Provide practical guidance by making policy choices clear and addressing barriers to effective policy implementation.
- Develop innovative solutions to complex problems by bringing together researchers in all relevant academic specialties.
- Achieve complete objectivity by avoiding partisanship and disregarding vested interests.
- Meet the highest technical standards by employing advanced empirical methods and rigorous peer review.
- Serve the public interest by widely disseminating research findings.

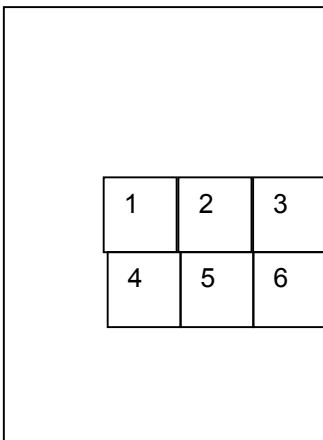
**FOURTH ANNUAL REPORT TO
THE PRESIDENT AND THE CONGRESS OF THE
ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE
CAPABILITIES FOR TERRORISM
INVOLVING WEAPONS OF MASS DESTRUCTION**

***IV. IMPLEMENTING THE
NATIONAL STRATEGY***

15 December 2002



PHOTO CREDITS FROM COVER PAGE



1—Recruits prepare to battle a simulated fire in a Fairfax County, Virginia, Fire Department training exercise. Photo courtesy of Fire and Rescue Department, Fairfax County, VA

2—FEMA/NY State Disaster Field Office personnel meet to coordinate federal, State and local disaster assistance programs. Photo by Andrea Booher/FEMA News Photo

3—New Mexico Urban Search and Rescue team leader discusses shoring methods with team during exercise. Photo by Andrea Booher/FEMA News Photo

4— Police Special Operations Unit during a VX Nerve Gas terrorist attack training exercise in the city of Glendale, California. Photo courtesy of Graham Owen, photographer, www.grahamowen.com

5—Firefighters being decontaminated at an exercise of responders in Gadsden County, Florida, to test the Terrorism Annex to the county's Comprehensive Emergency Management Plan. Photo courtesy of Capital Area Chapter, American Red Cross

6— NY-TF1 Incident Support Team Medical Unit Leader coordinating with local hospitals for triage of patients during exercise. Photo by Kevin Molloy/FEMA News Photo

THE ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION

James S. Gilmore, III
Chairman

L. Paul Bremer

George Foresman

Michael Freeman

William Garrison

Ellen M. Gordon

James Greenleaf

William Jenaway

William Dallas Jones

Paul M. Maniscalco

John O. Marsh, Jr.

Kathleen O'Brien

M. Patricia Quinlisk

Patrick Ralston

William Reno

Joseph Samuels, Jr.

Kenneth Shine

Alan D. Vickery

Hubert Williams

John Hathaway
U.S. Department of
Defense Representative

Michael Wermuth
RAND Executive
Project Director

Jennifer Brower
RAND Co-Project Director

December 15, 2002

To Our Readers:

I am pleased to provide this *Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*. The Advisory Panel was established by Section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105-261.

In the fifteen months since the murderous terrorist attacks were perpetrated on American soil, our nation has undergone a transformation. Citizens, governments at all levels, and the private sector continue to adjust to the new threats of terrorism. The effects of September 11, 2001, continue to reverberate throughout America and the World. Some are profound. Others are more subtle.

Considerable progress has been made by an international coalition of countries committed to eliminating the reach and ability of terrorists to inflict wanton destruction targeted against economies, societies, and people. We recognize that the risk will never be completely eliminated. Efforts to enhance preparedness have moved forward so that we can act decisively when attacks inevitably occur. It is clear, however, that actions designed to respond to terrorist attacks; whether conventional, cyber, or those involving weapons of mass destruction, require continuing attention. Achieving a more secure America requires that, as a nation, we better understand the risks we face, and structure the best and most comprehensive ability to prevent, respond, and contain terrorism in the Homeland.

The Advisory Panel was guided by five overarching conclusions this past year:

1. ***The threats we face are not diminishing*** – As the pitch of conflict escalates, the threat of an attack on the Homeland is increasing. We must accelerate the pace of preparation to prevent, respond to, and contain an attack.
2. ***Intelligence and information sharing has only marginally improved*** – Despite organizational reforms, more attention, and better oversight, the ability to gather, analyze and disseminate critical information effectively remains problematic. The best vehicle must be found to perform the counter-terrorism function and to share information between Federal agencies, the states and localities, and elements of the private sector.

Please address comments or questions to:

RAND

1200 South Hayes Street, Arlington, Virginia 22202-5050 Telephone: 703-413-1100 FAX: 703-413-8111
The Federally-Funded Research and Development Center providing support to the Advisory Panel

3. ***Federal structural changes alone will not significantly improve the security of the homeland*** – The current reorganization in the Federal executive branch will not be a panacea in countering the threat posed by terrorists. In fact these current changes must be carefully implemented and additional actions are needed if we are to be successful. It is imperative that a plan to enable state and local response be designed, funded, implemented, and exercised.
4. ***Measuring performance and sustaining efforts will be key to success*** – Billions of dollars are being committed to countering the terrorist threat. A system must be designed to define priorities, set standards, and measure progress to advance real preparedness.
5. ***Protecting democracy and individual liberties is paramount to achieving ultimate victory*** - Coming through this crisis without diminishing our freedoms or our core values of individual liberty is the entire game. If we pursue more security at the cost of what makes us Americans, the enemy will have won.

If we follow an all-hazards approach to Homeland Defense, we can justify the enormous expenditures coming at the Federal, state, and local levels, and in the private sector. A positive dividend can be reaped as we end up with a better ability to respond to natural disasters and a better public health capacity. Above all, we must remain unified in the same resolve and desire for resolute action that permeated every corner of America in the days and weeks immediately following the September 11, 2001, attacks. We must maintain our drive and momentum to prepare America to defend itself.

The Advisory Panel believes that our fundamental call to service is to inform the national debate on how best to achieve greater safety and security for America. The Advisory Panel will now enter our fifth year of service remaining firmly committed to that principle. The leadership of the Congress and the Administration will continue to be essential in implementing the *National Strategy for Homeland Security*, the corresponding structures, and processes that measure success. A Federal strategy is not a national strategy. Our efforts must be accomplished in strong partnership with our states, communities, private sector entities and every citizen. All segments of our readiness must be addressed in a comprehensive and coordinated fashion. All of us together will meet this challenge at this unparalleled time in the history of the United States. When this latest enemy is gone, the United States will remain, and will continue to be the beacon of freedom in a troubled world.

Sincerely,



James S. Gilmore, III
Chairman

CONTENTS

Letter from the Chairman	i
Contents	i
Executive Summary	iii
Chapter I. Introduction	1
Milestones of the Last Fifteen Months	1
Extension of the Advisory Panel	2
Summary of Recommendations in the Second Report	2
Summary of Recommendations in the Third Report	4
Chapter II. Reassessing the Threat	7
A Fresh Perspective	8
Trends in Terrorism	9
“Homegrown” Threats	16
The Threat of Unconventional Weapons	19
Conclusion	26
Chapter III. Applying Cross-Cutting Themes	28
Protecting Our Civil Liberties	28
Enhancing State and Local Responsibilities	28
Improving Intelligence and Information Sharing	30
Promoting Strategic Communications	30
Enhancing Coordination with the Private Sector	31
Chapter IV. Resourcing the National Effort	34
Rationalizing the Process—States Versus Localities	34
Establishing Appropriate Burden Sharing	36
Ensuring a Central Focus	36
Determining “How Much is Enough”	37
Measuring Effectiveness	37
Chapter V. Organizing the National Effort	38
Assessing the National Strategy	38
General Comments	38
Definitional Issues	39
“Threat and Vulnerability”	39
“Organizing for a Secure Homeland”	39
“Intelligence and Warning”	40
“Border and Transportation Security”	40
“Domestic Counterterrorism”	41
“Protecting Critical Infrastructures and Key Assets”	41
“Defending Against Catastrophic Threats”	41
“Emergency Preparedness and Response”	41
Improving the Strategy and Structure	42
Intelligence Collection, Analysis, and Dissemination	42
Managing Operations	49
Interagency Coordination	50
Legal Authorities	50
The Congress	51
Chapter VI. Improving Health and Medical Capabilities	52
Applying Resources Effectively	53
Establishing and Using Metrics	55
Improving Hospitals and Other Medical Facilities	56
Enhancing Communications	58

Improving Exercises	59
Perfecting Specialized Response Teams.....	60
Promoting Technical Assistance.....	60
Increasing Surge Capacity	61
Providing One-Stop Shopping	62
Enhancing Research.....	62
Enacting Legal and Regulatory Changes	63
Determining Who Is In Charge.....	64
Establishing Public Communications Strategies.....	65
Reconciling Interagency Issues.....	66
Enhancing Pharmaceutical Supplies and Distribution	66
Implementing a Smallpox Vaccine.....	67
Chapter VII. Defending Against Agricultural Terrorism.....	68
Improving Resource Allocations	69
Understanding the Threat.....	70
Enhancing Planning	71
Improving Laboratory Capacity.....	74
Compensating for Agricultural Losses	75
Promoting Better Education and Training	76
Chapter VIII. Improving the Protection of Our Critical Infrastructure.....	78
Reconciling Definitional Terms.....	78
Enhancing Resources and Establishing Appropriate Burden Sharing	79
Improving Information Sharing	80
Determining Appropriate Identification and Access Controls.....	81
Improving the Roles of the Public At Large	81
Enhancing Cyber Security	82
Accounting for Private Sector Concerns.....	84
The Need for an Independent Commission.....	84
Developing Threat Assessments	85
Creating More Effective Cyber Security Policy	86
Enhancing Aviation Security	86
Improving the Security of Dams.....	87
Using Models and Metrics.....	87
Chapter IX. Establishing Appropriate Structures, Roles, and Missions for the Department of Defense..	88
Understanding the Proper Role of the Military in Homeland Security.....	88
Providing for the Defense of the Homeland	89
Providing Military Support to Civil Authorities	89
Improving the Structures for Use of the Military	92
Organizing the Defense Civilian Structure	93
Organizing the Military Structure.....	93
Improving Military Capabilities for Homeland Security.....	95
Clarifying Posse Comitatus and Other Relevant Statutes.....	96
Identifying Requirements	97
Enhancing Training.....	97
Establishing New Capabilities for Military Support to Civil Authorities.....	98
Improving the National Guard’s Role.....	101
Table of Appendices	108
Appendices	
List of Key Recommendations.....	Inside Back Cover

EXECUTIVE SUMMARY

Fifteen months have passed since the murderous terrorist attacks of September 11, 2001 and the subsequent anthrax attacks. U.S. efforts in the war against terrorism have produced measurable dividends. But the vague and shadowy threat of terrorism continues to present unique challenges.

In July of this year, the President approved for release the first *National Strategy for Homeland Security*—a major milestone in the battle against terrorism. The President recently signed legislation creating the Department of Homeland Security—the most significant restructuring of the Federal government in 55 years. Congress also passed and the President signed into law other landmark legislation over the past 15 months, including the USA PATRIOT Act; measures to enhance physical and cyber infrastructure security and preparedness; Federal terrorism insurance legislation; a bill to improve the key function of intelligence; and additional resources and authority for the use of the U.S. Armed Forces to combat terrorism.

The conclusions and recommendations in this report are the result of almost four years of research and deliberation. The Advisory Panel began its work in 1999 by an in-depth consideration of the threats posed to the United States by terrorists. By the second year, the Advisory Panel shifted its emphasis to specific policy recommendations for the Executive and the Congress and a broad programmatic assessment and functional recommendations for consideration in developing an effective national strategy. In its third report, the panel continued its analysis of critical functional areas. At the time of this publication, 66 of the 79 substantive recommendation made by the panel have been, at this writing, adopted in whole or in major part.

In the National Defense Authorization Act for 2002, the Congress extended the tenure of this Advisory Panel for two years. Thus, we continue our work to contribute to the implementation of a truly effective national strategy for combating terrorism. Because of the attacks in the fall of 2001, and other events that have since unfolded, we felt it was necessary to reexamine the threat assessment of the first report. We then considered several cross cutting themes and applied an analysis of these themes to most, if not all of the functional areas. These themes are: Protecting Our Civil liberties; Enhancing State and Local Responsibilities; Improving Intelligence and Information Sharing; Promoting Strategic Communications; and Enhancing Coordination with the Private Sector. This year we make policy recommendations in five specific areas: Organizing the National Effort; Improving Health and Medical Capabilities; Defending Against Agricultural Terrorism; Improving the Protection of Our Critical Infrastructure; and Establishing Appropriate Structures, Roles, and Missions for the Department of Defense.

Organizing the National Effort

The new threat environment requires the consolidation in one entity of the fusion and analysis of foreign-collected and domestically-collected intelligence and information on international terrorists and terrorist organizations threatening attacks against the United States. ***We recommend that the President direct the establishment of a National Counter Terrorism Center (NCTC).***

The FBI's long standing law enforcement tradition and organizational culture persuade us that, even with the best of intentions, the FBI cannot soon be transformed into an organization dedicated to detecting and preventing terrorist attacks. It is also important to separate the intelligence collection function from the law enforcement function to avoid the impression that the U.S. is establishing a kind of "secret police." ***We recommend that the collection of intelligence and other information on international terrorist activities inside the United States, including the authorities, responsibilities and safeguards under the Foreign Intelligence Surveillance Act (FISA), which are currently in the FBI, be transferred to the NCTC.***

Focused and effective Congressional oversight of the domestic collection and analysis functions is required. Currently, the oversight of the FBI's FISA and other domestic intelligence activities is split between the Judiciary and Intelligence committees in each House of Congress. ***We recommend that the Congress ensure that oversight of the NCTC be concentrated in the intelligence committee in each House.***

The *National Strategy for Homeland Security* designates various lead or co-lead agencies to perform both strategic and tactical analysis and vulnerability assessments. There is no indication that strategic assessments of threats inside the U.S. will receive dissemination to State and local agencies. ***We recommend that the President direct that the NCTC produce continuing, comprehensive "strategic" assessments of threats inside the United States, to be provided to policymakers at all levels, to help ensure appropriate planning and allocation of preparedness and response resources.***

It appears that the new DHS will have no authority for intelligence collection, limited capability for intelligence analysis, but significant responsibility for threat warnings. ***We recommend that the Congress and the President ensure that the DHS has the authority to levy direct intelligence requirements on the Intelligence Community for the collection or additional analysis of intelligence of potential threats inside the United States to aid in the execution of its specific responsibilities in the area of critical infrastructure protection vulnerability assessments. We further recommend that the Congress and the President ensure that the DHS has robust capability for combining threat information generated by the Intelligence Community and the NCTC with vulnerability information the Department generates in cooperation with the private sector to provide comprehensive and continuing assessments on potential risks to U.S. critical infrastructure.***

The *National Strategy for Homeland Security* does not provide any clarity about the extent to which DHS will be "in charge" of executing a response during or after an attack on some CIP sector; nor does it specify which Federal agency is in charge for the Federal sector for other types of attacks, especially a biological one. ***We recommend that the President and the Congress clearly define the responsibilities of DHS and other Federal entities before, during, and after an attack has occurred, especially any authority for directing the activities of other Federal agencies.***

The question of who is in charge is especially problematic when it comes to a bioterrorism attack. No one in the Federal structure can currently identify who is or, even after DHS is formed, will be in charge in the event of a biological attack. ***We recommend that the President specifically designate the DHS as the Lead Federal Agency for response to a bioterrorism***

attack, and specify its responsibilities and authority before, during, and after an attack; and designate the DHHS as the Principal Supporting Agency to DHS to provide technical support and provide the interface with State and local public health entities and related private sector organizations.

There are numerous Federal interagency coordination structures and several combined Federal/State/local structures. The proliferation of such mechanisms will likely cause unnecessary duplication of effort. ***We recommend that the Assistant to the President for Homeland Security review and recommend to the President, and that the President direct, a restructuring of interagency mechanisms to ensure better coordination within the Federal government, and with States, localities, and the private sector, to avoid confusion and to reduce unnecessary expenditure of limited resources at all levels.***

The creation of DHS and the implementation of the *National Strategy* raise several legal and regulatory issues, not the least of which are quarantine, isolation, mandatory vaccinations, and other prescriptive measures. ***We recommend that the President direct the Attorney General to conduct a thorough review of applicable laws and regulations and recommend legislative changes before the opening of the next Congress.***

The Congress is still not well organized to address issues involving homeland security in a cohesive way. Jurisdiction for various aspects of this issue continues to be scattered over dozens of committees and subcommittees. ***We therefore restate our prior recommendation with a modification that each House of the Congress establish a separate authorizing committee and related appropriation subcommittee with jurisdiction over Federal programs and authority for Combating Terrorism/Homeland Security.***

Improving Health and Medical Capabilities

Officials in public health have indicated that it will take at least a five-year commitment from DHHS, at approximately \$1 billion per year, to have a material impact on States and local government preparedness to respond to bioterrorist events. ***We recommend that DHHS continue to provide financial support on the order of \$1 billion per year over the next five years to strengthen the public health system in the United States.***

The centralization and simplification of grants processes for public health and medical funds is essential to eliminate confusion and unnecessary redundancies. ***We recommend that DHS coordinate and centralize the access to information regarding funding from various agencies such as DHHS (including CDC), EPA, USDA, and others and simplify the application process.***

There is currently no framework in place for monitoring the States' progress in meeting the objectives of the bioterrorism preparedness cooperative agreements program and for evaluating States' performance with respect to various outcomes. Moreover, there is a general lack of understanding on the part of representatives from State and local governments on precisely what they will be held accountable for and how their programs will be evaluated. ***We recommend that DHHS, in consultation with State, local, and private sector stakeholders, establish and***

implement a formal process for evaluating the effectiveness of investment in State, local, and private preparedness for responses to terrorist attacks, especially bioterrorism.

There are not yet widely agreed upon metrics by which to assess levels of preparedness among the medical and public health workforce. Without baseline data, it is impossible to quantify the gap between the current workforce and a workforce “prepared” to address these issues. ***We recommend that DHHS fund studies aimed at modeling the size and scope of the healthcare and public health workforce needed to respond to a range of public health emergencies and day-to-day public health issues.***

Federal officials requested almost \$600 million to improve hospital preparedness for FY03. This level of funding is not sufficient to prepare the nation’s 5,000 hospitals to handle mass casualty events, mainly because hospitals, like public health agencies, have responded to fiscal pressures by cutting back on staff and other resources and otherwise reducing “excess capacity.” ***We recommend that DHHS conduct a comprehensive assessment of the resources required by the nation’s hospital system to respond to terrorism, and recommend appropriate Federal-State-Local-Private funding strategies.***

The CDC needs to provide assistance in coordinating and connecting some of its own laboratory and disease surveillance information systems initiatives. These information systems should be connected to provide circular information flow. ***We recommend that DHHS continue to strengthen the Health Alert Network and other secure and rapid communications systems, as well as public health information systems that generate surveillance, epidemiologic and laboratory information.***

Exercises are critical to ensure adequate training, to measure readiness, and to improve coordination. Resources directed to State and local entities to conduct these exercises have been limited and incentives for cross discipline coordination require strengthening. ***We restate a previous recommendation with a follow on that the Congress increase Federal resources for appropriately designed exercises to be implemented by State, local, private sector medical and public health and emergency medical response entities.***

There is an urgent need to clarify the role and functions of the various Federal and State emergency response teams and the extent to which their roles will be coordinated at the Federal, State, and local levels. ***We recommend that DHHS clearly articulate the roles, missions, capabilities and limitations of special response teams; that a plan be developed for the effective integration of such teams; and that focused training for special teams emphasize integration as well as coordination with States and localities.***

State and local officials require technical assistance from the Federal government to select among competing technologies, develop templates for communicating risks and information on actual events to the public, develop plans for surge capacity and pharmaceutical distribution, and provide adequate training to staff. ***We recommend that DHHS evaluate current processes for providing required technical assistance to States and localities, and implement changes to make the system more responsive.***

Some State public health officials are unclear about their role in assisting with planning for the staffing of hospital beds in the state and otherwise becoming involved in surge capacity issues. States are implementing a wide range of preparedness activities but have had little opportunity to share this information with colleagues in other States. ***We recommend that DHHS develop an electronic, continuously updated handbook on best practices in order to help States and localities more effectively manage surge capacity, the distribution of the National Pharmaceutical Stockpile, and other preparedness goals.***

In addition to the substantial research NIH is performing on prevention, treatment, and cures for bioterrorism agents, additional basic research and further research on the application of new technologies is urgently needed. ***We recommend that NIH, in collaboration with CDC, strengthen programs focusing on both basic medical research and applied public health research, and the application of new technologies or devices in public health; and that DHS and OHS, in cooperation, prioritize and coordinate research among NIAID, other NIH entities, and other agencies conducting or sponsoring medical and health research, including DoD, DOE, and USDA, to avoid unnecessary duplication.***

The Model Health Powers Emergency Act would give State authorities certain important powers in a public health emergency. ***We recommend that each State that has not done so either adopt the Model Health Powers Emergency Act, as modified to conform to any single State's special requirements, or develop legislation of its own that accomplishes the same fundamental purposes; and work to operationalize laws and regulations that apply to CBRN incidents—naturally occurring, accidental or intentional, especially those that may require isolation, quarantine, emergency vaccination of large segments of the population, or other significant emergency authorities.***

During investigations into potential bioterror events, there is often a conflict between the goals and operating procedures of health and medical officials on the one hand and public safety officials on the other. The Federal Health Insurance Portability and Accountability Act (HIPAA) is in part designed to keep information about patients confidential and defines narrowly the information and the circumstances under which that information can be released. ***We recommend that the Congress clarify the conditions under which public health agencies, EMS, and hospitals can share information with law enforcement officials in special emergency circumstances under HIPAA. We further recommend, as a prerequisite for receiving Federal law enforcement and health and medical funds from the Federal government, that States and localities be required to develop comprehensive plans for legally-appropriate cooperation between law enforcement and public health, EMS and hospital officials.***

The development of a clear Federal strategic communications strategy, in coordination with State and local medical, public health, and elected officials, is not evident. ***We recommend that DHHS, in coordination with DHS, develop an on-going, well coordinated strategy for education of the public on the prevention, risks, signs, symptoms, treatments, and other important health and medical information before, during and after an attack or large-scale naturally occurring outbreak occurs.***

There is still a lot to learn about the most effective ways to treat people with mental or emotional problems following a terrorist attack. ***We recommend that DHHS, through the National Institute of Mental Health, and in collaboration with CDC, enhance funding for research into the prevention and treatment of the short and long-term psychological consequences of terrorist attacks.***

In-house health and medical expertise in the intelligence community is not sufficiently robust to provide for continuing strategic assessments of bioterrorism cause and effect. ***We recommend that the Intelligence Community improve its capacity for health and medical analysis by obtaining additional expertise in the medical and health implications of various terrorist threats.***

A number of States came up short in their cooperative agreement proposals with respect to their plans for National Pharmaceutical Stockpile receipt and distribution. Federal technical assistance is needed by State and local health officials to develop and exercise these plans. ***We recommend that DHHS significantly enhance technical assistance to States to help develop plans and procedures for distributing the NPS, continue to require exercises that demonstrate the States' ability to employ the NPS, and use specific metrics for evaluating States' capabilities.***

The timely research, development, production, and distribution of certain critical vaccines and other medical supplies continue to be perplexing problems. ***We recommend that DHHS, in collaboration with DHS and DoD, establish a national strategy for vaccine development for bioterrorism which will be consistent with the nation's needs for other vaccines.***

Recently, Federal health officials recommended a multiphase smallpox vaccination program for at-risk emergency medical personnel, with the Federal government assuming liability for adverse events related to vaccination. ***We recommend that the smallpox vaccination plan be implemented in incremental stages with careful analysis and continuous assessment of the risks of the vaccine. We further recommend that DHHS place a high priority on research for a safer smallpox vaccine.***

Defending Against Agricultural Terrorism

There is a lack of an overarching appreciation of the true threat to America's agriculture. Without a broad threat assessment, it is difficult to prioritize resources to counter the terrorist threat. ***We recommend that the President direct that the National Intelligence Council, in coordination with DHS, USDA and DHHS, perform a National Intelligence Estimate on the potential terrorist threat to agriculture and food.***

The Animal Health Emergency Preparedness Plan provides a guide for comprehensive emergency management plans for the response to emergencies involving animals and the animal industry segment of production agriculture. The Emergency Support Function (ESF) in the Animal Health Emergency Preparedness Plan is not currently applicable to any ESF in the Federal Response Plan. ***We recommend that the Assistant to the President for Homeland Security ensure that an Emergency Support Function for Agriculture and Food, consistent***

with the intent of the ESF described in the Animal Health Emergency Preparedness Plan, be included in the Federal Response Plan and the National Incident Response Plan under development.

There are only two existing civilian biosafety level 4 (BSL 4) laboratories for working with and diagnosing the most hazardous animal pathogens. If a large-scale outbreak of a foreign animal disease occurs in the United States, these would provide insufficient capacity. Capabilities at the State level would increase the ability to detect foreign animal diseases early. ***We recommend that the President propose and that the Congress enact statutory provisions for the certification under rigid standards of additional laboratories to test for Foot and Mouth Disease and other highly dangerous animal pathogens.***

Without advance training, and the appropriate equipment and security in place prior to an outbreak, it is not likely that State veterinary labs will be adequately prepared to respond to a crisis. ***We recommend that the Secretaries of Homeland Security and Agriculture (consistent with the November 2001 resolution of the United States Animal Health Association) jointly publish regulations implementing a program to train, equip, and support specially designated, equipped, secure, and geographically distributed veterinary diagnostic laboratories to perform tests and enhance surveillance for agricultural diseases that are foreign to the United States.***

To encourage reporting of diseases and to ensure the stability of the agricultural sector, it is critical that a consistent scheme of national compensation is in place to provide financial assistance to producers and other agribusiness interests impacted by an animal disease outbreak. ***We recommend that the Secretary of Agriculture, in consultation with State and local governments and the private sector, institute a standard system for fair compensation for agriculture and food losses following an agroterrorism attack; and that the Secretary of Health and Human Services should develop a parallel system for non-meat or poultry food.***

There are not enough appropriately trained veterinarians capable of recognizing and treating exotic livestock diseases in the United States. Other types of expertise required for dealing with agricultural diseases are lacking. ***We recommend that the Secretary of Agriculture develop and that the Congress fund programs to improve higher education in veterinary medicine to include focused training on intentional attacks, and to provide additional incentives for professional tracks in that discipline. We further recommend that the Secretary of Agriculture, in coordination with States, improve education, training, and exercises between government and the agricultural private sector, for better understanding the agroterrorism threat, and for the identification and treatment of intentional introduction of animal diseases and other agricultural attacks.***

Improving the Protection of Our Critical Infrastructure

Physical and cyber infrastructure protection contains many very sensitive issues of great importance about which objective research and proposals are very difficult to conduct and develop within the political process. We have modified the recommendation in our third report to cover all infrastructures, both physical and cyber. ***We recommend that the***

Congress establish and that the President support an Independent Commission to suggest strategies for the protection of the nation's critical infrastructures.

The lack of a comprehensive assessment of threats to U.S. infrastructures significantly hampers defensive measures and preparedness activities. ***We recommend that the President direct that the National Intelligence Council perform a comprehensive National Intelligence Estimate on the threats to the nation's critical infrastructure.***

The continuing bifurcation of policy for the physical and cyber components of CIP has created confusion and resulted in less than effective policy formulation. ***We recommend that the President direct the merger of physical and cyber security policy development into a single policy entity in the White House.***

Progress in meeting airline passenger baggage-screening goals has been slow, and no screening technology will ever be foolproof. Perhaps equally important is the fact that much of the non-passenger cargo on commercial passenger aircraft is not being screened. ***We recommend that DHS elevate the priority of measures necessary for baggage and cargo screening on commercial passenger aircraft, especially non-passenger cargo.***

The security of general aviation aircraft and facilities is thin, where it exists at all. ***We recommend that that DHS, in conjunction with the airline industry, develop comprehensive guidelines for improving the security of general aviation.***

Hydroelectric and other dams on various watercourses present a significant hazard if terrorists find ways to exploit their controls. ***We recommend that DHS make dam security a priority, and consider establishing regulations for more effective security of dam facilities.***

One of the critical shortcomings in structuring programs and securing funds to protect critical infrastructures is the lack of risk-based models and metrics that help explain the value of protective measures in terms that public and private sector decision makers understand. ***We recommend that DHS use the NISAC modeling and analytic capabilities to develop metrics for describing infrastructure security in meaningful terms, and to determine the adequacy of preparedness of various critical infrastructure components.***

Establishing Appropriate Structures, Roles, and Missions for the Department of Defense

NORTHCOM is in a transitional phase between initial operational capability and full operational capability. In its initial structure, NORTHCOM has few permanently assigned forces, and most of them serve as part of its homeland security command structure. The creation of NORTHCOM is an important step toward enhanced civil-military integration for homeland security planning and operations, and could result in an enhancement of homeland security response capabilities. ***We recommend that the Secretary of Defense clarify the NORTHCOM mission to ensure that the Command is developing plans across the full spectrum of potential activities to provide military support to civil authorities, including circumstances when other national assets are fully engaged or otherwise unable to respond, or when the mission requires additional or different military support. NORTHCOM should plan and train for such missions accordingly.***

In our *Third Report*, we recommended that a unified command be created “to execute all functions for providing military support or assistance to civil authorities”—an all-hazards approach. The Advisory Panel is pleased that NORTHCOM will apparently execute *most* of these functions, and further ***we recommend that the NORTHCOM combatant commander have, at a minimum, operational control of all Federal military forces engaged in missions within the command’s area of responsibility for support to civil authorities.***

To achieve that clarity, the laws governing domestic use of the military should be consolidated and the Federal government should publish a document that clearly explains these laws. ***We recommend that the President and the Congress amend existing statutes to ensure that sufficient authorities and safeguards exist for use of the military across the entire spectrum of potential terrorist attacks (including conventional, chemical, biological, radiological, and nuclear threats as well as cyber); that the authorities be consolidated in a single chapter of Title 10; and that DoD prepare a legal “handbook” to ensure that military and civilian authorities better understand the legal authorities governing the use of the military domestically in support of civilian authorities for all hazards—natural and manmade.***

No process is clearly in place to identify among the full scope of requirements for military support to civil authorities. ***We recommend that the President direct the DHS to coordinate a comprehensive effort among DoD (including NORTHCOM) and Federal, State, and local authorities to identify the types and levels of Federal support, including military support, that may be required to assist civil authorities in homeland security efforts and to articulate those requirements in the National Incident Response Plan***

Insufficient attention has been planning and conducting military training specifically for the civil support mission. ***We recommend that the Secretary of Defense direct that all military personnel and units under NORTHCOM, or designated for NORTHCOM use in any contingency, receive special training for domestic missions. Furthermore, in those cases where military personnel support civil law enforcement, special training programs should be established and executed.***

There is a question about whether NORTHCOM’s commander “combatant command” (COCOM) relationship with the various service component commands is only for the purpose of unity of *homeland defense* authority and responsibility or applies more broadly to all *homeland security* missions, including NORTHCOM’s civil support mission. Thus, at this writing, the extent to which the new command will be able to direct new and expanded civil support training and exercises remains unclear. ***We recommend that the Secretary of Defense clarify NORTHCOM’s combatant command authority to ensure that Commander NORTHCOM can direct subordinate commands to conduct pre-incident planning, training, and exercising of forces required to conduct civil support missions.***

Rapid response-type capabilities should arguably be tailored to deal with homeland terrorist events that overwhelm State and local capabilities. ***We recommend that the Combatant Commander, NORTHCOM, have dedicated, rapid-reaction units with a wide range of response capabilities such as an ability to support implementation of a quarantine, support crowd control activities, provide CBRNE detection and***

decontamination, provide emergency medical response, perform engineering, and provide communication support to and among the leadership of civil authorities in the event of a terrorist attack.

States may have difficulty funding homeland security training and operations of the National Guard in State Active Duty status, especially if their missions are conducted for extended periods. Commanders are not clearly authorized under Title 32 to expend Federal funds for training for civil support tasks. ***We recommend that the Congress expressly authorize the Secretary of Defense to provide funds to the governor of a State when such funds are requested for civil support planning, training, exercising and operations by National Guard personnel acting in Title 32 duty status and that the Secretary of Defense collaborate with State governors to develop agreed lists of National Guard civil support activities for which the Defense Department will provide funds.***

The States' existing National Guard military support arrangements must be enhanced to provide for more effective response capabilities in Title 32 duty status. ***We recommend that the President and governors of the several States establish a collaborative process for deploying National Guard forces in Title 32 duty status to support missions of national significance at the President's request; and that the Congress provide new authority under Title 32 to employ the National Guard (in non-Title 10 status) on a multi-State basis, and with governors' consent to conduct homeland security missions, and that the Secretary of Defense define clearly the appropriate command relationships between DoD and the National Guard. We further recommend that the Congress and DoD promote and support the development of a system for National Guard civil support activities that can deploy forces regionally--in coordination with DoD--to respond to incidents that overwhelm the resources of an individual State.***

Further enhancement of the National Guard's civil support capability and responsibility is necessary. In the Third Report we recommended "that the Secretary of Defense . . . direct that National Guard units with priority homeland security missions plan, train, and exercise with State and local agencies," be expanded. ***We now recommend that the Secretary of Defense direct that certain National Guard units be trained for and assigned homeland security missions as their exclusive missions (rather than primary missions as stated in our Third Report) and provide resources consistent with the designated priority of their homeland missions.***

CHAPTER I. INTRODUCTION

Milestones of the Last Fifteen Months

Fifteen months have passed since the murderous terrorist attacks of September 11, 2001 and the subsequent anthrax attacks. We have been fortunate, indeed, that no additional, major terrorist attacks have been perpetrated inside our borders. But now is certainly no time to let down our guard.

The ability of al Qaeda and its cohorts may have been significantly degraded but it has not been destroyed. Terrorists linked with al Qaeda continue to carry out highly lethal attacks against Western targets around the world. Recent attacks in Bali, in Kenya, in Tunisia, and on the French tanker off the coast of Yemen, are examples of the work of that far-flung conspiracy and its continuing ability to kill people in large numbers. Intelligence sources continue to pick up “chatter” that indicates more attacks inside the United States are being planned. Some will certainly occur.

U.S. efforts in the war against terrorism have produced measurable dividends. Supported by our allies, we have overthrown the outlaw Taliban regime in Afghanistan, and have had marked success in killing or capturing numbers of al Qaeda followers and some key members of its leadership, including Mohammad Atef, Abu Zubaydah, Omer Farouk, Ramzi Binalshibh, Emad Abdewalid Ahmed Alwan, Abdl Rahman Nashiri, and Qaed Senyan al-Harhi. Yet others—including Ayman al-Zawahiri, reputed to be the number two man in the al Qaeda network—remain at large amid new evidence to suggest that Osama bin Laden himself may still be alive.

Moreover, the vague and shadowy threat of terrorism continues to present unique challenges. After more than fourteen months since the anthrax attacks claimed five lives, injured twelve others, and frightened countless thousands, no arrests have been made in that case.

In July, the President approved for release the first *National Strategy for Homeland Security*—a major milestone in the battle against terrorism. The President recently signed legislation creating the Department of Homeland Security—the most significant restructuring of the Federal government in 55 years.

During this period, Congress also passed and the President signed into law other landmark legislation, including:

- the USA PATRIOT Act, which enhances law enforcement against terrorists;
- Federal terrorism insurance legislation;
- measures to enhance the nation’s port security;
- aviation security legislation, including the new Transportation Security Administration;
- a \$4.6 billion bioterrorism preparedness program;
- an intelligence bill that attempts to strengthen coordination among agencies and that established the National Commission on Terrorist Attacks Upon the United States to examine the circumstances of the September 11 attacks;
- a \$903 billion program for enhancing cybersecurity; and
- additional resources and authority for the use of the U.S. Armed Forces to combat terrorism.

Despite the successes and the changes to law, policy, and the level of resources dedicated to the effort, significant additional improvements, across a broad spectrum of functions, remain to be accomplished.

Extension of the Advisory Panel

In the National Defense Authorization Act for 2002, the Congress extended the tenure of this Advisory Panel for two years with the requirement to submit two additional reports to the President and the Congress on December 15 of 2002 and 2003.¹

The conclusions and recommendations in this report are the result of almost four years of constant research and deliberation. The Advisory Panel began its work in 1999 with an in-depth consideration of the threats posed to the United States by terrorists, both individuals and organizations. A key finding in the first annual report was the urgent need for a comprehensive national strategy for combating terrorism.

By the second year, the Advisory Panel shifted its emphasis to specific policy recommendations for the Executive and the Congress and a broad programmatic assessment and functional recommendations for consideration in developing an effective national strategy. In its third report, the panel continued its analysis of critical functional areas.

To understand the key conclusions and recommendations in this fourth annual report, it is important to place the recommendations in the context of our previous research and analysis. We begin, therefore, with a brief summary of the recommendations contained in our Second and Third Annual Reports.

While 66 of the 79 substantive recommendations made by the panel have been, at this writing, adopted in whole or in major part, it has never been our intention to offer all the answers or necessarily the best answers for the daunting challenges that we face. Our recommendations are, nevertheless, based on the cumulative experience of our members, informed by exceptionally valuable research and analysis from our support staff at RAND, and are offered in the belief that they can contribute materially to the critical, continuing debate.

Summary of Recommendations in the Second Report

The capstone recommendation in the *Second Report* was the need for a comprehensive, coherent, functional national strategy: ***The President should develop and present to the Congress a national strategy for combating terrorism within one year of assuming office.*** As part of that recommendation, the panel identified the essential characteristics for a national strategy:

- It must be truly *national* in scope, not just Federal.
- It must be comprehensive, encompassing the full spectrum of *deterrence, prevention, preparedness, and response* against domestic and international threats.
- Domestically, it must be *responsive to* requirements from and fully *coordinated with State and local officials* as partners throughout the development and implementation process.
- It should be *built on existing emergency response systems.*

¹ See Appendix A.

- It must *include all key functional domains*—intelligence, law enforcement, fire services, emergency medical services, public health, medical care providers, emergency management, and the military.
- It must be *fully resourced* and based on *measurable performance*.

The Second Annual Report included a discussion of more effective Federal structures to address the national efforts to combat terrorism. We determined that the solutions offered by others who have studied the problem provide only partial answers. The Advisory Panel has attempted to craft recommendations to address the full spectrum of issues. Therefore, we submitted the following recommendation: ***The President should establish a senior level coordination entity in the Executive Office of the President.*** The characteristics of the office identified in that recommendation include:

- Director appointed by the President, by and with the advice and consent of the Senate, at “cabinet-level” rank
- Located in the Executive Office of the President
- Authority to exercise certain program and budget controls over those agencies with responsibilities for combating terrorism
- Responsibility for intelligence coordination and analysis
- Tasking for strategy formulation and implementation
- Responsibility for reviewing State and local plans and to serve as an information clearinghouse
- An interdisciplinary Advisory Board to assist in strategy development
- Multidisciplinary staff (including Federal, State, and local expertise)
- No operational control

We included a thorough explanation of each of these characteristics in our Second Annual Report.

To complement our recommendations for the Federal executive structure, we also included the following recommendation for the Congress: ***The Congress should establish a Special Committee for Combating Terrorism—either a joint committee between the Houses or separate committees in each House—to address authority and funding, and to provide congressional oversight, for Federal programs and authority for combating terrorism.***

The philosophy behind this recommendation is much the same as it is for the creation of the office in the Executive Office of the President. There needs to be a focal point in the Congress for the Administration to present its strategy and supporting plans, programs, and budgets, as well as a legislative “clearinghouse” where relevant measures are considered. At least 48 committees and subcommittees have some jurisdiction over the issue of terrorism. No existing standing committee can or should be empowered with all of these responsibilities because each existing committee is limited in its jurisdictional scope.

In conjunction with these structural recommendations, the Advisory Panel made a number of recommendations addressing functional requirements for the implementation of an effective strategy for combating terrorism. The recommendation listed below are discussed thoroughly in the Second Annual Report:

Enhance Intelligence/Threat Assessments/Information Sharing

- Improve human intelligence by the rescission of that portion of the 1995 guidelines, promulgated by the Director of Central Intelligence, which prohibits the engagement of certain foreign intelligence informants who may have previously been involved in human rights violations
- Improve Measurement and Signature Intelligence (MASINT) through an expansion in research, development, test, and evaluation (RDT&E) of reliable sensors and rapid readout capability and the subsequent fielding of a new generation of MASINT technology based on enhanced RDT&E efforts
- Review statutory and regulatory authorities in an effort to strengthen investigative and enforcement processes
- Improve forensics capabilities to identify and warn of terrorist use of unconventional weapons
- Expand information sharing and improve threat assessments

Foster Better Planning/Coordination/Operations

- Designate the senior emergency management entity in each State as the *focal point* for that State for coordination with the Federal government for preparedness for terrorism
- Improve collective planning among Federal, State, and local entities
- Enhance coordination of programs and activities
- Improve operational command and control of domestic responses
- The President should always designate a Federal civilian agency other than the Department of Defense (DoD) as the Lead Federal Agency

Enhance Training, Equipping, and Exercising

- Improve training through better coordination with State and local jurisdictions
- Make exercise programs more realistic and responsive

Improve Health and Medical Capabilities

- Establish a national advisory board composed of Federal, State, and local public health officials and representatives of public and private medical care providers as an adjunct to the new office, to ensure that such issues are an important part of the national strategy
- Improve health and medical education and training programs through actions that include licensing and certification requirements
- Establish standards and protocols for treatment facilities, laboratories, and reporting mechanisms
- Clarify authorities and procedures for health and medical response
- Medical entities, such as the Joint Commission on Accreditation of Healthcare Organizations, should conduct periodic assessments of medical facilities and capabilities

Promote Better Research and Development and Create National Standards

- That the new office, in coordination with the Office of Science and Technology Policy, develop a comprehensive plan for RDT&E, as a major component of the national strategy
- That the new office, in coordination with the National Institute for Standards and Technology (NIST) and the National Institute for Occupational Safety and Health (NIOSH) establish a national standards program for combating terrorism, focusing on equipment, training, and laboratory processes

Summary of Recommendations in the Third Report

The vast majority of those recommendations for its Third Report were adopted at the panel's regular meeting on August 27 and 28, 2001—two weeks prior to the September attacks. The

Advisory Panel continued to make specific recommendations in key functional areas in order to implement an effective strategy for combating terrorism. The recommendations listed below are discussed thoroughly in that Third Annual Report:

State and Local Response Capabilities

- Increase and accelerate the sharing of terrorism-related intelligence and threat assessments
- Design training and equipment programs for all-hazards preparedness
- Redesign Federal training and equipment grant programs to include sustainment components
- Increase funding to States and localities for combating terrorism
- Consolidate Federal grant program information and application procedures
- Design Federal preparedness programs to ensure first responder participation, especially volunteers
- Establish an information clearinghouse on Federal programs, assets, and agencies
- Configure Federal military response assets to support and reinforce existing structures and systems

Health and Medical Capabilities

- Implement the AMA Recommendations on Medical Preparedness for Terrorism
- Implement the JCAHO Revised Emergency Standards
- Fully resource the CDC Biological and Chemical Terrorism Strategic Plan
- Fully resource the CDC Laboratory Response Network for Bioterrorism
- Fully resource the CDC Secure and Rapid Communications Networks
- Develop standard medical response models for Federal, State, and local levels
- Reestablish a pre-hospital Emergency Medical Service Program Office
- Revise current EMT and PNST training and refresher curricula
- Increase Federal resources for exercises for State and local health and medical entities
- Establish a government-owned, contractor-operated national vaccine and therapeutics facility
- Review and recommend changes to plans for vaccine stockpiles and critical supplies
- Develop a comprehensive plan for research on terrorism-related health and medical issues
- Review MMRS and NDMS authorities, structures, and capabilities
- Develop an education plan on the legal and procedural issues for health and medical response to terrorism
- Develop on-going public education programs on terrorism causes and effects

Immigration and Border Control

- Create an intergovernmental border advisory group
- Fully integrate all affected entities into local or regional “port security committees”
- Ensure that all border agencies are partners in intelligence collection, analysis, and dissemination
- Create, provide resources for, and mandate participation in a “Border Security Awareness” database system
- Require shippers to submit cargo manifest information simultaneously with shipments transiting U.S. borders
- Establish “Trusted Shipper” programs
- Expand Coast Guard search authority to include U.S. owned—not just “flagged”—vessels
- Expand and consolidate research, development, and integration of sensor, detection, and warning systems
- Increase resources for the U.S. Coast Guard for homeland security missions
- Negotiate more comprehensive treaties and agreements for combating terrorism with Canada and Mexico

Cyber Security

- Include private and State and local representatives on the interagency critical infrastructure advisory panel
- Create a commission to assess and make recommendations on programs for cyber security
- Establish a government funded, not-for-profit entity for cyber detection, alert, and warning functions
- Convene a “summit” to address Federal statutory changes that would enhance cyber assurance
- Create a special “Cyber Court” patterned after the court established in FISA
- Develop and implement a comprehensive plan for cyber security research, development, test, and evaluation

Use of the Military

- Establish a homeland security under secretary position in the Department of Defense
- Establish a single unified command and control structure to execute all military support to civil authorities
- Develop detailed plans for the use of the military domestically across the spectrum of potential activities
- Expand training and exercises in relevant military units and with Federal, State, and local responders
- Direct new mission areas for the National Guard to provide support to civil authorities
- Publish a compendium of statutory authorities for using the military domestically to combat terrorism
- Improve the military full-time liaison elements in the ten Federal Emergency Management Agency regions

CHAPTER II. REASSESSING THE THREAT

The attacks of September 11, 2001 reinforced the threat of large-scale attacks inside the United States, and the subsequent anthrax attacks marked the first fatal use of a biological weapon in the United States. This chapter assesses what these and related developments indicate in terms of anti-American terrorism, including the use of chemical, biological, radiological, nuclear, or conventional explosive weapons (CBRNE) inside the United States. Events this past year, including the successful overthrow of the Taliban in Afghanistan, the continuing war on terrorism, and the increasing potential for war with Iraq also carry profound implications for understanding the threat.²

In one of its first decisions almost four years ago, the Advisory Panel concluded that, to assess preparedness for terrorist events effectively, one must understand the “full range of potential CBRN threats from terrorists.”³ In 1999, the panel commissioned its supporting staff at RAND, the National Defense Research Institute, to provide an “articulate, comprehensive, and current assessment and analysis of the potential domestic threat from terrorists who might seek to use a CBRN device or agent.” The report in 1999 concluded that, although terrorists had an interest in using CBRN weapons to cause mass casualties, significant technological constraints could thwart their malevolent intentions. Accordingly, while not dismissing that potentiality, the panel recommended that the United States must *also* be prepared for higher probability, lower consequence terrorist events—primarily continuing attacks with conventional weapons—which could have specific and unique response requirements of their own.⁴ We restate our firm opinion that planning for response to terrorism must not be based primarily on vulnerabilities; that is a misplaced approach. Initially, such planning and preparedness must be based upon a comprehensive analysis of threats before considerations of vulnerabilities.

While the 1995 bombing in Oklahoma City and the 1993 attack on the World Trade Center brought home the potential threat of terrorism, the attacks on September 11 further emphasized that the United States is not immune from foreign attacks of a mass scale on its own soil. It also indicated that, while the United States arguably has other enemies in a number of places, Osama bin Laden and his al Qaeda organization, then based in Afghanistan, posed the greatest threat to this country. In the 15 months since the September 11 attacks, bin Laden and al Qaeda remain the preeminent threat facing the United States today. It should, however, be emphasized that, while the September 11 attacks were horrific in terms of the loss of human life and economic damage inflicted on America, it was not the worst-case scenario that many policymakers, government officials, and scholars believed would befall the country either in terms of the

² The panel’s conclusions are based primarily on a second comprehensive assessment and analysis of potential terrorist threats by RAND staff, supplemented by briefings and other information provided to the panel and from the panel’s collective knowledge and experience. This assessment also borrows from an analysis of terrorism and counterterrorism since September 11, 2001 which is summarized in Bruce Hoffman, “Re-Thinking Terrorism and Counterterrorism Since 9/11,” *Studies in Conflict and Terrorism*, vol. 25, no. 5 (September – October 2002), pp. 303-316.

³ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction [Gilmore Commission], *First Annual Report to the President and the Congress, I, Assessing the Threat* (Washington, DC: RAND, December 15, 1999), p. vii.

⁴ *Ibid.*, pp. 38, 54.

numbers of casualties or even more specifically in the use of exotic or the otherwise unconventional weapons.⁵

A Fresh Perspective

This analysis focuses on changes both in the terrorist environment worldwide and in our nation's sense and perceptions of security since the Advisory Panel's first analysis of the threat. The overall conclusion remains that lower consequence events are of a higher probability than higher consequence events. Nevertheless, the higher consequence events may now be somewhat more probable for a variety of reasons, including:

- The dramatic illustration on September 11 of how terrorists' motives have changed, showing that groups like al Qaeda have as a goal killing large numbers of people;
- The level of sophistication and coordination, patience and determination achieved by al Qaeda in carrying out simultaneous or sequential attacks;
- What we know now about al Qaeda's ambitions to develop chemical, biological, nuclear and radiological weapons; and
- The measure of success, albeit limited, of the anthrax attacks last fall, coupled with the fact that the perpetrator or perpetrators of those attacks have not been found.

For those reasons and others, the nation must be sufficiently prepared to respond to threats across the weaponry and technological spectrum.

We are also compelled to take this new approach because of the discovery of crude biological and chemical weapons capabilities in Afghanistan,⁶ the subsequent capture of al Qaeda operatives, as well as the continuing series of lethal bombings overseas such as the attack off Yemen on the French oil tanker, the bombing in Bali, and the attacks in Kenya and in Tunisia—showing once again the agility of al Qaeda and its sympathizers to strike on terms of their own making.

The United States war on terror may have changed the character of the threat itself by forcing terrorists to change tactics and targets. According to Undersecretary of State John Bolton:

Today, the United States believes that the greatest threat to international peace and stability comes from rogue states and transnational terrorist groups that are unrestrained in their choice of weapon and undeterred by conventional means. The September 11 attacks showed that terrorist groups were much better organized, much more sophisticated, and much more capable of acting globally than we had assumed possible. Our concept of what terrorists are able to do to harm innocent civilians has changed fundamentally. There can be no doubt that, if

⁵ See U.S. Senate, Committee on the Judiciary, *Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*, Hearing, March 27, 2001, Washington: U.S. Government Printing Office, 2001.

⁶ David McGlinchey, "Al Qaeda: Coalition Forces Disabled Chemical Plant in 2001," *Global Security Newswire*, September 18, 2002.

given the opportunity, terrorist groups such as al Qaeda would not hesitate to use disease as a weapon against the unprotected; to spread chemical agents to inflict pain and death on the innocent; or to send suicide-bound adherents armed with radiological explosives on missions of murder.⁷

This chapter first explores general trends in terrorism with a focus on the high-end threat posed specifically by foreign terrorist organizations. It then turns to an examination of the domestic threat both from traditional, U.S. “homegrown” terrorists as well as from citizens and legal residents of the United States working with or influenced by foreign terrorists groups. Finally the chapter focuses on the specific threat of CBRN weapons.

We emphasize that this analysis is only “a snapshot in time.” In the future, changes in one of a number of significant factors could cause any threat analysis to be modified and to reach substantially different conclusions.

Trends in Terrorism

First, terrorism has undeniably continued its trend toward increasing lethality. While terrorist groups have consistently targeted U.S. citizens and businesses overseas for the past thirty years, within the span of just an hour and a half on September 11, more than three times the number of Americans were killed than during the entire previous 33 years.⁸ Indeed, terrorist groups have conducted approximately 3,300 attacks against U.S. targets since 1968.⁹ Yet in all of these attacks no more than some 1,000 total Americans were killed. Similarly, only 14 terrorist operations in the past 100 years have killed more than 100 persons.¹⁰ The attacks on the World Trade Center and the Pentagon, therefore, represent a dramatic increase in the lethality of terrorist attacks. The trend towards intense bloodshed has not subsided. The October 2002 attack in Bali killed approximately 200 people—the deadliest terrorist attack since September 11, 2001. Indeed, it is believed that the Bali incident was intentionally designed to cause maximum casualties.¹¹ This trend stems in part from changes in terrorists’ motivations. Throughout most of the last half of the twentieth century terrorists had a defined set of political, social, or economic objectives. A new generation of terrorists has emerged with different motives and includes millenarian movements and nationalist religious groups whose aims are much more deadly.¹²

⁷ John R. Bolton, Undersecretary Of State for Arms Control and International Security, “The International Aspects of Terrorism and Weapons of Mass Destruction,” Second Global Conference On Nuclear, Bio/Chem Terrorism: Mitigation And Response, The Hudson Institute, Washington, DC, November 1, 2002 as released by the State Department.

⁸ Hoffman, “Re-Thinking Terrorism...,” p. 304.

⁹ Several factors can account for this phenomenon, in addition to America’s position as the sole remaining superpower and leader of the free world. These include the geographical scope and diversity of America’s overseas business interests, the number of Americans traveling or working abroad, and the many U.S. military bases around the world.

¹⁰ Brian M. Jenkins, “The Organization Men: Anatomy of a Terrorist Attack,” in James F. Hoge, Jr. and Gideon Rose, *How Did This Happen? Terrorism and the New War* (NY: Public Affairs, 2001), p. 5.

¹¹ Maria Ressa, Atika Shubert, et al., “Hundreds missing in Bali bombing,” *CNN.com*, October 14, 2002, available at <http://www.cnn.com/2002/WORLD/asiapcf/southeast/10/13/bali.blast.missing/>, accessed November 6, 2002.

¹² Hoffman, “Lessons of 9/11,” p. 4.

Yet “lethality” is not necessarily the only way of measuring the increasingly significant impact that terrorism is having on the United States and the international community. Indeed, terrorist attacks have also inflicted growing economic damage on target societies. It appears that this trend may be the result of a conscious decision on the part of the organizations responsible for either perpetrating or fomenting this violence. For example, Osama bin Laden and other al Qaeda leaders were reportedly elated by the economic losses caused by the September 11 attacks. Bin Laden bragged in the October 2001 videotape declaring war on the United States about the “trillions of dollars” of economic losses. Similarly, Ahmed Omar Sheikh, the chief suspect in the killing of the American journalist, Daniel Pearl, echoed this same point. While being led out of a Pakistani court in March, he exhorted anyone listening to “sell your dollars, because America will be finished soon.”¹³ Even if al Qaeda did not hold economic damage as a primary objective in the September 11 attacks, these attacks have raised an awareness of how sensitive the U.S. and world economy can be to terrorism. Indeed, bin Laden and his chief lieutenant Ayman al-Zawahiri, in tapes released on October 6, 2002, reportedly reiterated the focus on economic targets. Bin Laden pointedly warned, “By God, the youths of God are preparing for you things that would fill your hearts with terror and target your economic lifeline until you stop your oppression and aggression.”¹⁴ And al-Zawahiri similarly echoed this theme, “The settlement of this overburdened account will indeed be heavy. We will also aim to continue, by permission of Allah, the destruction of the American economy.”¹⁵

The second general trend is more recent and, as such, likely the result of the U.S. war on terrorism. Despite a continued desire to execute large scale, high consequence attacks, smaller, more frequent attacks are more likely to occur in the near future. As law enforcement and intelligence services continue to disrupt al Qaeda and its affiliated groups overseas and degrade their capability to conduct mass casualty attacks inside the United States, these groups are likely to turn to smaller-scale alternatives against more accessible, softer targets.¹⁶ Inside the United States, these smaller-scale attacks could in the future take the form, among others, of suicide bombings, assassinations, low level biological attacks, car and truck bombings of government buildings and other symbolic targets, or arson attacks against banks.¹⁷ Indeed, Sheik Hassan Nasrallah, the leader of Hezbollah, recently called for global suicide attacks, although traditionally Hezbollah has only targeted Israelis in the Middle East.¹⁸ It is worth noting, however, that Hezbollah is widely believed to have been responsible for the 1992 and 1994 truck bombings outside the Israeli embassy and then a Jewish community center in Buenos Aires, thereby demonstrating a global terrorist reach.

¹³ Raymond Bonner, “Suspect in Killing of Reporter Is Brash and Threatening in a Pakistani Court,” *New York Times*, 13 March 2002.

¹⁴ Associated Press, “Bin Laden tape: 'Youths of God' plan more attacks,” October 7, 2002, available at <http://www.smh.com.au/articles/2002/10/07/1033538881353.html> on November 3, 2002.

¹⁵ Arena, Kelli, “U.S.: Latest Tapes Cause for Concern,” October 10, 2002, available at <http://www.cnn.com/2002/WORLD/asiapcf/central/10/08/alqaeda.threat.tape/> on November 3, 2002.

¹⁶ Peter Finn, Dana Priest, “Weaker al Qaeda Shifts To Smaller-Scale Attacks,” *Washington Post*, October 15, 2002, and available at <http://www.washingtonpost.com/wp-dyn/articles/A25832-2002Oct14.html>, accessed October 29, 2002.

¹⁷ Agence France-Presse, “Homeland Security chief sees new al Qaeda attacks in U.S.,” August 27, 2002, available at http://www.inq7.net/brk/2002/aug/27/brkafp_2-1.htm, accessed October 29, 2002.

¹⁸ In a recent speech at a rally broadcast on television in Lebanon, Nasrallah stated, “Martyrdom operations - suicide bombings - should be exported outside Palestine. I encourage Palestinians to take suicide bombings worldwide.” Paul Martin, “Hezbollah calls for global attacks,” *Washington Times*, December 4, 2002.

In conjunction with this, a trend towards softer, or unprotected, targets has also emerged, since September 11, in attacks against Western targets overseas. For example, al Qaeda, in conjunction with its affiliated groups, has conducted attacks against a synagogue in Tunisia (April 2002), a bus carrying French naval engineers in Pakistan (May 2002), a nightclub frequented by Westerners in Bali (October 2002), and an Israeli-owned hotel in Kenya (November 2002). The argument for this general trend was further reinforced in May 2002, when senior al Qaeda lieutenant Abu Zubaydah, currently in U.S. custody, warned that al Qaeda operatives were discussing attacks on soft targets, specifically non-governmental buildings and places where large number of Americans gather.¹⁹ Moreover, another al Qaeda operative in U.S. custody, Indonesian Mohammad Mansour Jabarah, told U.S. investigators, shortly before the tourist attacks on Bali in October that Jemaah Islamiyya operative Hambali was planning to conduct “small bombings in bars, cafes, or nightclubs frequented by Westerners in Thailand, Malaysia, Singapore, the Philippines, and Indonesia.”²⁰

Third, recent events indicate that terrorists will likely be forced to continue to innovate in the types of attacks they conduct, the methods they use, and the targets they select. Although historically, modern terrorists have been more imitative than innovative, recent attacks by al Qaeda demonstrate that this group, in particular, has proven adept at tactical innovation.²¹ For example, al Qaeda’s attacks against USS *Cole* demonstrated a degree of innovation, even if it were copying tactics that the Tamil Tigers have successfully used to target naval vessels off the coast of Sri Lanka. More significantly, the attacks of September 11 displayed al Qaeda’s ability to employ deception and innovative tactics to successfully attack targets. Since September 2001, it appears that al Qaeda is continuing to identify new U.S. vulnerabilities both at home and abroad, adjusting their tactics and targeting in part as a response to their lack of sanctuary and the need to be more careful in their logistical support activities and communications. For example, press reports have indicated that some al Qaeda operatives have engaged in scuba diver training in order to place explosives on ships in port,²² while other reports have pointed to threatened attacks on U.S. passenger trains.²³ Further sections of this report will focus on the chemical, biological, radiological and nuclear (CBRN) threats of terrorist groups. Suffice it to say for the moment that in March 2001, Italian authorities obtained evidence suggesting that a terrorist cell affiliated with al Qaeda had contemplated using poison gas in an attack on the U.S. Embassy in Rome. Italian authorities, working with U.S. officials, arrested members of this cell in January 2001.²⁴ The significance of this plan is the attempt by terrorist cells possibly independent of the organization’s command and control to adapt and innovate not only the means of attack but the tactics as well.

Additionally, there appears to be a general trend toward increasing cross-fertilization amongst terrorist groups. It is likely that as the war on terrorism reduces the ability of these groups to

¹⁹ Elaine Shannon, “Another warning from Zubaydah,” *Time*, May 11, 2002, available at <http://www.time.com/time/nation/article/0,8599,236992,00.html>, accessed November 12, 2002.

²⁰ Maria Ressa, “Building al Qaeda’s Asian terror network,” *CNN.com*, November 7, 2002, available at <http://asia.cnn.com/2002/WORLD/asiapcf/southeast/10/29/asia.jihad.2/>, accessed November 11, 2002.

²¹ Hoffman, “Lessons of 9/11,” p. 7.

²² “Terror alerts on small planes, scuba divers,” May, 26, 2002, available at <http://www.cnn.com/2002/US/05/26/terror.threats/index.html> accessed October, 25, 2002.

²³ “FBI Warns of Rail Threat,” *CBSNEWS.com*, October 25, 2002, available at <http://www.cbsnews.com/stories/2002/10/25/attack/main526923.shtml>, accessed November 14, 2002.

²⁴ *Patterns of Global Terrorism*, p. 38.

operate, they may begin to share expertise, training, materials, and even participate in each other's operations. This cross-fertilization has occurred in the past with groups such as the Palestine Liberation Organization (PLO), the Provisional Irish Republican Army (PIRA), and the Basque Fatherland and Freedom (ETA). However, al Qaeda's offer to train and equip other Islamic terrorist groups in exchange for their focus on Western targets represents a more concentrated and strengthened level of cross-fertilization. Indeed, terrorist groups in Southeast Asia, such as Jemaah Islamiya (JI), Kumpulan Mujahidin Malaysia (KMM), the Abu Sayyaf Group (ASG), and the Moro Islamic Liberation Front (MILF) in the Philippines illustrate that this type of cross-fertilization can have a significant and enhanced effect on group capabilities. For example, the MILF runs a training camp in the Philippines with funds from al Qaeda that both al Qaeda and the MILF can use to train not only themselves but other foreign terrorist groups, including the JI, in guerilla warfare and terrorism tactics.²⁵ In addition, a key member of the Abu Sayyaf Group, likely inspired by bin Laden and al Qaeda, was arrested in November 2002 for planning a series of bombings in Manila and the southern Philippines, including an attack on the U.S. Embassy. Two Yemeni nationals reportedly trained this ASG member with ties to the JI in explosive techniques.²⁶ Even groups that traditionally have not cooperated due to religious differences such as Hamas, al Qaeda, and Islamic Jihad (Sunni Muslim) and Hezbollah (Shiite Muslim) may be working together because their hatred for the West overcomes their dislike of each other.²⁷

A fourth trend is the continued evolution of "loose networks." Al Qaeda, for instance has direct influence over both its professional cadre, represented by terrorists such as Mohammed Atta and over the trained amateurs such as Ahmed Ressam,²⁸ but it also has indirect influence over a much larger group of people that range from local walk ins to like minded insurgents, guerillas and terrorists.²⁹

In such cases, group affiliations are not as clear and, therefore, it will be difficult for the U.S. government to determine responsibility for future attacks and response options accordingly. The disrupted terrorist plot against U.S. interests in Singapore in December 2001 is representative of this phenomenon. In this case, a network of extremists from throughout Southeast Asia worked in conjunction with al Qaeda leadership to plan an attack on the U.S. Embassy, a U.S. Navy ship, Navy personnel using the subway, and other facilities.³⁰ U.S. and Singapore intelligence eventually identified the JI as the primary group responsible. The JI relied heavily on al Qaeda operatives, however, for guidance and support and were acting as proxies of al Qaeda.³¹

²⁵ "MILF denies training camps used by al Qaeda," INQ7.net, September 18, 2002, available at http://www.inq7.net/brk/2002/sep/18/brkpol_10-1.htm, accessed November 20, 2002.

²⁶ Jess Liwanag, "Philippines arrests al Qaeda linked bomber," *CNN.com*, November 14, 2002, available at <http://www.cnn.com/2002/WORLD/asiapcf/southeast/11/14/phil.bomb.suspect/index.html>, accessed November 20, 2002.

²⁷ Hezbollah has recently been meeting in Lebanon with members of Hamas and Islamic Jihad and issuing joint press statements, *Martin*, December 4, 2002.

²⁸ Ressam was recruited into al Qaeda and trained in Afghanistan, but he was sent to the United States with open ended targeting instructions, whereas individuals such as Atta received plentiful resources and specific guidance on targets and tactics. Hoffman, "Lessons of 9/11," pp. 13-14.

²⁹ Local walk ins are local radical Islamic groups that look to al Qaeda for funding of their homegrown ideas. Like minded groups may have benefited from bin Laden's guidance and training and share his anti-American/anti-Western views. Hoffman, "Lessons of 9/11," pp. 14-15.

³⁰ Patterns of Global Terrorism, pp. 20-21.

³¹ *Ibid*, pp. 20-21.

Videotape was found amongst the rubble of the home of an al Qaeda leader in Afghanistan that showed surveillance footage of the intended targets in Singapore. Handwritten notes in Arabic that accompanied the tape were also discovered and revealed more details about the plot.³² This indicates that al Qaeda was intimately involved in the target identification and tactical decision-making. Yet what is most interesting about this plot, is that the JI had not previously been identified by policymakers as having an anti-U.S. agenda, again illustrating that loose networks can be difficult to measure in terms of threat salience.³³ Similarly, the string of attacks carried out earlier this year by Pakistani militants against Westerners in Karachi is another example where responsibility was not immediately clear. Because a number of terrorist groups are operating in Kashmir, most with predominantly local agendas, it was difficult to determine the perpetrators of these anti-Western attacks and therefore accurately assess future threats. The militants were eventually identified as belonging to a splinter group of the Harakat ul-Mujahedin (HUM), called the Harakat ul-Mujahedin al-Alami (HUM-A). This splinter group allegedly separated from the HUM because it wanted to focus more on Western, rather than local, targets. This group was responsible for the car bombing of the U.S. Consulate in Karachi in June 2002.³⁴ Most recently, in the attacks on the Israeli Hotel in Kenya suspicion has fallen on al Qaeda—al Qaeda communiqués have claimed credit³⁵—because of the earlier attack on the U.S. embassy in Nairobi in 1998. (But other suspects, such as Al Ittihad al Islami—a Somali group—and Hezbollah, have also emerged.³⁶)

Indeed, there are a number of loose networks of terrorists forming based on their common hatred of the West. This appears to signal that these organizations support bin Laden's "America first" policy, his goals of ousting pro-Western governments from the Islamic world, and the creation of a transnational Islamic Caliphate. Though the previously mentioned cooperation between Islamic extremist groups in Southeast Asia is the best example of how terrorists who subscribe to this ideology are creating new alliances, several Islamic extremist groups in Central Asia also decided to join forces in September 2002 to create a single Islamic terrorist entity, the Islamic Movement of Uzbekistan (IMU), which has ties to bin Laden, and encompasses separatists from Kyrgyzstan, Tajikistan, Chechnya, and the Xingjiang Province of China.³⁷

Despite the fact that some "loose networks" are forming around bin Laden's anti-Western agenda, it is also possible that other terrorist groups will return to their local goals, possibly because they no longer feel that pursuing an anti-Western agenda achieves their objectives or as a result of the pressure of the U.S. war on terrorism. This phenomenon may also indicate a failure on the part of al Qaeda to sell its propaganda of worldwide *jihad* and the restoration of the Islamic Caliphate to localized groups, as well as the success of the war on terror in deterring terrorist adversaries. Although al Qaeda wants groups affiliated with its organization to attack locally, because they know their own immediate environment best and can take responsibility, al

³² Ibid.

³³ Ibid, pp. 20-21, 123.

³⁴ CDI, "Action Update," Terrorism Project, October 22, 2002, available at <http://www.cdi.org/terrorism/actionupdate.cfm>, accessed October 29, 2002.

³⁵ "Al Qaeda Claims Kenya Attacks," December 3, 2002, available at <http://uk.news.yahoo.com/021202/140/dfvv0.html>; and "Al Qaeda Claims Role in Kenya Attacks," *Washington Post*, December 9, 2002 available at <http://www.washingtonpost.com/wp-dyn/articles/A27943-2002Dec8.html>

³⁶ Eric Lichtblau, "Striking 'Soft' Targets Complicates Security," *New York Times*, November 30, 2002.

³⁷ FBIS, "Russian Newspaper on Union of Islamic Movements in Central Asia," *Moscow Pravda*, September 16, 2002.

Qaeda wants these attacks to target Westerners, particularly Americans, in addition to their own governments. It does not further al Qaeda's global Islamic revolutionary goals for a particular Muslim group to reject the idea of targeting the West and to focus narrowly on obtaining power in Kashmir in isolation from the wider struggle. For example, since September 11, at least two Islamic terrorist groups that had previously been associated with al Qaeda have chosen to reject bin Laden's call for worldwide *jihad*. One of these groups, the HUM in Pakistan moved away from supporting bin Laden after 22 of its operatives were killed in U.S. air raids in Afghanistan, and its assets were frozen, arguably demonstrating the utility of direct pressure in combating terrorism.³⁸ Groups that turn inward to focus on local goals, however, often spur the formation of more extreme splinter organizations. If these splinter groups can muster resources and support, they can pose a serious threat to Americans and their interests. HUM's decision to reject involvement with al Qaeda sparked a split within the group, and the more violent HUM-A was formed. Since the HUM-A was created, it has conducted a number of attacks against Westerners and Christians in Pakistan, including the bombing of the U.S. Consulate in Karachi in June 2002.

Terrorists are also relying on new technologies, such as email, the Internet, and video/audio production, to enhance internal communications and spread their message to a variety of audiences to enhance recruitment, popular support, and intimidate their adversaries.³⁹ Although in al Qaeda's case this stems in part from a loss of a dedicated safe haven, it should be noted that this group has always been especially adept at external communications, public relations, and propaganda. While this innovation may increase the danger to Americans by rallying additional support to bin Laden and his cause, it may also provide a vulnerability that can be targeted in the war on terrorism because terrorists have become highly dependent on these communications technologies. Secure email, cell phone calls, and Internet communications have proven largely effective in the short run and have allowed terrorists to maintain the momentum they would surely have lost after the U.S. and allied bombing of Afghanistan last fall, had these technologies not been available for their use. Indeed, al Qaeda leadership has utilized both video and audiotapes more frequently since September 11 to send messages directly to their followers while at the same time also warning their adversaries. For example, Zawahiri gave a taped interview to al-Jazeera news network in October 2002 in which he addressed the U.S. and its allies directly:

Our message to our enemies is this: America and its allies should know that their crimes will not go unpunished... We advise them to hasten to leave Palestine, the Arabian Peninsula, Afghanistan, and all Muslim countries, before they lose everything.⁴⁰

To his followers, Zawahiri had praise and perhaps an indication of what the next al Qaeda targets might be:

³⁸ "Pakistan Arrests Bomb Mastermind," Associated Press, CBSnews.com, September 18, 2002, available at <http://www.cbsnews.com/stories/2002/09/25/world/main523196.shtml>, accessed November 14, 2002.

³⁹ Andrew Higgins, Karby Leggett, Alan Cullison, "How al Qaeda put the Internet to use," *The Wall Street Journal*, November 11, 2002, available at <http://www.msnbc.com/news/833533.asp?0si>, accessed November 20, 2002.

⁴⁰ FBIS, "Al-Zawahiri Says Bin Laden, Mullah Omar 'Enjoy Good Health,' Doha Al-Jazeera Satellite Channel Television Arabic, October 8, 2002.

The mujahid youths have addressed a message to Germany and another to France. If the measures have not been sufficient, we are ready...to increase them.⁴¹

At the time of this October 2002 interview, al Qaeda had claimed responsibility for an attack that same month against a French oil tanker and for the attack against German tourists at a Jewish synagogue in Tunisia the previous March. This method of communication serves two purposes: it boosts the morale of al Qaeda operatives who can no longer regularly meet with bin Laden and al-Zawahiri in Afghanistan, and it conveys the message to al Qaeda's supporters that the organization is still intact and that they are continuing to conduct successful operations. Easily accessible and widely used technologies, such as the Internet, also give terrorists the advantage of spreading the message that they want to send to counteract the often negative press that terrorism receives in the popular media.⁴² Al Qaeda and its affiliate organizations have used not only video and audio production to craft the message they want to send to their followers and the broader public, but have also created a number of websites to spread information.⁴³

The United States and its allies can exploit the inherent vulnerabilities of these technologies for intelligence gathering, especially as terrorists rely more upon these means, rather than direct face-to-face communications for operational planning.⁴⁴ Terrorists compromised in an attempt to circumvent electronic detection are also relying more heavily on trusted couriers to deliver important handwritten messages with information that terrorist leaders must have.⁴⁵ Another consequence of al Qaeda's awareness of Western intelligence gathering methods is the deliberate creation of disinformation and noise in the system to confuse and overwhelm intelligence agencies tracking terrorist communications.

Finally, it also appears that the threat from individual terrorists is increasing. A poignant example of this phenomenon is the case of Hesham Mohamed Ali Hadayet, the Egyptian who shot two Israeli agents at the El Al counter at Los Angeles International Airport on July 4, 2002.⁴⁶ It is important to note that the threat of individual attacks is not solely from al Qaeda and its affiliates. Individuals acting on their own without any particular group association and likely to sympathize with al Qaeda, the Palestinian cause, or any other grievance against the United States and its policies overseas also pose a threat. While individual terrorists are harder to detect and stop, individuals, particularly those who have very loose ties to terrorist organizations, are often not as well trained and are therefore more likely to fail or compromise their operations. They are also less likely to have the technical expertise to carry out large-scale operations on their own. Of particular concern to the United States are its own citizens who are loyal to, trained by, or

⁴¹ Ibid.

⁴² Bruce Hoffman, "Underground Voices: Insurgent and Terrorist Communication in the 21st Century," unpublished paper, August 2002.

⁴³ For example, www.jihad.net, www.mojahedoon.net, www.hizbollah.org, and www.jihad-online.com.

⁴⁴ Mike Williams, "Analysis: What next for al Qaeda?" November 22, 2001, http://news.bbc.co.uk/1/hi/world/south_asia/1678467.stm, accessed October 25, 2002.

⁴⁵ Peter Finn, "Al Qaeda Deputies Harbored By Iran," *Washington Post Foreign Service*, August 28, 2002, available at www.patriotdrive.com/waronterror/patriot/News/iranharbor.html, p. A01.

⁴⁶ "The FBI is investigating the July 4 double murder-suicide at Los Angeles International Airport as possible terrorism even though there's no evidence linking the alleged shooter to any terrorist group, a spokesman said Tuesday." Christopher Newton, "FBI Labels Inquiry Into Los Angeles Airport Shooting a Terrorism Investigation," Associated Press, September 3, 2002, available at <http://ap.tbo.com/ap/breaking/MGAGDWGGO5D.html>, accessed October 29, 2002.

inspired by al Qaeda, who are willing to act on his behalf both at home and abroad against Americans. It is to these and other threats in the United States that we now turn.

“Homegrown” Threats

Although significant and deserved focus has been directed at the danger posed by foreign terrorists coming from abroad, the panel believes it is important to remember the continued threat posed from domestic sources inside the United States. Globalizing factors have blurred some of the distinctions between strictly domestic versus international terrorism, and yet, the term “domestic terrorism” is still most appropriate in describing some of the threats internal to the United States, as discussed below.⁴⁷

Doubtless the greatest asset to al Qaeda today in striking in the United States would be the activation or recruitment of individuals who are American citizens. Of course, the threat is still significant from foreign elements attempting to infiltrate into the United States or from non-citizen “sleeper” agents who had even been put in place before September 11. U.S. citizens and legal residents, inspired by al Qaeda’s ideology, might serve as a support base—or possibly operatives—in future al Qaeda attacks. Arrests this year of terrorist suspects in Detroit, Michigan,⁴⁸ in Lackawanna, New York,⁴⁹ and in Portland, Oregon⁵⁰ are illustrative. The alleged “dirty bomb” plot of Jose Padilla (a.k.a., Abdullah al-Muhajir), an American citizen who apparently sought to carry out attacks against his country also demonstrates the potential threat, despite Padilla’s amateurish approach.⁵¹ Similarly, American citizens that support foreign interests other than al Qaeda, such as the Palestinian issue, may present a particularly difficult scenario to defend against because American citizens may not present as recognizable a threat. This is particularly pertinent given the recent “justification” for attacking American citizens by bin Laden.⁵² In this statement, the American people are singled out as specifically responsible for the actions of the U.S. government because of the democratic process in the United States, and thus the justification for targeting American citizens for al Qaeda terrorist violence has been specifically broadened.

In the past, Palestinian groups such as Hamas, Hezbollah, and the Palestinian Islamic Jihad (PIJ) have insisted that their attacks were part of a limited struggle against Israel.⁵³ While these groups have not agreed with U.S. government support for the state of Israel, they have not targeted U.S.

⁴⁷ The panel is aware of the current debate over the utility of these labels but finds the category helpful in making distinctions between those who might attack from outside the U.S. and those who originate their activities within the United States.

⁴⁸ See, BBC World News, June 11, 2002, *Profile: Jose Padilla*, available at, <http://news.bbc.co.uk/1/hi/world/americas/2037444.stm>

⁴⁹ U.S. Arrests Six in Probe of Possible al Qaeda Group, PBS Online News Hour, September 16, 2002, available at, http://www.pbs.org/newshour/updates/qaida_09-16-02.html accessed on December 2, 2002.

⁵⁰ See for instance, Daikha Dridi and Chris McGann, Infiltrator links men at Oregon ranch to al Qaeda, *Seattle Post Intelligencer Reports*, Tuesday, July 30, 2002.

⁵¹ Amanda Ripley, *Time*, June 16, 2002, “The Case of the Dirty Bomber: How a Chicago street gangster allegedly became a soldier for Osama bin Laden,” available at, <http://www.time.com/time/nation/article/0,8599,262917,00.html> accessed on December 2, 2002.

⁵² See, Observer Worldview, November 24, 2002, Translation of bin Laden’s Statement, available at, <http://www.observer.co.uk/worldview/story/0.11581.845725.00.html>.

⁵³ See for instance, Anders Strindberg, “Interview: ‘Imad al-’Almi, Hamas Chief Representative in Syria,” *Janes Intelligence Review*, Vol. 13, #12, December 2001, p.56.

citizens inside America.⁵⁴ In addition, as noted above, some individuals in these groups have called for a broadening of their strategy to include Americans. If bin Laden’s “justification” were to be adopted by Palestinian Islamic groups, the likelihood of increased terrorist activity in the U.S. would be quite significant. Acknowledging this possibility, the government would be prudent to recognize that a ready-made support system for anti-Israeli activism potentially exists in the United States in the form of some “Identity Theology” adherents.⁵⁵

The events of September 11 profoundly affected the worldview of many extremist groups within the United States. Many of these groups, such as the now dispersed Aryan Nations of Idaho and various Ku Klux Klan factions, have struggled to interpret the events in light of their Manichean⁵⁶ framework and anti U.S government rhetoric. Some of these groups, particularly the militias, neo-constitutionalists, and others focusing on Second Amendment rights, became for a time, less hostile toward the government following the attacks of September 11.⁵⁷ Factions within the militia movement have moved away from talking about wanting to carry out actions against the U.S. government since September 11 and are more inclined to see “foreign terrorists”—even those on their own soil—as the enemy.⁵⁸ On the other hand, some adherents of Identity Theology have seen the event as justifying their apocalyptic message.⁵⁹

The reorganization of the Idaho based Identity/neo-Nazi group, Aryan Nations, following the successful civil suit brought against the organization by Southern Poverty Law Center leader, Morris Dees, has created instability within the radical fringe of Identity believers formerly associated with this group.⁶⁰ As with the foreign terrorist groups discussed above, splinter groups can be more extreme, and various factions are currently vying for power in this arena, providing the opportunity for up-and-coming leadership to express commitment to their cause by carrying

⁵⁴ Certain Palestinian groups, such as Hezbollah, have targeted U.S. citizens outside of the United States, as in the 1983 attack on the Marine barracks in Lebanon. The panel is aware that there have been limited fundraising attempts in the U.S. on the part of some of these groups and that Hamas and Hezbollah are known to have cells in the United States. See for instance, James A. Damasak, “Cigarette Smuggling: Financing Terrorism?,” *Mackinac Center for Public Policy*, July 9, 2002, available at, <http://www.mackinac.org/4461>.

⁵⁵ Identity Theology is a dynamically evolving theological system based on the British Israel thought—the idea that the British and other Europeans are the “lost tribes of Israel,” rather than modern Jewish people. There are four distinct types of Identity theology, three of which pose a terrorist threat. Identity is the theological basis for groups such as Aryan Nations, Covenant, Sword, and the Arm (CSA) of the Lord, and many segments of the Ku Klux Klan (KKK). For a discussion of the different types of Identity theology see, David W. Brannan, “The Evolution of the Church of Israel: Dangerous Mutations,” *Terrorism and Political Violence*, Vol.11, #3, Autumn 1999, pp.106-118, Jeffrey Kaplan, *The Context of American Millenarian Revolutionary Theology: The Case of the ‘Identity Christian’ Church of Israel*. *Terrorism and Political Violence*, Vol. 5, Spring 1993, #1, or, Michael Barkun, *Religion and the Racist Right: The Origins of the Christian Identity Movement*. (Chapel Hill, NC: The University of North Carolina Press, 1997).

⁵⁶ Manichean worldviews are a form of Dualism and see every earthly act and situation as a struggle between good and evil. When a terrorist group is said to hold a Manichean world view, they are distinguished by their perception that the group’s view is accepted as “truth” or “good” while all other views are seen as “false” or “evil” and thus directly opposed to the group’s worldview.

⁵⁷ Based on interviews and informal discussions with various followers of these extremist groups from October 2001—October 2002.

⁵⁸ Statement of several unidentified militia activists, December, 2001, Springfield, MO.

⁵⁹ From a phone interview with Richard Butler, November 29, 2002.

⁶⁰ August Kreis attempted an internal coup and was ousted from the Idaho based group. Kreis has set up a rival faction in Leola, PA. Information on the rival Aryan Nations groups can be found at, <http://www.Aryan-nations.org>, or see, <http://www.twelvearyannations.com/> for Butler’s view of the conflict going on within Aryan Nations.

out increasingly violent attacks potentially against individual or government targets.⁶¹ Similarly, the death of National Alliance leader, William Pierce (1933-2002)—author of the influential and radical racist book, *The Turner Diaries*, which inspired Timothy McVeigh—has left a power vacuum that may lead to increased violence from the white nationalist movement.⁶² A more desirable option—that the group might lose direction and synergy following Pierce’s death—is also possible.

Anti-globalists continue to be a threat in the United States.⁶³ This hard to define collection of ideologies is a loose network rather than the traditionally defined cell structure. The violence they promote is often difficult to defend against as it may erupt during a legal protest by American citizens.⁶⁴ The loose confederacy created is comprised of coalitions between socialists, environmentalists and anarchists.⁶⁵ Earth First—the radical environmentalist group founded by David Broder—has been particularly active collaborating with anti-globalists. Similar concerns emanate from other environmentalist special interest groups such as the Animal Liberation Front, (ALF) and the Earth Liberation Front, (ELF), who have committed over 600 criminal acts in the United States since 1996, resulting in damages in excess of 43 million dollars.⁶⁶

In relation to the panel’s primary focus, that of countering the terrorist use of so-called “weapons of mass destruction,” the lack of strong centralized command and control has impaired many purely domestic groups from acquiring significant CBRN capabilities. But as the anthrax attacks in fall 2001 showed, even small scale attacks, in terms of casualties, can have a significant impact on the economy and public perception.⁶⁷ This does not mean that significant attacks will not come from radical domestic groups; rather, that it will be more difficult to detect an impending attack because it will likely emanate from individuals influenced by certain ideologies rather than coming from a “terrorist organization” *per se*. Timothy McVeigh exemplifies this threat. While not acting completely alone, he was also not part of an identified terrorist organization in the United States, yet he carried out the second largest terrorist attack on American soil.

We now turn to a specific look at the effect of the events since 1999 with regard to the CBRN threat.

⁶¹ The increased violence of groups that splinter from the parent groups has been seen in several venues, such as the Real IRA’s separation from the PIRA or the PFLP-GC’s separation from the PFLP.

⁶² While Erich J. Glibe has been appointed the new leadership of the National Alliance, there have been suggestions that long serving second-in-command, Billy Roper might split from the National Alliance to form his own group.

⁶³ “Anti-Globalists” emerged as a label, following the 1999, “Battle for Seattle,” the violent confrontation between anarchists, their supporters and police at the World Trade Organization (WTO) Summit in Seattle Washington.

⁶⁴ As in the case of the WTO Summit in Seattle, see for instance, WTO protests awaken 60’s style activism,” CNN.com, December 2, 1999, available at, <http://www.cnn.com/1999/US/12/02/wto.protest.perspective/> accessed on December 9, 2002.

⁶⁵ See a description of the network, Cindy Hasz, “Anarchists of Seattle are Headed to Washington,” *The American Reporter*, Vol. 6, No. 1288, March 15, 2000.

⁶⁶ “Inside the FBI: eco-terrorism,” *WashingtonPost.com*, February 27, 2002, available at, <http://discuss.washingtonpost.com/wp-srv/zforum/02/fbi0227.htm> accessed on December 9, 2002.

⁶⁷ See for instance, Bruce Hoffman, *Lessons of 9/11* (Santa Monica: RAND, 2002) p. 24 or *American Anthrax Outbreak of 2001*, available at, http://www.ph.ucla.edu/epi/bioter/detect/antdetect_intro.html.

The Threat of Unconventional Weapons

It continues to be surprising that the potential power of unconventional weapons remains largely untapped by terrorists. As the panel concluded in 1999, “the hurdles faced by terrorists seeking to develop true weapons of mass . . . destruction are more formidable than is often imagined.”⁶⁸ That conclusion is equally valid in 2002. As a U.S. General Accounting Office official testified to Congress last year, technical and operational challenges remain formidable obstacles to terrorist acquisition and use of unconventional weapons.⁶⁹ The observation made by the authors of *America’s Achilles’ Heel* four years ago remain valid: “A combination of motivational constraints and technological barriers explains why the thresholds to acquisition and use of NBC [nuclear, biological, chemical] weapons by non-state actors have almost never been crossed.”⁷⁰

Bin Laden has been quoted as saying that the procurement of unconventional weapons is a “religious duty.”⁷¹ But even al Qaeda, with its vast resources, global network of operators, and shadow businesses has so far seemed incapable of developing or acquiring a sophisticated chemical or biological weapons capability, although they have demonstrated an interest in doing so.

Although terrorists may be able to overcome technical and operational hurdles in the future, particularly if they receive assistance from states, they have historically employed explosives and firearms, which are easier to produce and use than unconventional weapons. The al Qaeda terrorists who killed nearly 3,000 at the World Trade Center did so using comparatively simple means—commercial passenger aircraft laden with jet fuel. They did not employ CBRN weapons, as many U.S. government officials feared al Qaeda might.

In this discussion, though, it is critical to separate intentions from capabilities. For a full discussion on the difficulties of obtaining and using chemical, biological (including against agricultural targets), radiological, and nuclear weapons, we direct you to the first panel report. The challenges outlined in that initial examination in developing or acquiring these weapons were reinforced by many of the events over the past three years. Changes in the appreciation of the threat from unconventional weapons with respect to major events related to terrorism are discussed below.

The Implications of September 11 and Other Recent Events for the Use of CBRN Weapons

September 11, 2001: Three aspects of the September 11 attacks have important implications for the possible terrorist use of CBRN weapons in the future. First, terrorists willing to destroy skyscrapers filled with people will probably not hesitate to use unconventional means to cause similarly high numbers of casualties if the groups were able to overcome the technical and

⁶⁸ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction [Gilmore Commission], *First Annual Report to the President and the Congress*, vol. I, *Assessing the Threat* (Washington, DC: RAND, December 15, 1999), p. 20.

⁶⁹ Henry L. Hinton, testimony before the U.S. Senate Committee on Governmental Affairs, October 17, 2001, GAO-02-162T, p. 4.

⁷⁰ Richard A. Falkenrath, Robert D. Newman, and Bradley A. Thayer, *America’s Achilles’ Heel: Nuclear Biological, and Chemical Terrorism and Covert Attack*, (Cambridge, Massachusetts: MIT Press, 1998), p. 28.

⁷¹ John J. Lumpkin, “Bin Laden sees ‘religious duty’ in targeting all Americans,” *The Associated Press*, September 28, 2001, http://www.oakridger.com/stories/092801/stt_0110040004.html, accessed December 6, 2002.

operational hurdles. Second, historically, terrorists who have sought to use unconventional weapons have failed to inflict the number of casualties these weapons could potentially cause because of a combination of their inflated expectations about their capabilities and the amateurishness of their effort.⁷² The September 11 attackers demonstrated patience, determination, and practicality that may enable their confederates to succeed in some future spectacular use of unconventional weapons where other groups have only been able to muster an amateurish level of attack. The motivations and determination of al Qaeda should not necessarily be interpreted as indicators of an inevitable escalation to using CBRN weapons. However, these aspects of the September 11 attack and the evidence discovered in Afghanistan of considerable interest in unconventional weapons bears attention. Finally, the September 11 attacks demonstrated that even al Qaeda, a terrorist organization with significant resources, both human and financial, chose to use a “conventional” weapon albeit with innovative *tactics* (fully-fueled airliners) to strike a symbolic target and kill a large number of people rather than using CBRN weapons. Al Qaeda has demonstrated that it can have mass effects—a significant disruption of society, huge economic losses, strong reactions by governments—without the necessity of using an unconventional weapon—a so-called “weapon of mass destruction.” Al Qaeda achieved “mass destruction,” by anyone’s logical definition, in September 2001.

Discoveries in Afghanistan: Many al Qaeda safehouses in Afghanistan contained documents the terrorists had collected from the Internet on nuclear, biological, and chemical weapons. Director of Central Intelligence (DCI) George Tenet told Congress that al Qaeda “was working to acquire some of the most dangerous chemical agents and toxins.”⁷³ He also testified that “[d]ocuments recovered from al Qaeda facilities in Afghanistan show that bin Laden was pursuing a sophisticated biological weapons research program.”⁷⁴ The DCI further stated that al Qaeda provided training in Afghan camps “in the production and use of toxic chemicals and biological toxins.”⁷⁵ Department of Defense officials had also indicated that evidence of al Qaeda’s efforts to acquire biological weapons (BW) was discovered, although they judged the capability as rudimentary.⁷⁶

The interest in acquiring a capability and actually using it are quite different propositions. Although Tenet categorized al Qaeda’s efforts as “sophisticated,” several U.S. officials have noted that the evidence discovered by American forces showed al Qaeda’s great interest in unconventional weapons, but little evidence of much success in acquiring the capabilities to use them. U.S. Secretary of Defense Donald Rumsfeld, has repeatedly stated that while there is evidence of considerable al Qaeda interest in unconventional weapons, nothing thus far suggests

⁷² See, Bruce Hoffman, *Terrorism and Weapons of Mass Destruction: An Analysis of Trends and Motivations*, RAND, P-8039, 1999, p. 34; and ; Jonathan B. Tucker, *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, (Cambridge, Massachusetts: MIT Press, 2000), pp. 256-257.

⁷³ Testimony of Director of Central Intelligence, George J. Tenet, Worldwide Threat--Converging Dangers in a Post 9/11 World, Senate Select Committee on Intelligence, February 6, 2002, available at http://cia.gov/cia/public_affairs/speeches/dci_speech_02062002.htm, accessed December 5, 2002.

⁷⁴ Testimony of George J. Tenet, Director of Central Intelligence, before the U.S. Senate Armed Services Committee, March 19, 2002.

⁷⁵ Written Statement for the Record of the Director of Central Intelligence, Joint Inquiry Committee, October 17, 2002, available at http://www.cia.gov/cia/public_affairs/speeches/dci_testimony_10172002.html accessed on December 5, 2002.

⁷⁶ Judith Miller, “Lab Suggests Qaeda Planned to Build Arms, Official Say, *New York Times*, September 15, 2002.

that the terrorists have been able to acquire or weaponize CBRN.⁷⁷ Even DCI Tenet's testimony reveals this distinction. He stated that the evidence proved only that they were "working to acquire" chemical agents and that they were "pursuing" a biological weapons capability—not that al Qaeda had been successful in either obtaining or fabricating on their own such weapons.

The CNN tapes of an al-Qaeda member killing a small dog with a toxic liquid provided gruesome confirmation of a crude capability to use toxic chemicals to kill.⁷⁸ This film footage—showing the agonizing death of a dog—confirms what Ahmed Ressay revealed in court testimony: in al-Qaeda training camps, trainers demonstrated how to use a toxic chemical, probably potassium cyanide, to kill small animals. Ressay testified that he was also instructed on how to introduce toxic chemicals into the air intake vent of a building.⁷⁹ While film footage and Ressay's testimony are disturbing, they reveal only a primitive capability to use toxic chemicals as a means of killing. Ressay's testimony about training with chemical agents in 1998⁸⁰ is consistent with discoveries made in Afghanistan in 2001 and 2002. This suggests, from available evidence, that al-Qaeda's chemical weapons capabilities remain unsophisticated.

If these efforts are indicative of the sophistication of al Qaeda's capability to use unconventional weapons, they are hardly different from previous attempts by terrorists to use these types of weapons. While the group has demonstrated interest in acquiring and using chemical, biological and nuclear weapons, our fears exceed what they seem capable of accomplishing *at this time*. Further, if a so well-funded and well-resourced an entity as al Qaeda has difficulty in building or acquiring significant unconventional weapons capabilities when they have both the motivation to kill as many Americans as possible and the resources to organize large-scale attacks, then it is unlikely that other less sophisticated or well-resourced groups, or those with less ambitious agendas, will be able, in the near future, to acquire or build a CBRN weapon that could kill people in large numbers without detection. Nevertheless, as we state elsewhere, terrorists may still attempt to use weapons, including CBR (but probably not N), with the intent of achieving "mass effect" but are unlikely to achieve "mass casualties" or "mass destruction." The danger, however, remains, that any nonstate adversary might acquire more sophisticated CBRN capabilities from the arsenals of established nation-states.

Anthrax attacks: The anthrax attacks last autumn represent another new development that must be taken into account as part of an assessment of the overall CBRN threat. While the attacks tragically killed five people and 17 others contracted the disease, these attacks caused far fewer casualties than the September 11 attacks, the African embassy bombings in 1998, the 1995 Oklahoma City bombing, or the 1993 World Trade Center bombing. Despite the significantly lower number of casualties, the anthrax attacks caused considerable public concern, but no real panic. Nevertheless, the government response in the aftermath of those attacks is another

⁷⁷ Transcript of testimony by Secretary of Defense Donald H. Rumsfeld, Defense Subcommittee of the Senate Appropriations Committee, May 21, 2002, available at www.defenselink.mil/speeches/2002/s20020521-secdef.html accessed December 6, 2002. See also, Transcript of DoD News Briefing featuring Secretary Rumsfeld and General Richard Myers, January 16, 2002.

⁷⁸ Dana Priest, "Archive of Al Qaeda Videotapes Broadcast, Dogs Shown Dying from Toxic Vapor," *Washington Post*, August 21, 2002, p. A13.

⁷⁹ Testimony of Ahmed Ressay, Prosecution Witness, *United States of America v. Mokhtar Haouri*, S400Cr.15(JFK), June 3, 2001, pp. 620-622.

⁸⁰ *Ibid*, p. 546.

example of the need for a more comprehensive understanding of such threats, better planning, and more effective communications.

Regardless of the perpetrator of the attacks (who at this writing is still unknown), the sophisticated nature of the material and its potency marks a watershed.⁸¹ Experts previously believed that a state weapons program could only produce this type of material. Similarly, most experts assumed that a state would not clandestinely attack for fear of retaliation.⁸² If the attacks are the work of a state or a state using a terrorist group to conduct the attacks, this is a new development.

If the attacks are the work of an individual, then this again points to the difficulty in tracking down and stopping a committed lone terrorist. A consensus is emerging in the U.S. government and among outside experts that the perpetrator or perpetrators had some connection to the U.S. biodefense program.⁸³ Those involved would be most likely to have the capability to produce such a weapon. If the perpetrator or perpetrators of the anthrax attacks are in fact “our own,” it raises fundamental issues about security at our Federal laboratories, personnel background screening, and the nature and scope of our defensive program. Alternatively, if the perpetrator is indeed a foreign state waging a covert attack against the United States, this is also a significant development. This case remains an important consideration in any threat assessment, although until the perpetrator is identified, it is difficult to know how to characterize the implications for the threat of the future use of biological weapons. Despite the tragic loss of life caused by the event, useful insight has been gained into the requirement to improve the capabilities of law enforcement authorities and public health officials to handle such an attack.

The Arrest of Jose Padilla: The threat of a radioactive dispersal device, or dirty bomb, was highlighted by the detention of Jose Padilla, an al Qaeda member who allegedly plotted to develop such a device in the United States to cause panic, death, and destruction. Despite initial indications to the contrary,⁸⁴ FBI officials now believe that the plot was never fully developed, and that Padilla was not a well-trained operative.⁸⁵ Although the Padilla plot did not have much substance, there are insufficient controls on access to radioactive material in the United States; this material may pose a threat in the future if acquired by people with nefarious objectives. In

⁸¹ Richard O. Spertzel, testimony before the House Committee on International Relations, “Russia, Iraq, and Other Potential Sources of Anthrax, Smallpox, and Other Bioterrorist Weapons,” December 5, 2001, available at www.house.gov/international_relations/sper1205.htm accessed December 6, 2002.

⁸² Richard A. Falkenrath, Robert D. Newman, and Bradley A. Thayer, *America’s Achilles’ Heel: Nuclear Biological, and Chemical Terrorism and Covert Attack* (Cambridge, Massachusetts: MIT Press, 1998), pp. 28 and 94. See also, Brad Roberts and Michael Moodie, “Biological Weapons: Toward a Threat Reduction Strategy,” *Defense Horizons*, No. 15 (Center for Technology and National Security Policy, National Defense University), July 2002.

⁸³ Barbara Hatch Rosenberg, “Anthrax Attacks Pushed Open an Ominous Door,” *Los Angeles Times*, September 22, 2002. See also, Nicholas D. Kristof, “Anthrax? The F.B.I. Yawns,” *New York Times*, July 2, 2002, p. 21; Laura Rozen, “Our Own Worst Enemy?” *The American Prospect*, Vol. 13, Issue 9, May 20, 2002, available at <http://www.prospect.org/V13/9/rozen-1.html> accessed April 24, 2002; Andrew Stephen, “America,” *New Statesman*, August 5, 2002.

⁸⁴ “Transcript of the Attorney General John Ashcroft Regarding the transfer of Abdullah Al Muhajir (Born Jose Padilla) to the Department of Defense as an Enemy Combatant,” June 10, 2002 available at <http://www.justice.gov/ag/speeches/2002/061002agtranscripts.htm> on December 5, 2002.

⁸⁵ Mark Hosenball, Michael Hirsh and Ron Moreau, “Odyssey Into The Shadows,” *Newsweek*, June 24, 2002. Kevin Johnson and Toni Locy, “Threat Of ‘Dirty Bomb’ Softened,” *USA Today*, June 12, 2002.

addition, U.S. officials have indicated that low-grade uranium-238 was discovered in tunnels in Afghanistan near a former al Qaeda base, enough to make one “dirty bomb.”⁸⁶

Use of Toxic Material as Weapons and Threats Against Industrial Facilities: In addition to more traditional chemical weapons, terrorists have shown an increased interest in employing toxic industrial chemicals, pesticides, and commercial poisons. The al Qaeda attack in Tunisia in which a gas truck was used as a weapon against a synagogue and the thwarted attack on a main gas storage facility in Israel may be a harbinger of attacks to come in the short- to mid-term.⁸⁷ There is a potential for an attack using industrial materials that can be as toxic as military grade weapons. An attack on a facility storing or manufacturing toxic materials could also produce substantial effects, potentially including mass casualties.⁸⁸ Security measures protecting these materials and controls on hauling them around the country continue to be weak and may not thwart the efforts of determined terrorists bent on using poison as a weapon.⁸⁹ The use of toxic materials by terrorists again represents a case where the United States has recognized a huge potential vulnerability, but where a clear threat from terrorists has not been demonstrated.

The Outbreak of Foot and Mouth Disease in the UK and the Threat to Agriculture: There have been no significant attacks on agriculture since the panel’s first report; however, the outbreak of Foot and Mouth Disease (FMD) in the UK in 2001 highlighted the potential economic consequences of a large-scale agricultural attack. This combined with the trend towards attacking economic targets noted above enhances the chance that America’s agriculture base may become a target.

The agricultural sector has still not received the focus that other infrastructures have received with regard to effectively developing vulnerability-threat analyses used to maximize both anti-terrorist contingencies and consequence management modalities. Agriculture and the general food industry remain critical to the social, economic and, arguably, political stability of the United States, yet there are significant vulnerabilities within the agricultural sector.⁹⁰ What makes the vulnerabilities inherent in agriculture so worrying is that the capability requirements for exploiting these weaknesses are not significant and certainly far less than those needed for a biological attack against humans. Notwithstanding its operational ease relative to other unconventional attacks, the ramifications of a concerted bio-assault on the U.S. meat and food base would be far-reaching and could easily extend beyond the immediate agricultural community to affect other segments of society.

Despite the relative ease by which an act of agroterrorism could be carried out and the severe ramifications that a successful assault could elicit, it has not appeared as a primary form of terrorist aggression. Traditionally, terrorist tactics have been designed to produce immediate, visible effects. In this light, it is perhaps understandable that biological attacks against agriculture have not yet emerged as more of a problem. Since 1912, there have been twelve documented cases involving the substate use of pathogenic agents to infect livestock or contaminate a related produce. Several could be termed terrorist in nature: the 1984 Rajneeshee

⁸⁶ Neil Doyle, “Al Qaeda Nukes Are Reality, Intelligence Says,” *Washington Times*, October 28, 2002, p. 17.

⁸⁷ John Kifner, “Israel Thwarts Bomb Attack, but Fears More to Come,” *New York Times*, May 25, 2002, p. 3.

⁸⁸ See <http://ifpafletcher.cambridge.info/transcripts/dallas.htm>.

⁸⁹ Andrew C. Revkin, “Little Done Yet to Keep Trucks from Terrorists,” *New York Times*, October 20, 2002, p. 1

⁹⁰ Ellen Shell, “Could Mad Cow Disease Happen Here?” *The Atlantic Monthly* 282/3 (1998): 92; “Stockgrowers Warned of Terrorism Threat,” *The Chieftain*, August 19, 1999.

salmonella food poisoning in Oregon; the 1952 Mau Mau plant toxin incident in Kenya,⁹¹ the Palestinian plot to poison Israeli oranges; and the Chilean grape scare.⁹² That being said, agroterrorism could well emerge as a favored form of secondary aggression designed to exacerbate the general societal disorientation caused by a more conventional campaign of bombings. The mere ability to employ cheap and unsophisticated means to undermine a state's economic base and possibly overwhelm its public management resources potentially give livestock and food-related attacks a highly attractive, cost-to-benefit payoff that would be of considerable interest to any group faced with significant power asymmetries. These considerations have particular pertinence to an organization, such as al Qaeda, which has repeatedly stated its intention to conduct economic warfare against the United States and explicitly endorsed the acquisition and use of biological agents to undermine American interests.⁹³ Though economic warfare has been threatened by al Qaeda, there has been no clear indication that they or other terrorists are currently interested in attacking agriculture on a large scale. Nevertheless, several factors, including our continuing success at forcing terrorists to change tactics and targets, could in the future cause them to consider this avenue of attack.⁹⁴

The Impact of State Assistance to Terrorist Groups on CBRN Acquisition

Terrorists might overcome some of the technical and operational barriers to weaponizing chemical, biological, and nuclear materials with assistance from a state's unconventional weapons program. Such assistance would be particularly important in the case of nuclear weapons. Obtaining such a weapon, or acquiring the fissile material required to build a crude nuclear device, remains arguably the most formidable hurdle for terrorists.⁹⁵ Even states have struggled to marshal the resources necessary to meet the technical and operational challenges, and the states that have acquired these capabilities are not known to have transferred the capability to terrorist groups.

However, the normative prohibition against states transferring CBRN weapons capability to terrorists may be eroding. President Bush has repeatedly indicated his concern over states that clandestinely seek nuclear, biological, and chemical weapons in contravention of a number of

⁹¹ The group used the African Milk Bush to poison 32 steer at a Kenyan mission. "W. Seth Carus, "Bioterrorism and Biocrimes: Illicit Use of Biological Agents in the 20th Century," Center for Counterproliferation Research, National Defense University, July 1999 revision, and Pushpraj Singh, "All About Agricultural Terrorism," November 15, 2001.

⁹² In the former, between 1977 and 1979, over 40 percent of the Israeli European citrus market was curtailed by a Palestinian plot to inject Jaffa oranges with mercury. The latter was a plot in 1989 by anti-Pinochet extremists to lace fruit bound for the U.S. with sodium cyanide. Import suspensions subsequently imposed by the U.S., Canada, Denmark, Germany and Hong Kong cost Chile in excess of US\$200 million in lost revenue earnings. See Ron Purver, *Chemical and Biological Terrorism: A New Threat to Public Safety*, Conflict Studies No. 295 (London: Research Institute for the Study of Conflict and Terrorism, 1996/1997), pp. 13-14; David Rapoport, "Terrorists and Weapons of the Apocalypse," paper presented before the "Future Developments in Terrorism" Conference, Cork, Ireland, March 1999, pp. 13-14; and "Plant Scientists Sound the Alarm on Agroterrorism," *The Philadelphia Inquirer*, September 13, 1999.

⁹³ "The World's Newest Fear: Germ Warfare," *The Vancouver Sun* (Canada), September 24, 2001; "Fear and Breathing," *The Economist*, September 29, 2001, p. 37.

⁹⁴ See Chapter VII, and Appendices E and F.

⁹⁵ Central Intelligence Agency, questions for the record from the Worldwide Threat Hearing before the Senate Select Committee on Intelligence, April 8, 2002, p. 7, available at http://www.fas.org/irp/congress/2002_hr/020602cia.html.

international agreements⁹⁶ and also that provide extensive support to terrorist groups.⁹⁷ In a similar vein, Secretary of Defense Rumsfeld testified that, “we have to recognize that terrorist networks have relationships with terrorist states that have weapons of mass destruction and that they inevitably are going to get their hands on them.”⁹⁸ During the Cold War, the Soviet Union and China supported a number of terrorist groups and insurgency movements that used terrorism as a tactic. The countries provided conventional arms, sanctuary, financing, intelligence, documentation, and logistics. Today, the states that are of greatest concern with respect to CBRN terrorism are Syria, Iran, and Iraq. All of these countries seek unconventional weapons capabilities or already possess them and have contacts with terrorist groups.⁹⁹ This danger is not inevitable, but neither can it be dismissed. Statements by the President and other officials may be “brightening” the red line of deterrence.

Among states that sponsor terrorism, Iran is the most active. Iran provides a full range of support to Lebanese Hezbollah and to a somewhat lesser extent Hamas, Palestinian Islamic Jihad, and military entities affiliated with the Palestinian Authority. While these terrorist groups have not traditionally attacked targets on U.S. soil, as noted above, at least some individuals within these groups are advocating broadening their objectives to global targets. In addition, Iran provides at least transit and temporary safe haven to some al Qaeda members and their associates. Groups supported by Iran were purportedly responsible for the devastating attack on U.S. interests at Khobar Towers in Saudi Arabia. The FBI argued in court documents that elements of the Iranian government were involved in the 1996 attack, which killed 19 U.S. service people and injured many more.¹⁰⁰ The case of Khobar Towers is a good example of how a faction within the Iranian government might have provided an unconventional capability to a terrorist group. This becomes more problematic if the faction within the government that controls part of the state’s unconventional weapons program provides unauthorized assistance to a terrorist group they sponsor.

After Iran, Syria is the most active state sponsor of terrorism and is included on the U.S. State Department list of state sponsors of terrorism. Libya is another country that has a history of supporting terrorism and is known to possess chemical weapons.

Iraq provides sanctuary to a number of notorious anti-Israeli Arab nationalist groups, but it is not nearly as active in its support as either Iran or Syria. Senior U.S. officials have stated that Iraq trained terrorists on how to handle chemical weapons.¹⁰¹ Some Iraqi defectors alleged that Iraq trained terrorists in the use of chemical and biological weapons.¹⁰² Iraq’s defeat in the Gulf War and repeated American military attacks in the years following the war undoubtedly have boosted Iraqi dictator Saddam Hussein’s intense hatred of the United States. Yet, despite Hussein’s

⁹⁶ Including the Nuclear Non-Proliferation Treaty, the Chemical Weapons Convention and the Biological Weapons Convention.

⁹⁷ Office of the Press Secretary, “President Delivers State of Union Address,” January 29, 2002, [<http://www.whitehouse.gov/news/releases/2002/01/20020129/11.htm>.]

⁹⁸ Transcript of testimony by Secretary of Defense Donald H. Rumsfeld, Defense Subcommittee of U.S. Senate Appropriations Committee, May 21, 2002.

⁹⁹ U.S. Department of State, *Patterns of Global Terrorism* (2001), available at <http://www.state.gov/s/ct/ris/pgtpt/2001/htl/10249.htm> accessed on December 6, 2002.

¹⁰⁰ Elsa Walsh, “Louis Freeh’s Last Case,” *The New Yorker*, May 14, 2001, pp. 68-79.

¹⁰¹ Interview with Dr. Condoleeza Rice, National Security Advisor, *The News Hour*, September 25, 2002.

¹⁰² Gwynne Roberts, “Militia Defector Claims Baghdad Trained Al Qaeda Fighters in Chemical Warfare,” *London Sunday Times*, July 14, 2002, p. 23.

motivation to use terrorist forces as a vector against the United States and the possibility that Iraq could transfer unconventional weapons capabilities to terrorist groups for their own purposes, there is no consensus that this has occurred.

Given the weapons ambitions of these states and their contacts with terrorist groups, the possibility of transfer of CBRN weapons between these states and terrorist organizations requires careful attention. While the danger remains that the context may change and these states will view transfers of unconventional weapons to terrorist groups as in their interest, there is no evidence that they have yet done so. The United States should work to maintain this prohibition.

Unauthorized assistance by weapons scientists from some of the newly independent republics of the former Soviet Union may also enable terrorists to develop an unconventional capability on their own. There are reports, for example, of Russian biological weapons scientists helping Iran.¹⁰³ While these reports are disturbing, the contact is believed to have been limited in scope and was discontinued after American officials brought the contacts to the attention of Russian scientific officials.¹⁰⁴ Over the decade since the collapse of the Soviet Union, Russia has experienced severe economic troubles. While some nuclear smuggling and brain drain has occurred, it is difficult to “know the extent or magnitude” of these developments, much less to assess their actual implications on both rogue state and nonstate acquisition efforts.¹⁰⁵ Al Qaeda’s attempts to cultivate its own expertise in CBRN manufacturing and deployment, however, indicates that the threat of proliferation of Soviet expertise in this area may have been overblown. The potential danger remains, but it should be viewed in the context of the last ten years, during which a multitude of cooperative threat reduction programs have thus far thwarted this danger and managed the threat alongside the improvement of conditions in several of the former republics of the former Soviet Union, most notably Russia. The threat has not materialized, as many officials and analysts feared a decade ago; but continued vigilance is required.

Conclusion

The anthrax attacks of 2001 have continued to keep much of the U.S. focused on the potential for terrorists to employ unconventional weapons. However, our analysis of the threat indicates that terrorists intent on conducting future mass casualty attacks are more likely to use conventional than sophisticated CBRN weapons in the near term. September 11 illustrated that terrorists can achieve a high number of casualties and widespread panic without the difficulties involved in a sophisticated CBRN attack. Furthermore, the few deaths resulting from the anthrax attacks carried out in the United States in the fall of 2001 reinforced the idea that conventional attacks at this stage are likely to produce a larger number of casualties. Outside of al Qaeda and some of its affiliate groups, such as the Egyptian Islamic Jihad, that have acquired at least a crude CBRN capability, only a limited number of groups have access to this material and are capable of

¹⁰³ Judith Miller, Stephen Engelberg, William Broad, *Germs: Biological Weapons and America’s Secret War* (New York: Simon & Schuster, 2001), pp. 205-207.

¹⁰⁴ Ibid.

¹⁰⁵ National Intelligence Council, Annual Report to Congress on the Safety and Security of Russian Nuclear Facilities and Military Forces, February 2002, available at http://www.ciagov/nic/pubs/other_icarussiansecurity.htm accessed December 6, 2002. See also, Emily S. Ewell, “NIS Smuggling since 1995: A Lull in Significant Cases?,” *The Nonproliferation Review*, Spring-Summer 1998, Vol. 5, No. 3, pp. 119-125.

conducting attacks of this type inside the United States.¹⁰⁶ As a result, fundamental analysis of the first report of the panel remains valid today, albeit colored by some the trends noted above, especially toward increasing lethality.

A better understanding of why terrorists do or do not opt for unconventional weapons may provide direction for strengthening policy measures that will continue to deter terrorist use of these weapons. The “worst-case” scenario approach that has dominated certain U.S. planning and preparedness has resulted in several decisions that may have been made differently if other policies were based on a wider range of scenarios.¹⁰⁷

The current threat of terrorist acquisition and use of chemical, biological, radiological or nuclear weapons to cause “mass casualties” or “mass destruction” remains, on balance, a lower risk than other means terrorists might use to inflict mass casualties. That said, terrorists may choose the use of an unconventional weapon, especially a chemical or biological one, perhaps even a small-scale radiological one, that can still cause “mass effects” in terms of psychological, sociological, or economic damage. Policymakers should continue to plan for increases in the volume and lethality of terrorism and for attacks across the entire spectrum of weapons (including CBRN), tactics, and targets. In addition, with the passage of time, it becomes more likely that terrorists could have access to or the ability to create and then use unconventional weapons with a mass effect.

Significant efforts have been undertaken to deter, detect, interdict, prevent, and develop response capabilities for terrorism in the intervening three years; however, much remains to be done. This is the subject of the remainder of the report.

¹⁰⁶ U.S. General Accounting Office, *Combating Terrorism: Linking Threats to Strategies and Resources*, GPO Access. July 26, 2000, available at <http://www.gao.gov/new.items/ns00218t.pdf>, accessed October 29, 2002.

¹⁰⁷ See, for example, the argument in Hoffman, “Lessons of 9/11,” (pp. 19-20) that planning would benefit from an approach that, in addition to asking the usual questions of “what could or what might happen?,” attempts also to inquire “what hasn’t happened, or what type of attacks have terrorists only perpetrated rarely?,” and then to walk-backward analytically in assessing these potentialities as a way of obtaining a better understanding of the capabilities and resources required by terrorists to carry out a range of nontraditional attacks.

CHAPTER III. APPLYING CROSS-CUTTING THEMES

Each subsequent chapter of this report will address issues in various functional areas. We have identified several cross-cutting themes that may be related to any number of the issues we address. Where they are applicable, we will highlight those themes in each chapter. Here, we explain our rationale for each of those thematic topics.

Protecting Our Civil Liberties

The civil liberties of all U.S. persons have been paramount in all of the panel's deliberations and are always a key consideration in each recommendation that we make. The Constitutional protections that we enjoy are what make our country unique in all the world. No other country has the same degree of protections or takes the pains to ensure their strict enforcement as ours. We have previously quoted our founding fathers as guiding lights for the consideration of these difficult issues. One of the most appropriate:

They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety. *Benjamin Franklin, 1759.*

We firmly believe that it will not be necessary to “give up essential liberty” to achieve a marked increase in our security. We have previously recognized that 100 percent security will be unattainable if we maintain our uniquely American way of life. Americans understand and accept that. They only ask of their governments that the most effective measures that can be taken within the context of our Constitutional protections be implemented.

At the same time, the vast majority of Americans understand that for every civil right a corresponding obligation exists; for every privilege there is usually some cost. Driver licenses are not a civil right; they are a privilege that require testing and normally proof of age and photographic identification. Airline travel is not a civil right; it is a privilege that subjects us to what, in other contexts, would be considered an unlawful search.

Striking an appropriate balance will always be a challenge, but we are convinced it can be done. Our analysis indicates that all of the legislation enacted in the aftermath of the attacks of last year—the USA PATRIOT Act and several others—are likely to pass Constitutional muster. Our concern continues to be that we pass legislation that addresses remaining security issues in other than crisis times. Responding to the next crisis after it occurs may run the greater risk of impinging upon our important Constitutional protections.

Enhancing State and Local Capabilities

It is our principal legislative mandate to assess Federal programs for their effectiveness for improving the ability of States and localities to respond to terrorist attacks. Our States and communities must have the knowledge and the resources to fulfill their critical roles in the national effort.

We have from the beginning of our deliberations maintained a key set of principles that have guided our deliberations in this regard:

- All terrorist incidents are local or at least will start that way. Effective response and recovery can only be achieved with the recognition that local responders¹⁰⁸ are the first line of defense and through the proper integration of State and Federal assets into existing response networks.
- Building effective and sustainable response and recovery capabilities requires an “all-hazards” approach that integrates planning and response with existing processes.
- To be most effective, plans and programs for combating terrorism should build on existing State and local management structures and command and control mechanisms.
- Capabilities for combating terrorism should be designed to the greatest extent practicable for dual- or multi-purpose applications, for maximum utility and fiscal economies of scale.
- Effective preparedness for combating terrorism—planning, training, exercises, and operational structures—requires a fully integrated network of Federal, State, and local organizations. At the local level, this network includes the traditional “first responders”—law enforcement, fire, and emergency medical services personnel—and also *must* include other State and local agencies, such as public health departments, hospitals and other medical care providers, and offices of emergency management.

For this report, we add another:

- The effectiveness of programs should be based on carefully crafted, well-understood measures of performance. Without such metrics, we will be relegated to determine effectiveness based the amount of money being spent.

For those reasons, we have consistently adhered to the view that all strategy and programs for combating terrorism inside the United States must be approached from the “bottom up”—starting from the viewpoint of the localities and States, not from a Federal, or “top-down” perspective. As a current example, much of the resources to protect critical infrastructures come from State and local governments, yet the flow of information and certain resources is currently a “top-down” approach—Federal to private sector with minimal State and local engagement. States and localities must be intimately involved in these efforts.

During the current report period, we updated the major nationwide survey that we conducted for our Third Report, by returning to the same survey audience of State and local responders to find out what, if anything had changed. The results are telling. Throughout this report, as appropriate, we include analysis from the most recent survey in each of the substantive chapters, and also include a full analysis of the survey results at Appendix D.

¹⁰⁸ As noted in its *First Annual Report*, the panel has chosen to use “local responders”—as opposed to “first responders”—to characterize those persons and entities most likely to be involved in the early stages following a terrorist attack. That characterization includes not only law enforcement, fire services, emergency medical technicians, emergency management personnel, and others who may be required to respond to the “scene” of an incident, but also other medical and public health personnel who may be required to provide their services in the immediate aftermath of an attack.

Improving Intelligence and Information Sharing

Intelligence—its timely collection, thoughtful analysis, and appropriate dissemination—is the key to effective prevention of terrorist attacks. From the inception of our deliberations, we have said that “more can and must be done to provide timely information—up, down, and laterally, at all levels of government—to those who need the information to provide effective deterrence, interdiction, protection, or response to potential threats.”¹⁰⁹ While improvements have been made, that statement is still true today.

The creation of the Foreign Terrorist Tracking Task Force and the U.S. Attorneys Antiterrorism Tasks Forces, the expansion of the regional Joint Terrorism Task Forces (JTTF) and the creation of a National JTTF, and the enhancement of other Federal interagency mechanisms are all important steps. What is unclear is how all of those entities will necessarily be coordinated.

We have made several recommendations in previous reports about ways to improve the sharing of intelligence and other information horizontally and vertically among government entities and which now increasingly must include certain entities in the private sector. We make explicit recommendations in this report, especially in the Strategy and Structure chapter, for additional improvements in those processes.

Promoting Strategic Communications

The attacks of 2001 hopefully have taught us important lessons about the ways in which governments talk to the American people about homeland security issues.

Effective communications serve a variety of salutary purposes:

Preparedness: In the period before a terrorist incident, public communications contribute to preparedness by educating the public and the media about the types of events that might occur, how the government would respond to them, and most importantly, steps the public can take to reduce their personal risk to terrorist impacts. In this way, members of the media will develop an understanding of the types of information that will be important during a terrorist event. And members of the public will be educated about the types of actions that will be required, and the resources that will be available for recovery.

Deterrence: Public communications may play a role to deter terrorist plans if they convey the scale of preparedness, capabilities to limit impacts, and reduced levels of vulnerability. Ideally, this element of public communication would coordinate with other deterrent strategies, most importantly implementing appropriate security measures. The deterrent role of public information can occur at all times: as part of preparedness efforts before a terrorist incident, in the communications immediately following an incident, and as part of long term recovery efforts.

Reassurance: In the time immediately following an event, it is most critical that communications contribute to public reassurance and calming. This can be accomplished through a number of ways: by establishing a sense of control and authority over the current situation, by conveying

¹⁰⁹ *First Report*, p. 57.

the scale of emergency management operations, and demonstrating that the government is working to prevent further terrorist attacks.

Conveying key information: Following certain types of events, there will be a need to communicate with the public to limit the scale of the impacts and to speed recovery. This will be especially critical following a chemical or biological events where there will be a need to limit exposures to hazard materials, direct populations toward medical treatment, and limit the spread of disease. To carry out these tasks, it will be critical to have strong coordination between public communication efforts and internal incident management and public health communication systems (e.g., the Health Alert Network).

There are three temporal components of an effective communications strategy:

- **Pre-Attack**—Those programs to educate the American public, including the media, on the causes and effects of various terrorist attacks. Some have argued that trying to explain to potential for loss of life from unconventional attacks, especially those with biological agents, will cause unnecessary fear among our fellow citizens. We disagree. We trust the common sense and resiliency of the American people to understand and process information on such threats. The challenge will be to “package” that information in ways that will be most effective. The media should be a central part of that educational process. It is essential to build public trust in government and its pronouncements before attacks occur.
- **Trans-Attack**—Critical communications as an event is unfolding to lessen public panic and mitigate loss of life and injury. National, State, and local leaders must develop processes for determining, based on different scenarios, who will speak on behalf of each level of government and then exercise those plans prior to events occurring. Advance planning and exercises for communications trans-attack are especially critical for bioterrorist incidents.
- **Post-Attack**—Effective communications in a post-attack environment to restore public confidence, to mitigate further damage, and to facilitate recovery operations. While this area of communications strategy is more mature, based on the nation’s experiences with natural disasters, more needs to be done to plan for more effective communications in the aftermath of an attack by terrorists. The government communications following last fall’s anthrax attacks demonstrate of why we need improvements.

Additional proposals for improving strategic communications are discussed in considerable detail in Appendix H.

Enhancing Coordination with the Private Sector

National security is no longer solely the purview of the Federal government, as it was during the Cold War. The private sector controls approximately 85 percent of the infrastructure in this country and employs approximately 85 percent of the national workforce. It is also critical to innovations to protect and defend against terrorism. The *National Strategy for Homeland Security* includes as one of its precepts a coordinated government private sector effort to combat terrorism. As defined in the *Strategy*, the Federal government and the DHS are focusing on protecting vulnerabilities of critical infrastructures. This leaves significant gaps in areas where government private coordination and cooperation is essential, including the innate

interdependencies of their functions and the need for businesses to plan to protect the 122 million people they employ.¹¹⁰ Gaps in these areas will undermine efforts to secure the homeland.

The *Strategy* does not explicitly recognize the dependence of the Federal government on the private sector in responding to a terrorist event. When the national airspace was shut down to commercial traffic following the September 11 attacks, both the government and the private sector were significantly effected by the limited ability to move people and goods.¹¹¹ Military planes performed some of the critical transportation functions, but actions were hampered. One intimate example the transportation shutdown hindered the delivery of life-saving products is the case of Jurgen Kansog, a New Jersey resident. On September 11, 2001, he was one of several patients anticipating the arrival of life saving blood stem cells from overseas. He had already undergone exhaustive chemotherapy and radiation treatment and without the stem cells, which only survive for a limited time after donation, he was likely to die. Because no plan was in place that anticipated the shutdown of all air traffic, the National Marrow Donor Program and others had to work quickly to find a way to transport the cells. In the end, they secured “lifeguard status” from the Federal Aviation Administration (FAA) and used a chartered jet to deliver the material.¹¹²

Understanding the requirements for obtaining “lifeguard status” is one example of how private and public organizations should work together to plan contingencies that explicitly identify critical interdependencies and solutions ahead of time. A second example of the interdependence is the destruction of significant communications nodes at the World Trade Center, which again impaired both government and private sector response functions.¹¹³ If larger sections of the telecommunications infrastructure were impaired or destroyed, the impact would have been even more significant than that felt from the limitations on civilian airliners because the government does not have pervasive backup systems as it does in the case of air transport.¹¹⁴ The lack of recognition of the critical interdependencies means that such contingencies as the one described above are not explored, well planned for, or exercised.

The *Strategy* also remains silent on the fact that should a terrorist attack occur, it is likely that many people will be at their places of employment and, thus, the inclusion of the private sector in planning for terrorism is critical to ensure the safety of the private workforce. The government already plans for the safety and security of the Federal civilian workforce who numbered nearly 2.7 million (325,000 in the Washington DC Metropolitan area alone¹¹⁵) in

¹¹⁰ Available at <http://www.bls.gov/opub/rtaw/pdf/intro.pdf> accessed December 2, 2002.

¹¹¹ Prior to September 11, the National Airspace System, also know as the “NAS,” handled 1.9 million passengers, 40,000 tons of cargo, and 60,000 flights through the system daily. Data from Claire D. Rubin and Irmak Renda-Tanali, “Quick Response Report #140,” Natural Hazards Research and Applications Information Center, 2001, available at www.colorado.edu/hazaeds/gr/gr140.html, accessed on December 2, 2002.

¹¹² “A Life Saved Hope in the Face of Tragedy,” National Marrow Donor Program, <http://www.marrow.org/NEWS/ARTICLES/lifesaved09102002.html>.

¹¹³ The attacks resulted in the loss of five phone-switching stations, two electrical substations, 300,000 telephone lines, and 33 miles of cable. It has been estimated that replacing the destroyed subway lines would cost around \$3 billion and that utility repairs, including 300,000 telephone lines, one phone switching station, and six miles of electrical cable are estimated to cost \$2 billion. Data from report #140.

¹¹⁴ It is widely reported that 99 percent of government communications is on the publicly switched network, which is owned by the private sector.

¹¹⁵ “Federal Civilian Workforce Statistics, The Fact Book,” 2002 Edition, Owi-02-02, U.S. Office of Management And Budget.

2001.¹¹⁶ Private sector planning saves lives. For instance, on September 11, 2001, the emergency response plans or the actions of leaders within companies of the businesses occupying the World Trade Center likely contributed to the relatively successful evacuation of thousands of workers from the buildings.¹¹⁷ After saving lives, companies then turn to restoring their business functions. Many of the WTC firms began operating relatively quickly after the attacks because of emergency planning that began after the 1987 stock market crash and picked up after the 1993 World Trade Center bombing. However, more lives may have been saved and less money lost if the public and private planners had focused on joint preplanning, exercising, and training.

While the *National Strategy* recognizes the need for inclusion of the private sector in the government's anti-terrorism planning, it is short on details, and an analysis of efforts in this area shows that with the exception of health and medical initiatives, the Federal government does not have a history of cooperative, strategic efforts with the private sector for terrorism preparedness and response. Two areas where the Federal government and private sector work together relatively well are noteworthy, purchasing of goods and services through contracts and grants and protection of vulnerabilities in critical infrastructure, but long-term, strategic partnerships are lacking.

This may change with the creation of DHS. In Section 430 of the bill creating the Department of Homeland Security, the Department is given responsibility for "the preparedness of the United States for acts of terrorism, including. . .coordinating preparedness efforts at the Federal level, and working with all State, local, tribal, parish, and private sector emergency response providers on all matters pertaining to combating terrorism, including training, exercises, and equipment support."

States and localities have a longer history of working with the private sector, primarily on the basis of personal relationships. These entities are currently working together in many cases¹¹⁸ to develop terrorism prevention and response plans.

Examples of specific public private initiatives are discussed in the appropriate chapters.

¹¹⁶ There are almost 15 million State and local government civilian employees. Table C-5, Statistical Review Of Government In Utah 2000, Data From U.S. Bureau of the Census, Public Employment Series. The Utah Foundation, available at www.Utahfoundation.Org/Stat_Review/Section_C/UF%20stat%20review%20table%20c5%200101.Pdf accessed December 1, 2002.

¹¹⁷ More than 430 companies from 28 countries and employing approximately 50,000 people occupied the World Trade Center.

¹¹⁸ With the exception, noted above, of direct Federal to private sector on certain critical infrastructure issues.

CHAPTER IV. RESOURCING THE NATIONAL EFFORT

In our previous reports, we have discussed in general terms the types, levels, and targets of Federal funding for combating terrorism. Prior to the attacks of 2001, we suggested that the total *amount* of funding was not as important as the necessity to prioritize funding and direct resources to those areas most in need. We reaffirm that prior conclusion.

In the aftermath of the 2001 attacks, Congress appropriated roughly \$40 billion in emergency supplemental funds, of which a little less than \$11 billion was for domestic or “homeland security” programs¹¹⁹—only \$240 million of that being specifically allocated directly to States and localities for enhancing preparedness. In the President’s budget request for Fiscal Year 2003, \$3.5 billion is intended to be provided directly¹²⁰ for State and local preparedness.¹²¹ With this massive infusion of additional Federal resources, setting priorities and applying realistic measures of effectiveness are even more important. For more detailed budget information, see Appendix O.

Rationalizing the Process—States Versus Localities

There is a current and pointed debate about the method or methods for moving Federal resources to State and local response agencies—especially those intended for the local level. States and localities are very much at odds over the way in which Federal funds should flow. The stark level of that disagreement was made apparent to this panel in materials provided to us during the course of our deliberations, especially at our meeting in June of this year, when representatives of organizations of State entities on the one hand and local entities on the other pointedly presented their respective positions to us.

Many localities and the response organizations within them argue that such Federal funds, or at least some sizable portion of them, should be channeled directly to the localities, bypassing any measure of State control. The rationale for that argument is that States will “siphon off” too large a share of those resources for applications at the State level and that localities will, therefore, not receive the levels of funding necessary to improve preparedness significantly or that State agencies can delay the timely application of resources.

There is some merit to that argument, based on certain historical precedents in other contexts. Nevertheless, we continue to adhere to the view that Federal funds provided for the purpose of improving local capabilities must be subject to a level of prioritization.¹²² The only logical way to do that, in our view, is for States to exercise some degree of oversight over the application of

¹¹⁹ Approximately \$8.2 billion was designated as assistance to Pennsylvania, New York, and Virginia to aid in the immediate mitigation and response activities, and an additional \$2.5 billion was made available to HHS as part of its emergency fund to assist the Federal, State, and local public health system

¹²⁰ An additional \$1.2 billion has been requested to increase hospitals’ capacity to respond to bio-terrorism incidents, and \$175 million to improve interoperability in communication networks between Federal, State and local entities.

¹²¹ At the time of the writing of this report, the Congress has passed only two of thirteen regular appropriations bills for Fiscal Year 2003.

¹²² See our *Third Report*, at p. 10.

such funds to ensure that resources are allocated on the basis of assessed needs.¹²³ That view has been correctly, we believe, adopted as the general rule by the current Administration.¹²⁴

We have resisted a “one size fits all” approach to this problem. Indeed, every city of a certain population size does not necessarily have to own a specific set of equipment. That is especially true where a number of municipalities make up a larger metropolitan area. Some municipalities and counties have been smart—even in the absence of definitive Federal guidance—in setting up mechanisms for pooling resources and providing mutual assistance in an emergency.¹²⁵ In many cases, those mechanisms have been facilitated by broader State level mutual aid efforts. A designated State agency—most likely its emergency management agency or homeland security agency or coordinator—is logically in a position to understand needs on a statewide basis and, therefore, be able to articulate more effectively the requirements and priorities for Federal assistance. Determinations in such areas as standardization and interoperability can more effectively be made at the State level as well. The responsibility for overall preparedness within a State ultimately rests with the Governor.

Furthermore, Federal resources should not be distributed to those localities that happen to have the best grant-writers. With 3,141 counties jurisdiction and more than 600 municipalities with a population over 50,000, the Federal government cannot be expected to prioritize allocations for that many jurisdictions. It can, however, make rationale decisions for the application of Federal dollars based on comprehensive State-by-State assessments of capabilities and requirements.

By the same token, States must be held to some reasonable standard in withholding, at the State level, any portion of funds are intended exclusively or primarily for improving local capabilities. It is logical to us that States should be expected to assist in facilitating responses to terrorist attacks that may exceed local capabilities, either through the provisions of State-level response or by coordinating supporting response capabilities from other jurisdictions within the State that is the target of the attack or from neighboring States under mutual assistance compacts.

As a general rule of thumb, we believe that States should not withhold at the State level more than 25 percent of Federal funds that are exclusively or primarily intended for improving local and/or State response capabilities. For those activities where funding is available for combined State and local efforts, the State’s share should be no more proportionally that the level of effort of State entities in such combined efforts. In each case, justification for the allocation of funds should be comprehensive and transparent, and periodic reporting and other audit mechanisms should be used to ensure the appropriate expenditure of Federal resources. States must be required to develop comprehensive strategies, combining both local and State-level capabilities and requirements. Those State strategies must be tied to the imperatives in the *National Strategy* and must be updated on an annual basis.

¹²³ For an excellent discourse on the subject, see Spencer S. Hsu and Lyndsey Layton, “Scattershot Spending in Terror Fight,” *Washington Post*, September 10, 2002, page A1.

¹²⁴ For a contrary view, see Sen. Hillary Rodham Clinton, “First Things First,” *New York Daily News*, November 21, 2002, available at http://www.nydailynews.com/news/ideas_opinions/story/38008p-35892c.html.

¹²⁵ We have previously noted the Los Angeles Operational Area entities as models in this regard. They still are.

Establishing Appropriate Burden Sharing

In our Third Report, we listed several guiding principles when considering measures for improving State and local capabilities.¹²⁶ Among them:

- *Governments at all levels must share in the costs of domestic preparedness and response, but the Federal government should be prepared to provide resources for the “incremental” or “exceptional” costs of combating terrorism beyond those normally required for public health and safety.*

States and localities clearly have the primary burden of providing resources for the health and safety of its citizens. The response capabilities that will inevitably be brought to bear in the event of a terrorist attack—hopefully only very rarely—are for the most part capabilities that are used daily for other purposes—law enforcement, fire services, public health, emergency medical services, primary and emergency medical care, and emergency management of natural disasters. That is logically—and preferably—the case: response capabilities based on an “all-hazards” approach. But it will be a rare case, indeed, where an act of terrorism will not rise to some level of national importance.

While it is appropriate that States and localities should continue to share a portion of preparedness and response for programs to combat terrorism, we believe that a good general rule for the State share of funding as a condition for receiving Federal assistance should be no more than 25 percent and that, where appropriate, such share may be through “in kind” resources. As we stated earlier with respect to the method of funds for States and localities, justification for the allocation of funds for Federal-State burden shared programs should be comprehensive and transparent, and periodic reporting and other audit mechanisms should be used to ensure the appropriate expenditure of Federal resources.

Ensuring a Central Focus

We continue to suggest that setting priorities and allocating resources according to those priorities is essential to an effective national effort to combat terrorism. The establishment of the new Department of Homeland Security (DHS) will hopefully achieve some measure of more effective priority setting for those agencies that will be part of the new Department. Nevertheless, DHS will not “own” all of the Federal assets, including resources designed for assistance to States and localities. A prime example will continue to be the Department of Health and Human Services.

We recommended in our *Second Report* that a White House office for combating terrorism be given certain budget oversight and controls. We continue to believe that such a function is required for setting resource priorities for Federal programs for combating terrorism, and one that is implemented before the Office of Management and Budget is required to make budget choices among a multitude of other competing priorities. That function can and should be accomplished by the White House Office of Homeland Security.

¹²⁶ *Third Report*, pp. 6-7.

We have also previously recommended “consolidating information and application procedures for Federal grant programs for terrorism preparedness in the Office of Homeland Security.” With the advent of DHS, it is conceivable that such a function could be performed by that Department, as it will own many such grant programs after full consolidation. In any event, those processes should be consolidated in one central location and with a standard set of forms for grant application, in order to reduce confusion among States and localities regarding the availability of grants and the processes for applying.

Determining “How Much Is Enough”

In our *Third Report*, we recommended “that the Congress increase the level of funding to States and local government for combating terrorism.” That is now—appropriately—starting to be accomplished. In our earlier reports and again here, we avoid placing a specific price tag on the costs in Federal funds for improving State and local capabilities. We continue to adhere to the view that the key it is not necessarily the total amount of funds but the necessity to ensure that such resources are applied most effectively. We do not, therefore, apply some arbitrary “scorecard” of how much or how little Federal funds have been provided to enhance State and local efforts from year to year, but rather how effective the application of those funds have been or are likely to be over time. We note again an example that we have discussed previously: the lack of resources for sustaining programs in the out years. Irrespective of the formula that may be applied for burden sharing by States and localities, most Federal programs, especially those for training and equipping State and local responders, must be designed with clear goals and implemented with long-term sustainment in mind.

Measuring Effectiveness

However resources are applied and at whatever level, more must be done to create and implement a system of metrics for judging how well resources are being applied over time. Program evaluations must be more than just an audit trail of dollars and must be part of an integrated metrics system. A program in an agency may impact or duplicate or even contradict the intent of a program in another. It will be incumbent on the White House Office of Homeland Security to ensure a Federal agency-wide approach to such measures.

As we have previously stated, we as a nation can never expect to be 100 percent prepared to deal with every possible terrorist attack scenario. But without a comprehensive approach to measuring how well we are doing with the resources being applied at any point in time, there will be very little prospect for answering the question, “How well prepared *are* we?”

CHAPTER V. ORGANIZING THE NATIONAL EFFORT

ASSESSING THE NATIONAL STRATEGY

The capstone recommendation in our *Second Report* was the need for a comprehensive, coherent, functional national strategy: “The President should develop and present to the Congress a national strategy for combating terrorism within one year of assuming office.” In that report, we described, in considerable detail, our proposed framework for that strategy.

In July of this year, the President approved for release the first *National Strategy for Homeland Security*.¹²⁷ To lay the groundwork for most of the recommendations in this chapter, we start with a commentary on that *National Strategy* from the panel’s perspective, for the most part tracking the subject headings of the chapters on “critical mission areas” in that document.

General Comments

We applaud the President and his staff for publishing this comprehensive vision to see as the framework for the entire national effort. It is a foundation document and an important first step. It should not—indeed it cannot—be seen as being all of the answers to the challenges that we face. It will require periodic updates: we suggest annually. It will require detailed implementation plans; some are already being developed.

It contains well-crafted “vision” statements of where we should be headed as a nation. It acknowledges—as we have said before that any comprehensive strategy must—that there are significant international implications for “domestic” efforts.

It recognizes that this strategic approach must be a truly *national*, not just a Federal approach:

*... based on the principles of shared responsibility and partnership with the Congress, state and local governments, the private sector, and the American people. The National Strategy for Homeland Security belongs and applies to the Nation as a whole, not just to the President’s proposed Department of Homeland Security or the federal government.*¹²⁸

It contains—importantly—definitions of both *homeland security* and *terrorism*.¹²⁹

Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.

The National Strategy for Homeland Security characterizes terrorism as any premeditated, unlawful act dangerous to human life or public welfare that is intended to intimidate or coerce civilian populations or governments.

¹²⁷ *National Strategy for Homeland Security*, available at <http://www.whitehouse.gov/homeland/book/index.html>, last accessed December 5, 2002, hereinafter the “*National Strategy*.”

¹²⁸ *National Strategy*, p. 2.

¹²⁹ *Id.*

It contains language about the importance of measures of performance but does not articulate what those measures should be. Importantly, in our view—being consistent with our expressions since our *First Report*—it eliminates the arbitrary, artificial, and confusing distinction between so-called “crisis management” and “consequence management” activities.

It recognizes the importance of creating a national incident management system with an “all-hazards” approach—one that combines preparedness and response for natural disasters, accidents, and intentionally perpetrated attacks.¹³⁰

Definitional Issues

Despite a commendable attempt to reduce confusion by articulating certain definitions, it does not fully accomplish the task. The *National Strategy* uses CBRN or CBRNE¹³¹ and Weapons of Mass Destruction or WMD seemingly interchangeably.

It uses different terms apparently to describe the same function or category: “health,” “public health,” “medical,” “medical care.” And it is unclear whether “emergency medical providers” does or does not include emergency medical technicians. It uses other terms interchangeably with not clear delineation or distinction: “anti-terrorism,” “counterterrorism,” and “combating terrorism.” And it is not clear whether “enemies” and “terrorists” are synonymous.

“Threat and Vulnerability”

This chapter of the *National Strategy* appropriately recognizes that the nature of our society—our “American way of life—makes us inherently vulnerable to terrorist attacks. It also acknowledges the imperatives not only of safeguarding our security and economy but also our culture, our civil liberties, democracy itself.

It appropriately, in our view, disaggregates chemical, biological, radiological, nuclear, conventional, and cyber attacks. But it suggests that chemical and biological weapons, generically, are “easy to manufacture,” using “basic equipment.” We have noted, in our threat assessments, including the one in this report, that such broad categorizations are unfortunate. Many of the more sophisticated chemical and biological weapons, especially those that could cause fatalities in the thousands or tens of thousands are very difficult to produce, maintain, and deliver.

It appropriately recognizes the potential damage that could result from an attack on U.S. agriculture.

“Organizing for a Secure Homeland”

This chapter of the *National Strategy* recognizes and explains the interconnected and interdependent roles of the Federal government, States and localities, the private sector, and the American people in a united national effort. It stresses the “vital need for cooperation between

¹³⁰ Ibid, p. 3.

¹³¹ Chemical, biological, radiological, nuclear, and conventional explosives.

the Federal government and State and local governments . . . horizontally (within each level of government) and vertically (among various levels of government).”

In a move that we strongly endorse, it announces the intention to retain the White House Office of Homeland Security, even after the formation of the new Department of Homeland Security, with authority “to certify that the budgets of . . . executive branch departments will enable them to carry out their homeland security responsibilities.”

It appropriately notes that the Department of Defense has important roles in homeland security, both for “homeland defense”—“military missions such as combat air patrols or maritime defense” in which the Department would “take the lead in defending the people and territory of our country—as well as “military support to civil authorities”—where the Department supports other agencies in responding to attacks, natural disasters, or “other catastrophies.”

It appropriately, we believe, calls on the Governors of the several States “to establish a single Homeland Security Task Force (HSTF) for the state, to serve as his or her primary coordinating body with the federal government,” but unfortunately does not offer to do the same in return. (We address this issue directly later in this report.)

“Intelligence and Warning”

This chapter correctly notes that appropriate assessments—both “tactical” and strategic”—of terrorist threats must precede any realistic assessment of our vulnerability. We are arguably infinitely vulnerable. Only when we can realistically determine what threats exist that would seek to exploit particular vulnerabilities will we be in position to take preventive and defensive steps and other appropriate responses.

Unfortunately, the *Strategy* does not suggest what products of the tactical or strategic (especially strategic) assessments will be produced or how and to whom such products will be disseminated.

We address, in considerable detail, the issues of intelligence collection, analysis, and dissemination and make specific policy recommendations with respect thereto, later in this chapter.

“Border and Transportation Security”

That chapter clearly and appropriately sets forth important initiatives for improving security at our borders and in our transportation systems. It notes the potential for using biometrics for improved identification, the criticality of deploying a border “entry-exit” system for foreign visitors, for increasing security with respect to commercial cargo entering the United States, for implementing “unified, national standards” for transportation security, for providing additional resources for the U.S. Coast Guard, and for improving visa processes.

On the latter issue, it suggests that the new Department of Homeland Security will “control the issuance of visas to foreigners” but provides no detail on how that will be accomplished.

“Domestic Counterterrorism”

Near the beginning of that chapter of the *National Strategy* is an explicit statement:

The U.S. government has not yet developed a satisfactory system to analyze information in order to predict and assess the threat of a terrorist attack within the United States.

We fully concur and offer a specific recommendation later in this chapter directed at helping to solve that problem.

While discussing several tactical and operational approaches to address the challenges in this arena, this chapter does not, in our view, address some of the more strategic issues, such as the important relationship between the Department of Justice and the Department of Homeland Security and the critical role that State and local law enforcement have in this area. It also does nothing to address the proliferation of interagency and intergovernmental mechanisms, which seem not to be part of any overall design. We address that issue below, as well.

“Protecting Critical Infrastructures and Key Assets”

We applaud the policy decision, articulated in this chapter, to “unify the responsibility for coordinating cyber and physical infrastructure protection efforts” into the new DHS, especially for providing a single point of contact on such issues for States, localities, and the private sector.

The chapter also notes the intention to create a national infrastructure protection plan—a laudable goal—as well as the recognition of the international interdependencies of many critical infrastructures, especially in the transportation and cyber realms.

We also note with approval the careful articulation of Lead Agency responsibilities for critical infrastructure protection. We believe that that model should be applied to other functional areas for combating terrorisms and cite specific instances of that in other parts of this report.

We discuss those and related issues in considerable detail in Chapter VIII, below.

“Defending Against Catastrophic Threats”

We concur in the initiatives in this chapter for specific improvements in sensors and other detection and health surveillance capabilities. Those initiatives are fully consistent with specific recommendations contained in earlier reports of this panel.

The chapter acknowledges the need for improvements in laboratory capabilities but does not articulate specific proposals to address that issue. We do so, along with other policy recommendations, in our health and medical chapter later in this report.

“Emergency Preparedness and Response”

We concur strongly in the views expressed in the chapter on the different, separate response plans. We agree (as we have consistently expressed) that such plans should be merged. That chapter calls that proposed plan the “Federal Incident Management Plan.” We suggest that the

better title would be *National Incident Response Plan*, which by its name would recognize the important role of States, localities, and the private sector. The accompanying proposal to establish a national incident management system certainly recognizes that, and the name of the plan should as well.

We wholeheartedly endorse the intention to develop a “national emergency communications plan” designed to establish “protocols, processes, and national standards for technology acquisition.” We have previously recommended such a process for all emergency response equipment and systems. It is especially critical in the area of communications.

We also applaud the emphasis in that chapter of the *National Strategy* of improving both coordination with and the capabilities of the public health sector. We have previously made recommendations in this area, and make additional ones below, in our chapter on health and medical issues.

On the issue of military support to civil authorities, the parameters of which are outlined in this chapter of the *Strategy*, we devote a considerable amount of our Chapter IX, below, with several specific policy recommendations.

IMPROVING THE STRATEGY AND STRUCTURE

Intelligence Collection, Analysis, and Dissemination

Dealing with the Terrorists Among Us

It is now clear from contemporaneous reports and recent arrests that potential terrorists, perhaps in large numbers, are inside the United States. Many of them may have received training in foreign camps. They may seek to carry out more attacks against U.S. citizens and property. This new aspect of the terrorist threat requires a new approach in two key areas:

- The need for a focused and comprehensive analysis of threats of potential attacks inside the United States; and
- The need to address the gaps in collecting intelligence on foreign terrorists threats inside this country

The U.S. government’s organization reflects an artificial distinction between “foreign” and “domestic” terrorist threats. The new threat environment, where those distinctions are increasingly blurred, requires a more robust and focused approach to all aspects of intelligence – collection, analysis and dissemination – whether it is collected at home or abroad. And this must be done in a way that respects American civil liberties.

The CIA, FBI, other members of the Intelligence Community, and the proposed Department of Homeland Security (DHS) will all have roles for intelligence-related functions. DHS will have responsibility only for vulnerability assessments for critical infrastructure protection, as well as for providing nationwide alerts. As things now stand, the FBI and CIA will each continue to have its own domain for terrorism intelligence with only marginal direct coordination between those entities, and no direct, formal relationship with the proposed DHS. Yet, such large, multi-mission agencies as the FBI and the CIA are incapable of changing direction quickly enough,

and should not be tasked further, to respond to current dangers. There is a risk of duplication, overlap, and bureaucratic “stovepiping” in this vital area. So a consolidation of certain activities is required.

Recommendation: That the President direct the establishment of a National Counter Terrorism Center (NCTC)

That entity should be a “stand-alone” organization outside of the FBI, CIA, or the DHS. The objective is to consolidate in one entity the analysis of foreign-collected and domestically-collected intelligence and information on international terrorists and terrorist organizations threatening attacks against the United States. This would be accomplished by permanently transferring (not “detailing”) analysts currently performing those functions within the CIA (i.e., the core analytic capability within the CIA’s Counter Terrorism Center), the FBI (the newly-expanded analytical section), other appropriate members of the Intelligence Community, representation from DHS (when formed), and supplementing with new hires as necessary.

The NCTC should be an Independent Agency of the Federal Executive Branch, similar to the standing of the Environmental Protection Agency, the Federal Emergency Management Agency, NASA, or the General Services Administration. The new entity should be a full member of the U.S. Intelligence Community. The agency head should be appointed by the President with the advice and consent of the U.S. Senate.

Advantages and Disadvantages of an Independent Agency

The members of the Advisory Panel discussed at length whether the NCTC should be placed within an existing department or agency or within the proposed Department of Homeland Security.

The panel discounted its placement in the Central Intelligence Agency for legal, policy, perception, and cultural reasons. The panel discussed and rejected the notion that this entity could be part of the FBI or an agency within the Department of Justice. Panel members felt that such placement would cause the entity to have too much law enforcement focus—building cases for prosecution—rather than detection and prevention.

The panel considered the prospect of placing the entity in the proposed Department of Homeland Security (DHS). While many panel members agree that such placement is a viable option, that alternative was eventually rejected for several reasons. First and most important, DHS will not be the only “customer” of the products of the NCTC. Other key Federal entities—notably the Department of Justice and its agencies, the Department of Health and Human Services, the Department of Defense, the Department of State, and the Department of Agriculture—will all require significant intelligence products from the NCTC. States, localities, and elements of the private sector will all be considerable consumers of NCTC products. Moreover, it would be viewed by other Federal agencies as being more responsive to DHS activities and priorities at the expense of other agencies’ requirements. As a DHS entity, the NCTC would have to compete for resources with other DHS functions.

The panel concluded that a stand-alone entity, with its own funding, would be more likely to set priorities for its activities more objectively—an “honest broker” for competing requirements—and would not be viewed as tied to any single agency’s mission.

The disadvantage to a stand-alone agency is that it may simply create more bureaucracy. That argument will be neither more nor less valid than the suggestion that DHS will create new bureaucracy. Moving existing resources and responsibilities from the FBI and from other entities in the Intelligence Community will minimize any real growth of government. The advantages gained in this structure outweigh any adverse impact, in the panel’s view.

The NCTC would be responsible for the fusion of intelligence—from all sources, foreign and domestic—on potential terrorist attacks inside the United States. It would be responsible for the production and dissemination of analytical products to all appropriate “customers,” including the Departments of Justice, Homeland Security, State, Health and Human Services, Agriculture, and Defense, and in coordination with those agencies, to designated and cleared officials in States, localities, and the private sector. It would have the authority to levy direct intelligence requirements on the Intelligence Community for the collection of intelligence on potential threats inside the United States. (See further discussion on collection below.)

The NCTC should be the entity that manages the “Collaborative Classified Enterprise” outlined in the *National Strategy for Homeland Security*, which links Federal, State, and local efforts in analyzing the activities of persons who have links to foreign states or to foreign terrorist organizations. The intelligence and information sharing functions currently being developed through the U.S. Attorney Antiterrorism Task Forces and slated to be moved to the proposed DHS should instead be imbedded in the NCTC.

The Critical Role of States, Localities, and the Private Sector

State and local entities, as well as key segments of the private sector, currently develop important intelligence and related information on potential terrorist threats to the homeland. No comprehensive system currently exists for consolidating all of that information into coherent threat analyses. To accomplish these functions and to establish other important coordination with States, localities, and the private sector, the NCTC staff should include significant representation from each of those segments. The panel envisions the NCTC hiring personnel with related experience at the State and local level and in the private sector, either on a permanent or rotational basis or a combination of the two. In addition, functions for developing guidance and for improving procedures should be informed by an advisory council consisting of senior officials from States (governors, State emergency managers, State police, State public health) localities (mayors, city managers, law enforcement, emergency managers, fire services, emergency medical technicians, and other local responders), and appropriate private sector entities (especially representatives from critical infrastructures). Moreover, formal operational relationships should be established with States and localities that have created structures and processes with similar missions that can be used as models for other areas of the country. Examples include the California Terrorism Information Center (CATIC), the Los Angeles Operational Area Terrorism Early Warning Group, and similar efforts in New York City.¹³²

It is clear that the Federal government is far from perfecting a system of sharing national security intelligence and other information, developed at the Federal level, with States, localities, and certain segments of the private sector. While important progress has been made, the flow of intelligence and information is still not completely a “two-way street.” The prevailing view continues to be that the “Feds” like to receive information but are too reluctant to share completely. Not all officials at every level of government need to be cleared for classified information. The Federal government must do a better job of designating “trusted agents” at the State and local level and in the private sector and move forward with clearing those trusted agents—at Federal expense. This should not be a case of the Federal government allowing those

¹³² For additional information on the partnership of CATIC with the New York Police Department's Counter Terrorism Division and the Defense Intelligence Agency to share information and intelligence about suspected terrorist activities, see <http://caag.state.ca.us/newsalerts/2002/02-107.htm>, and “State Joins U.S., N.Y. to Fight Terror,” by William Overend, Los Angeles (CA) Times, October 1, 2002.

agents access and then giving them the “privilege” of paying for it. This is a national requirement—not Federal on the one hand, and States, localities and the private sector on the other. Additional Federal resources are required, and soon, to make this process work.

Improving the Collection Function

Recommendation: That the collection of intelligence and other information on international terrorist activities inside the United States, including the authorities, responsibilities and safeguards under the Foreign Intelligence Surveillance Act (FISA), which are currently in the FBI, be transferred to the NCTC

This collection function would be functionally separate from, but physically co-located with, the analytical fusion component.

The panel makes this recommendation for two reasons. First, while the FBI remains the world’s preeminent law enforcement agency, there is a big difference between dealing with a terrorist act as a crime to be punished and dealing with it as an attack to be prevented. We commend the FBI leadership for its efforts to make these changes. But the Bureau’s long standing tradition and organizational culture persuade us that, even with the best of intentions, the FBI cannot soon be made over into an organization dedicated to detecting and preventing attacks rather than one dedicated to punishing them.

Second, even if the FBI could be remade, the panel believes it important to separate the intelligence collection function from the law enforcement function to avoid the impression that the U.S. is establishing a kind of “secret police.”

The collection component of the NCTC should be based on the concept of the Foreign Terrorist Tracking Task Force created by the Attorney General in fall of 2002—multiple agency representation and robust technological capabilities—but with authority to collect intelligence and information within the United States. It would be authorized to collect intelligence only on international terrorism threats. It could not lawfully collect any other intelligence. Counter terrorism intelligence collection outside the United States would continue to be accomplished by the CIA, NSA, and other foreign IC components.

The NCTC would have no “sanction” authority. It would not have arrest powers—that authority will continue to rest with the FBI, other Federal law enforcement agencies, and State and local law enforcement. The NCTC would have no authority to engage in deportations or other actions with respect to immigration issues, to seize the assets of foreign terrorists or their supporters, or to conduct any other punitive activities against persons suspected of being terrorists or supporters of terrorism. The NCTC will provide information that can be “actionable” to those agencies that do have the authority to take action. A challenge will arise on those occasions when the NCTC will need to pass intelligence “cueing” to law enforcement agencies for the purpose of constituting an arrest. But the challenge will be fundamentally no greater than it is today when existing U.S. intelligence agencies “cue” Federal law enforcements agencies for such purposes.

This new collection component of the NCTC would operate under significant judicial, policy, and administrative restraints. It will be subject to the requirements of the Foreign Intelligence

Surveillance Act (FISA)¹³³ and the Attorney General’s Guidelines for terrorism investigations. This component would be required to seek legal authority from the Foreign Intelligence Surveillance Court (FISC) for intrusive (surveillance or search) activities. Moreover, the NCTC would not require any expansion of the authority under FISA or the conditions and strictures that apply thereto, or additional authority beyond that contained in the USA PATRIOT Act. The FBI would continue to have responsibility for purely domestic terrorist organizations and for non-terrorism related organized crime. Title III wiretap responsibilities would remain with the FBI for criminal activities.

To ensure that the NCTC remained within these guidelines, a Policy and Program Steering Committee for the new agency should be established, consisting of the new agency’s director, the Director of Central Intelligence, the Attorney General, and the new Secretary of DHS (when appointed and confirmed). The functions of the Office of Intelligence and Policy Review currently in the Department of Justice (DOJ) would move to the new NCTC to staff this steering committee, to assist in ensuring that the entity adheres to all relevant constitutional, statutory, regulatory, and policy requirements, and to assist in coordinating the activities of the new entity with the FBI, and other law enforcement agencies.

In addition, there could be more focused and effective Congressional oversight of the domestic collection and analysis functions. Currently, the oversight of the FBI’s FISA and other domestic intelligence activities is split between the Judiciary and Intelligence committees in each House of Congress. Creation of the NCTC would clearly place the primary responsibility for oversight of that agency under the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. Such a structure and improved oversight would likely provide an even better mechanism for protecting civil liberties than do current structure and processes. For that reason, the panel makes the following, related

Recommendation: That the Congress ensure that oversight of the NCTC be concentrated in the intelligence committee in each House

How will the NCTC enhance civil liberties protections?

- It will have no “sanction” authorities—law enforcement, prosecution, deportation, asset seizures, etc.
- It will improve Congressional oversight
- It will create more effective oversight mechanisms within the Executive Branch
- It will have internal and external safeguards that will be focused on intelligence issues

The panel recognizes that the creation of this new entity, the NCTC, cannot happen overnight. Nonetheless, its creation should begin immediately. Some may argue that we should not attempt to make this change in the midst of the “war on terrorism.” But that war may continue for many years, and the danger now posed by terrorists underscores the need for moving ahead on an urgent basis. In the near term, the FBI will continue to have FISA and other domestic collection responsibilities. Deliberate and thoughtful planning will be required to ensure continuity and to

¹³³ 50 U.S. Code, Chapter 36 (50 USC Sections 1801-1863) (PL 105-511, October 25, 1978)

transfer effectively and as seamlessly as possible the capabilities and functions required for the NCTC. But, to underline the point, the NCTC should be established right away.¹³⁴

The panel also recognizes that other agencies may continue to require some limited analytical capability. The NCTC will be responsible for strategic level intelligence analysis and for creating intelligence products that will inform operational decisions. Individual agencies, such as the FBI and the new DHS when formed, may need some internal analytical capability to take NCTC product and convert it from the operational level into tactical, actionable intelligence. It will be necessary, however, to ensure that other agencies do not seek to duplicate the NCTC

¹³⁴ Panel Chairman Jim Gilmore filed the following statement, in which he was joined by Panel Member Ellen Gordon, concurring in the recommendation with reservations:

"The Commission has devoted much time to the discussion of a new agency to collect information on international terrorist activities inside the U.S. My approach has been to maintain these functions within the FBI, and to build upon their considerable structures, sources and resources to upgrade and improve this function. After great discussion and testimony, the Commission has decided to recommend the creation of a new agency. I will support this recommendation, but only with the oversight provisions and legal requirements contained and described in the report, to ensure no diminution of the civil liberties of the People of the United States."

Panel Member Jim Greenleaf filed the following dissent:

"I am in favor of the creation of the NCTC but only for the analytical 'fusion' function. I am opposed to the creation of an independent organization within the NCTC that would collect intelligence and other information on international terrorists activities inside the United States.

"I believe that the FBI is fully capable of collecting the needed information in an effective, efficient, and lawful manner. The Bureau is like most bureaucracies and change comes slowly. However, knowing the caliber and dedication of the men and woman in the organization, they can meet these new challenges and make the appropriate adjustments to counter the terrorist threat.

"It will take years for a new organization to be created and become an effective resource in the fight against terrorism. The FBI already has agents in the field with the proper contacts to collect much of the needed intelligence. More certainly needs to be done. I am concerned about creating an organization that places detection and prevention ahead of prosecution. The FBI culture as a law enforcement agency provides a backdrop and check and balance against any abuse of civil liberties.

"Terrorism is a crime and needs to be addressed in that fashion following the current AG Guidelines and the Constitution. An organization designed to detect and prevent will not by definition be as sensitive and cautious in carrying out their mandate to protect civil liberties. I fully understand the restrictions that will be placed on the new agency, but doubt they can do the job required of them by operating in a very murky area of law and governmental guidelines. The issue of "secret police" becomes more of a factor for the new organization rather than with the FBI. "Although the new organization would only collect intelligence on international terrorism threats, I find it difficult to visualize how they would carry out that mandate without involving domestic persons and organizations, since many cases involve both domestic subjects as well as international subjects. Many of the cases would evolve into complex relationships between domestic and international people and organizations, thus creating a difficult problem of jurisdiction and further concerns about 'stovepiping' between agencies.

"I am concerned about any agency that doesn't have to be held accountable for their actions by not having to defend their investigation by use of 'sanctions.' The ultimate arrest and prosecution of a subject acts as a logical process for the organization to demonstrate that they have operated within the law in conducting their business. Decisions made as to what course of action should be followed in order to 'detect and prevent' may very well result in a situation where the subject or subjects could not be prosecuted, thereby leaving the system with the question of what to do with them once the case becomes public knowledge. Certainly the prevention of a terrorist attack is of the highest priority, but what do we sacrifice in the process?

"I would prefer to see the FBI given additional resources especially in the area of computer support. They should place an increased emphasis on building a robust analytical capability to do a better job of recognizing and connecting the 'elusive dots' so they can provide valuable input to the NCTC. The AG Guidelines should also be revisited with the view of making them more 'user-friendly' and identify areas where lines can be drawn clearly and distinctly for aggressive investigative activity. Agents shouldn't have to worry about interpreting the rules. They need to know what is expected of them so they can go forward with an aggressive intelligence collecting process that is carried out in a way the American people would expect, and in a manner that the Constitution demands."

intelligence analytical fusion function, as has been the case in certain other historical contexts within the Intelligence Community. The President must ensure that the NCTC is the primary fusion center for all domestic intelligence. It must not be allowed to become a “coordinator of coordinators.”

The panel is aware of other recent proposals that appear to be designed to address the collection problem. One was made by “The Task Force on National Security in the Information Age” of the Markle Foundation.¹³⁵ That proposal would place certain information collection functions in the proposed DHS, but would leave domestic intelligence collection with the FBI. We believe that that proposal does not go far enough in resolving the problem.

We are also aware of proposals similar to ours that are being made by U.S. Senators John Edwards (NC) and Bob Graham (FL).¹³⁶ The major distinction is that those proposals, while creating a separate collection entity, would leave that entity in the Department of Justice. For reasons stated above, we believe that the new entity must stand alone and clearly separated from law enforcement. Apparently, the Executive Branch is also considering some alternative to address the problem, reportedly including the establishment of something like an American version of the British MI5.¹³⁷ The panel has, however, avoided any comparison between our proposal and MI5. Our Constitution, our laws, our history, and our culture require a United States solution.

Collection Function—Summary of Key Points

- Would not *create* a domestic intelligence function; that function is already being performed by the FBI
- Would transfer that function to an entity with a detection and prevention, not law enforcement, focus and culture
- Would execute FISA and other foreign terrorist legal authorities inside the United States
- Would only effect persons with connections to foreign terrorists or terrorist entities, not purely domestic organizations or persons
- Would have no responsibility for non-terrorism related criminal activity
- Would *not* have arrest powers or other “sanction” authority
- Would be subject to requirements and restrictions in FISA (including application to the Foreign Intelligence Surveillance Court) and in the AG Guidelines
- Would not require new or expanded authority
- Would *not* have Title III wiretap authority
- Would be monitored by a steering committee and staff verification function (OIPR)
- Would likely provide better civil liberties and liberties protection
- Would have direct and significant relationships with States, localities, and the private sector

¹³⁵ *Protecting America’s Freedom in the Information Age*, New York: Markle Foundation, October 2002.

¹³⁶ “Spies in the Ointment? Experts Debate Whether U.S. Should Launch Domestic Espionage Agency,” CQ Homeland Security bulletin, *Congressional Quarterly*, Oct. 14, 2002.

¹³⁷ “U.S. may set up MI5-style spy agency in security shake-up.” *The Telegraph* (U.K.), October 31, 2002.

The Importance of Threat and Vulnerability Assessments

The *National Strategy for Homeland Security* appropriately notes the requirement for both strategic and tactical analysis and vulnerability assessments and designates various lead or co-lead agencies for those functions. The proposed DHS is only responsible for disseminating “real time actionable” information to others. It apparently has sole responsibility only for vulnerability assessments for critical infrastructure protection. There is no indication that strategic assessments of threats inside the U.S. will receive dissemination to State and local agencies.

Recommendation: That the President direct that the NCTC produce continuing, comprehensive “strategic” assessments of threats inside the United States, to be provided to policymakers at all levels, to help ensure appropriate planning and allocation of preparedness and response resources

The Role of the Department of Homeland Security in Intelligence Functions

It appears that the new DHS will have no authority for intelligence collection, limited capability for intelligence analysis, and significant responsibility for threat warnings.

Recommendations: That the Congress and the President ensure that the DHS has the authority to levy direct intelligence requirements on the Intelligence Community for the collection or additional analysis of intelligence of potential threats inside the United States to aid in the execution of its specific responsibilities in the area of critical infrastructure protection vulnerability assessments

That the Congress and the President ensure that the DHS has robust capability for combining threat information generated by the Intelligence Community and the NCTC with vulnerability information the Department generates in cooperation with the private sector to provide comprehensive and continuing assessments on potential risks to U.S. critical infrastructure

These capabilities will be important not only for the DHS specified missions but also for the DHS role in the NCTC.

Managing Operations

The *National Strategy for Homeland Security* has eliminated the distinction between “crisis” and “consequence” management. This will help remove certain ambiguities in the responsibilities and authority for planning and response. The creation of an overarching National Incident Response Plan to replace the Federal Response Plan and numerous other Federal plans can also clarify responsibilities. With the merger of the U.S. Customs Service (USCS), the U.S. Coast Guard (USCG), and the Immigration and Naturalization Service (INS)(and others) into the new DHS, that agency will have control over some but not all Federal law enforcement capability. The *National Strategy* provides that the Secretary of DHS will have the responsibility for “coordination and integration” of Federal, State, local, and private” activities for critical infrastructure protection (CIP). But it does not provide any vision about the extent to which DHS will be “in charge” of executing a response during or after an attack on some CIP sector;

nor does it specify which Federal agency is in charge for the Federal sector for other types of attacks, especially a biological one.

Recommendations: That the President and the Congress clearly define the responsibilities of DHS and other Federal entities before, during, and after an attack has occurred, especially any authority for directing the activities of other Federal agencies.

That situation is especially problematic when it comes to a bioterrorism attack. No one in the Federal structure can currently identify who is or, after DHS is formed, will be in charge in the event of a biological attack.

Recommendation: That the President specifically designate the DHS as the Lead Federal Agency for response to a bioterrorism attack, and specify its responsibilities and authority before, during, and after an attack; and designate the DHHS as the Principal Supporting Agency to DHS to provide technical support and provide the interface with State and local public health entities and related private sector organizations

Interagency Coordination

There are numerous Federal interagency coordination structures and several combined Federal/State/local structures. As examples of the later, the Joint Terrorism Tasks Forces (JTTF) (FBI) will remain with the FBI and a new National JTTF (FBI) will be formed. But JTTFs are organized differently in various jurisdictions. And according to the *National Strategy*, the responsibilities (for intelligence/information sharing with State and local law enforcement) of the U.S. Attorney Antiterrorism Task Forces (ATTFs) will shift to the DHS. The proliferation of such mechanisms will likely cause unnecessary duplication of effort. More important, the *National Strategy* calls on the Governors of the several States “to establish a single Homeland Security Task Force. . .to serve as [the] primary coordinating body with the Federal government.” But there is no similar call for a single mechanism at the Federal end.

Recommendation: That the Assistant to the President for Homeland Security review and recommend to the President, and that the President direct, a restructuring of interagency mechanisms to ensure better coordination within the Federal government, and with States, localities, and the private sector, to avoid confusion and to reduce unnecessary expenditure of limited resources at all levels

Legal Authorities

With the formation of the new DHS and other initiatives envisioned in the *National Strategy*, various statutory, regulatory, and other authorities (e.g., PDDs 37, 62, and 63) will be directly implicated. The *Strategy* appropriately calls for a review of legal authority for use of the military domestically. But other legal and regulatory issues must be addressed, not the least of which are quarantine, isolation, mandatory vaccinations, and other prescriptive measures that may be called for in the event of a biological attack.

Recommendation: That the President direct the Attorney General to conduct a thorough review of applicable laws and regulations and recommend legislative changes before the opening of the next Congress.

The Congress

The Congress is still not well organized to address issues involving homeland security in a cohesive way. The House recently took the bold, necessary, but unfortunately only temporary step of creating a special committee just to consider the proposal to create the Department of Homeland Security. Structures of that nature are required on a longer-term basis. Jurisdiction for various aspects of this issue continues to be scattered over dozens of committees and subcommittees. We therefore restate our prior recommendation with a modification.

Recommendation: That each House of the Congress establish a separate authorizing committee and related appropriation subcommittee with jurisdiction over Federal programs and authority for Combating Terrorism/Homeland Security

CHAPTER VI. IMPROVING HEALTH AND MEDICAL CAPABILITIES

Progress continues to be made with respect to health and medical care in response to terrorism in the United States. The infusion of nearly \$1 billion dollars from the Department of Health and Human Services (DHHS) over the past year has done much to focus States and localities on developing a plan and building capabilities to respond to bioterrorism. There was a broad consensus among interviewed State and local public health and medical officials¹³⁸ that DHHS should receive high marks for distributing both the public health and hospital preparedness cooperative agreement funds efficiently and equitably. A number of interviewees commented that they had never seen the Federal government respond to any problem with such rapidity. This distribution of funds should serve as a shining example of how the Federal government can assist State and local governments and entities in terrorism preparedness. However, because the Constitution vests the power to act to preserve the public's health in the States as an application of their police powers,¹³⁹ the nation's health and medical preparedness cannot rely heavily on the Federal government. In addition, a review of DHHS¹⁴⁰ has shown that its anti-terrorism focus is primarily but not exclusively bioterrorism. While DHHS will clearly lead the technical and operational efforts to prevent, detect, and respond to bioterrorism, other types of terrorist attacks, such as those using chemical, radiological, conventional explosive, or nuclear devices, have significant public health and medical dimensions, and the preparedness for these should not be de-linked from that of bioterrorism.

The initial focus on bioterrorism was appropriate because biological terrorism had been virtually ignored prior to 1995. However, as the system has been strengthened to deal with bioterrorism DHHS goals should be broadened, and DHHS should have a comprehensive approach to terrorism response and prepare across the entire range of potential terrorism events. While interviewees stated that the bioterrorism preparedness grants will likely be applied to the full array of public health threats and, moreover, that other agencies and funding sources—including FEMA, local “first responders,” and others—have addressed chemical, radiological, and explosive threats to a greater extent than bioterrorist ones, the Advisory Panel reiterates that response to all of these events should be integrated.

Supporting the view of the panel, an influential emergency preparedness policymaker argued that the bioterrorism preparedness program was misguided in that it further encouraged a “stovepiping” mentality among officials at all levels of government, which, in turn, inhibited them from “ratcheting up the dialogue to talk about the entire threat matrix.” This individual went on to state that DHHS has done a poor job in integrating both its programmatic efforts and

¹³⁸ RAND interviewed seven federal health officials, five State and three local public health and emergency preparedness officials, five staff members of organizations representing State and local public health officials, two academics/health policy researchers, and one physician who directs several hospital emergency rooms in a major metropolitan area between June and October 2002 using a semi-structured interview protocol. The State and local health officials were drawn from agencies located in five States, and the emergency room physician worked in a sixth State.

¹³⁹ Gostin, L.O., J.W. Sapsin, S.P. Teret, S. Burris, J.S. Mair, J.G. Hodge, Jr., and J.S. Vernick, “The Model State Emergency Health Powers Act: Planning for and Response to Bioterrorism and Naturally Occurring Infectious Diseases,” *JAMA*, 288(5), pp. 622-628.

¹⁴⁰ Reviews performed by RAND researchers and in Appendix J.

the public health perspective, in general, into the overall emergency response structure. Evidence to support this assertion was provided by a number of interviewees who maintained that DHHS has done a very poor job in coordinating activities with FEMA, in particular, as well as other Federal agencies, including the Departments of Justice, Agriculture, and State.

It is now essential that DHS, DHHS, OHS, and all other affected Federal agencies improve the planning, coordination, and implementation processes for all public health and medical efforts for combating terrorism.

Applying Resources Effectively

The President's FY03 budget request for bioterrorism is \$5.9 billion with \$4.3 billion allocated to DHHS. The President has allocated \$1.2 billion to upgrade State and local capacity including: \$591 million for hospital preparedness; \$210 million for states to evaluate and improve their capacity to respond to bioterrorism; and \$200 million to increase laboratory capacity at the State level. The President has also requested \$300 million for management of the National Pharmaceutical Stockpile (NPS). These funds will also allow the United States to increase the supply of chemical antidotes and plan and train with the States for utilization of the stockpile. An additional \$100 million is devoted solely to distribution and use of the smallpox vaccine. The President's budget recommends \$392 million to improve our detection of and communication about bioterrorism-related outbreaks through improved communications. Of this amount, \$175 million is designated for the acquisition of hardware and the provision of technical assistance to State and local public health providers.¹⁴¹

As noted above, funding has begun to flow to States and localities through DHHS bioterrorism preparedness grants, much of it directed toward public health. After years of cutbacks, State public health agencies' efforts to confront the terrorist threat are "beginning from a standing start."¹⁴² Officials in public health have indicated that it will take at least a five-year commitment from DHHS, at approximately \$1 billion per year to have a material impact on States and local government preparedness to respond to bioterrorist events. Interestingly, public health officials also believe that \$1 billion is the "right" annual level, arguing that while the need to develop the public health infrastructure to better prepare for and respond to terrorist act was acute, it would be difficult to absorb the funds if the funding rate were increased appreciably. This stems in part from the difficulty of finding qualified people to fill newly-created positions, evaluating and purchasing new communications and information systems, and so on.

As one state public health survey respondent noted: "Our State, like many others, is just establishing an infrastructure to administer the Federal resources available for bioterrorism preparedness and response."

Another state public health survey respondent also commented, "We have a great plan to move forward and prepare the entire state health care system—we just need the staff to carry out."

¹⁴¹ Office of Management and Budget, "Budget for FY03," The Office of the President, Washington, DC, <http://www.whitehouse.gov/omb/budget/FY03/bud05.html>, last accessed December 10, 2002.

¹⁴² Inglesby, 2002

Multi-year funding, in addition to providing the required resources and allowing sufficient time for the States and locales to hire staff and to acquire new equipment, is critical in allowing States and local governments to attract and retain first-rate individuals and to invest an appropriate amount of money in new technologies. Many reported that long-term funding uncertainties presented a formidable barrier in their attempts increase their levels of preparedness. This problem is further exacerbated by the presence of severe State budget constraints, which increase the difficulties associated with making long-term plans.

As one state public health survey respondent commented, “With the introduction of increased federal funding, we saw a REDUCTION of State funding.”

Several respondents noted that DHHS even failed to prioritize the various components of the cooperative agreements, leaving State and local official in a quandary over where they should devote their resources. Additionally, DHHS has not effectively defined roles for Federal, State, and local public health officials. Moreover, with the exception of the hospital preparedness cooperative agreements that require States to work with hospitals, DHHS has offered States virtually no guidance on how, and with whom, to establish private sector partnerships.

As one local public health department survey respondent noted, “From a Health Department’s local perspective, the critical issues are 1) private cooperation and 2) “dual use” of new resources. At the Federal level, guidance regarding public/private health response tends to be inadequate, overly prescriptive, or otherwise unhelpful.”

As an example of the difficulty facing States in recruiting qualified personnel, some State health department representatives reported major difficulties finding and hiring qualified epidemiologists, although little is known about the actual number of epidemiologists needed within the public health system, because no empirical studies have explored this to date. In one State, recruitment for epidemiologist positions has been “spotty”; the department often does not draw any “stellar” applicants. Individuals who apply for the positions are generally not trained epidemiologists, but have instead been veterinarians, statisticians, and individuals with doctorates in related areas. During a discussion of bioterrorism and public health at the American College of Epidemiology meeting in September 2002, panelists and other meeting participants used the fall 2001 experience to illustrate the interface between epidemiology and bioterrorism, and participants reiterated the great need for epidemiologists to fill positions in State and local health departments created by recent Federal funding programs.

Recommendation: That DHHS continue to provide financial support on the order of \$1 billion per year over the next five years to strengthen the public health system in the United States

Attention should thereafter be paid to sustaining these resources beyond this time to maintain the system at a well-functioning level.

Recommendation: That DHS coordinate and centralize the access to information regarding funding from various agencies such as DHHS (including CDC), EPA, USDA, and others and simplify the application process

This centralization and simplification of grants processes is essential to eliminate confusion and unnecessary redundancies. (See our related, broader recommendation on this issue in Chapter IV, Resourcing the National Effort.)

Establishing and Using Metrics

In addition to providing significant resources for strengthening the public health sector, the Federal government should place renewed emphasis on multiyear funds to State, local, and private sector medical facilities to improve preparedness across the spectrum of response capabilities. All of these efforts must be evaluated with defined metrics to ensure the money is actually enhancing preparedness and that the resources are appropriate to the mission.

While many resources are being used to enhance capabilities to respond to terrorism, there is currently no framework in place for monitoring the States' progress in meeting the objectives of the cooperative agreements program and for evaluating States' performance with respect to various outcomes, although Federal officials have indicated that they are working to develop evaluation protocols. Moreover, there is a general lack of understanding on the part of representatives from State and local governments on precisely what they will be held accountable for and how their programs will be evaluated. Many of the respondents voiced a high level of frustration with the lack of evaluation plans from DHHS. One observer noted that DHHS needs to develop a common taxonomy for measuring program, as opposed to fiscal, accountability. Others expressed concern over the need for DHHS to articulate appropriate programs outcomes, how one would go about measuring progress towards reaching them, and a time line for achieving particular milestones.

Recommendation: That DHHS, in consultation with State, local, and private sector stakeholders, establish and implement a formal process for evaluating the effectiveness of investment in State, local, and private preparedness for responses to terrorist attacks, especially bioterrorism

In the absence of Federal criteria, some national organizations are developing competencies by which health departments can gauge their level of preparedness, beyond workforce preparedness. For example, the National Association of City and County Health Officials (NACCHO) is working with public health partners "to develop a module of performance measures, as part of the National Public Health Performance Standards Program, that will assist communities in assessing their capacity to respond to bioterrorist disease threats."¹⁴³ The goals of this project are to identify possible capacities, prioritize these capacities, and gather the input of stakeholders with the aim of reaching consensus. This is the first attempt at developing a potential credentialing process for public health departments, and the group hoped to implement field tests in late fall or early winter 2002.

Additionally, there are not yet widely agreed metrics by which to assess levels of preparedness among the workforce, although there are some aimed at particular sectors. There is not even a single definition of a "prepared workforce" because there is no consensus on what being prepared is. According to the U.S. General Accounting Office (GAO), as of 2002, "There is no

¹⁴³ National Association of City and County Health Officials. 2002. National Public Health Performance Standards Program. Available at <http://www.naccho.org/project48.cfm> accessed November 14, 2002.

consensus on the optimal number and ratio of health professionals needed to meet the population's health care needs,"¹⁴⁴ Those who RAND interviewed¹⁴⁵ for the study seemed inclined to use the "critical capacities" outlined in CDC's bioterrorism funding guidance to States as benchmarks for their success in preparing the workforce for bioterrorism specifically following receipt of funding.

While it is important to evaluate programs, it is particularly challenging given the low likelihood of a bioterrorism event. There have fortunately been few incidents to test workforce preparedness in real life situations. Nevertheless, some measure of requirements identification and an evaluation of the preparedness to meet those requirements must be accomplished before incidents occur.

Recommendation: That DHHS fund studies aimed at modeling the size and scope of the healthcare and public health workforce needed to respond to a range of public health emergencies and day-to-day public health issues

This type of modeling will help to develop a goal or baseline of preparedness so that during evaluations actual readiness can be compared to the preparedness goal. Without the kind of data that will result from such studies, it is impossible to quantify the gap between the current workforce and a workforce "prepared" to address these issues.

Improving Hospitals and Other Medical Facilities

DHHS bioterrorism preparedness grants have begun to address public health shortfalls; hospitals and other medical facilities are less prepared. A nationwide survey of hospital emergency departments conducted by RAND on behalf of the Gilmore Commission just prior to September 11, 2001, found that only 32 percent of hospitals indicated they had plans or standard operating procedures (SOPs) that address a moderate-sized biological incident, whereas 54 percent reported having a plan or SOP in place for a moderate-sized chemical incident.¹⁴⁶ Similarly, a 1998 survey of hospital emergency departments in four northwestern States found that fewer than 20 percent had plans in place for addressing chemical or biological events, less than half had integral decontamination units, and most did not have adequate respiratory protective equipment for the emergency departments' staff.¹⁴⁷ A second, follow-up survey conducted by RAND just prior to the anniversary of September 11 found that while 30 percent of hospitals have increased or shifted staff since the attacks to focus on bioterrorism and other Weapons of

¹⁴⁴ U.S. General Accounting Office. 2001. Health workforce: ensuring adequate supply and distribution remains challenging. Report No. GAO 01-1042T. Available at <http://www.gao.gov/> accessed September 15, 2002.

¹⁴⁵ Fourteen individuals involved in enhancing workforce preparedness at various levels (State health department, trade association, Federal government) were interviewed to learn about their activities, concerns, and unmet needs around response to the potential threat of terrorism, bioterrorism, and other public health emergencies. We developed two formal interview scripts—one for State health officials and another association or academic institution representatives. Our interviews with Federal officials were organized around questions related to specific Federal initiatives. Each interview lasted approximately one hour. Four were conducted in person, and the rest via telephone.

¹⁴⁶ Davis, L.M. and J.C. Blanchard, *Are Local Health Responders Ready for Biological and Chemical Terrorism?* IP-221-OSD, RAND, 2002.

¹⁴⁷ Wetter, D.C., W.E. Daniell, and C.D. Treser, "Hospital Preparedness for Victims of Chemical or Biological Terrorism," *American Journal of Public Health*, Vol. 91, pp. 710-716, 2001.

Mass Destruction (WMD) preparedness issues, only 33 percent of relevant hospital personnel¹⁴⁸ have been trained to date on WMD awareness of response (see Appendix D—Survey Information and Analysis). This represents a significant increase from the 5 percent of relevant hospital personnel trained in WMD awareness and response prior to September 11, 2001.

Findings from the second RAND survey also supported the idea that public health and not the medical response has been the focus of Federal resources for bioterrorism preparedness to date. Only 20 percent of hospitals indicated that since September 11, 2001, they have received an increase in funding or other resources to address WMD preparedness in FY02, in contrast to the more than 70 percent of local public health departments that received an increase in funding or other types of resources. In FY03, just over 30 percent of hospitals expect to receive additional funding, while more than half of local public health departments expected an increase in the new fiscal year (See Appendix D).

“If additional funding is not provided to hospitals, the cost of WMD preparedness will be difficult if not impossible to meet.” A local hospital responder, second survey

“We are a rural medical facility. Financial survival is difficult in the current climate. Funding is not available for training...” A local hospital responder, second survey

In contrast to the public health cooperative agreements, the hospital preparedness cooperative agreements were viewed as being inadequately funded (i.e., \$125 million for FY 2002), with many, if not most, of the respondents arguing that DHHS, and HRSA in particular, has unrealistic expectations for their program, as articulated in the guidance documents, given what was viewed as a relatively meager level of support.

Because relatively little money—on average, approximately \$25,000 per year—will be available for individual hospitals, several respondents noted that there may be a tendency to “go for the low-hanging fruit,” in the words of one, and purchase communications or decontamination equipment in instances where the money could better be used, say, to increase surge capacity, to upgrade and expand information technology systems, and to improve coordination among local hospitals and health care providers. In fairness, Federal officials have recognized the inadequacy of the funding level. As a result, they have requested \$500 million for FY03. Still, some experts believe that even this level of funding would not be sufficient to prepare the nation’s 5,000 hospitals to handle mass casualty events, mainly because hospitals, like public health agencies, have responded to fiscal pressures by cutting back on staff and other resources and otherwise reducing “excess capacity.”¹⁴⁹ The American Hospital Association estimated that it would take approximately \$11 billion to ensure the preparedness of the nearly 5,000 hospitals throughout the nation.¹⁵⁰ In Colorado, initial DHHS funding amounted to \$24,000 per hospital, FY03 funding

¹⁴⁸ Survey respondents were asked to indicate what percent of their hospital personnel who deal with acute response, environmental health, or coordination of emergency medical response had been trained in WMD awareness or response (particularly for incidents involving biological weapons).

¹⁴⁹ O’Toole, T. “Department of Health and Human Services Budget Priorities for FY03,” testimony before the U.S. House of Representatives Budget Committee, February 28, 2002.

¹⁵⁰ In testimony to the Committee on Government Efficiency, Financial Management, and Intergovernmental Relations, Larry Wall, President of the Colorado Health and Hospital Association, member of the Governor’s Expert Epidemic Emergency Response Committee, and Chairman of the Hospital Preparedness Advisory Committee, on August 18, 2002, the hospitals must address preparedness issues in at least eight areas: communication and

will provide an addition \$46,000, but necessary improvements in communications alone would cost approximately \$37,500 for a non-metropolitan hospital and \$75,000 for a metropolitan hospital.¹⁵¹

Recommendation: That DHHS conduct a comprehensive assessment of the resources required by the nation’s hospital system to respond to terrorism, and recommend appropriate Federal-State-Local-Private funding strategies

As part of that process, DHHS should, of course, consider recommendations of national organization like the American Hospital Association, but its assessment should be objective and independent.

Enhancing Communications

DHHS funds several programs aimed at improving the level of electronic connectivity among public health organizations. Examples of these programs include the Laboratory Response Network (LRN), which connects more than 80 public health laboratories in order to quickly identify pathogens used in bioterrorist attacks; the Health Alert Network (HAN), an Internet-based communications system to facilitate information sharing and distance-learning that links public health departments covering more than 90 percent of the nation’s counties; the National Electronic Data Surveillance System (NEDSS), a Federal initiative aimed at promoting the adoption of data and information system standards in disease surveillance systems used at the Federal, State, and local levels; and the Epidemic Information Exchange (Epi-X), a secure, Internet-based system that enables State health departments to communicate with CDC. These information systems are focused on connecting public health entities but lack connectivity with medical, emergency services, and public safety officials. Interviewees pointed out that the CDC needs to assist in coordinating and connecting some of its own laboratory and disease surveillance information systems initiatives (e.g., NEDSS, LRN, HAN, Epi-X).

Recommendation: That DHHS continue to strengthen the Health Alert Network and other secure and rapid communications systems, as well as public health information systems that generate surveillance, epidemiologic and laboratory information

These information systems should be connected to provide circular information flow. A complete circle of communications is required, not a one-way or even two-way flow of information. This need was recognized in part in three of the 14 critical benchmarks in DHHS’ bioterrorism preparedness grants:

notification; disease surveillance, disease reporting and laboratory identification; personal protective equipment; facility enhancements; dedicated decontamination facilities; medical/surgical and pharmaceutical supplies; training and drills; and mental health resources. Available at http://reform.house.gov/gefmir/hearings/2002hearings/0823_denver/wall_testimony.doc accessed December 2, 2002.

¹⁵¹ Wall testimony.

“10. Develop a plan to improve working relationships and communication between Level A (clinical) laboratories and Level B/C laboratories, (i.e., Laboratory Response Network laboratories) as well as other public health officials.

11. Prepare a timeline for a plan that ensures that 90 percent of the population is covered by the Health Alert Network (HAN).

12. Prepare a timeline for the development of a communications system that provides a 24/7 flow of critical health information among hospital emergency departments, State and local health officials, and law enforcement officials.”¹⁵²

The development of an all-inclusive communications system would enhance the ability of officials to recognize, communicate, and respond to natural disease outbreaks as well as terrorist threats.

Improving Exercises

In our previous reports, we recognized that exercises are critical to ensure adequate training, to measure readiness, and to improve coordination among all responding entities. While various funding streams may encourage fragmentation of resources, exercises can be used to bring the pieces together as a functional whole. Common elements in exercises taking place in different parts of the system will be important for comparing performance among entities to ensure “system wide” capacity and serve as opportunities for testing how well the roles of these entities fit together in the overall coordinated response.

The second RAND survey, indeed, has found that since September 11, 2001, a majority of local health organizations (65 percent of local public health departments and 80 percent of hospitals) have participated in different types of field or tabletop exercises, particularly for chemical or biological incidents and for natural disasters. In addition, nearly all State public health departments since September 11, 2001, have participated in such exercises, particularly related to bioterrorism or chemical incidents (See Appendix D).

However, resources directed to State and local entities to conduct these exercises have been limited and incentives for cross discipline coordination require strengthening. We restate a previous recommendation with a follow on:

Recommendation: That the Congress increase Federal resources for appropriately designed exercises to be implemented by State, local, private sector medical and public health and emergency medical response entities

A variety of issues should be integrated into exercises. For example, the American Nurses Association (ANA) is concerned about personal protective issues as important considerations in their ability to respond to bioterrorism attacks. Nurses have voiced concerns about not being able to reach their children in the event of a hospital lockdown. The American Hospital Association has been involved in leading joint role-playing activities and developing guidelines around the workforce issues that need to be addressed to enhance the ability to respond to events.

¹⁵² U.S. Department of Health and Human Services, HHS Fact Sheet, June 6, 2002

For example, they have recommended getting various community organizations involved in planning and thinking about who could check on healthcare providers' children in the event of an attack.

Perfecting Specialized Response Teams

The National Disaster Medical System and the Metropolitan Medical Response System attempt to provide surge and specialized health related assets to victims of natural and manmade disasters. On November 1, 2002, DHHS announced \$2 million in grants to 42 communities to create local Medical Reserve Corps (MRCs), which are designed to help communities prepare for and respond to public health emergencies.¹⁵³ The MRC program is administered by the Office of the Surgeon General, although all MRCs will be developed, managed, and sustained at the local level. Additionally, the ANA is working with DHHS to develop National Nurses Response Teams (NNRT), which will consist of 200 nurses per region (2,000 nurses in total) who will receive standardized education aimed at preparing them to assist with mass vaccination and chemoprophylaxis efforts. Finally, the American Pharmaceutical Association is working with DHHS's Office of Emergency Preparedness and several colleges of pharmacy to develop National Pharmacy Emergency Response Teams (NPRT). The goal of the program is to sign up and credential 2,000 pharmacists who can be mobilized to help respond to public health emergencies. However, it is not clear that enough professionals or equipment are available to staff and equip these teams, or how the teams will work together in the event of an emergency. An urgent need exists to clarify the role and functions of these various teams and the extent to which their roles will be coordinated at the Federal, State, and local levels.

Recommendation: That DHHS clearly articulate the roles, missions, capabilities and limitations of special response teams; that a plan be developed for the effective integration of such teams; and that focused training for special teams emphasize integration as well as coordination with States and localities

Promoting Technical Assistance

While public health and medical experts interviewed by RAND generally believed that they were provided a sufficient level of resources to begin establishing a reasonable capacity for responding to a bioterrorist attack, many felt that they lacked the expertise for, among other things selecting among competing technologies, developing templates for communicating risks and information on actual events to the public, developing plans for surge capacity and pharmaceutical distribution, and providing adequate training to staff.

All of this has been exacerbated by the aggressive vendors who have been inundating State and local officials with promotional materials and requests for meetings. Along these lines, a number of interviewees suggested that Federal officials should make a greater effort to establish standards for communications systems, information technologies, and even laboratory protocols.

Recommendation: That DHHS evaluate current processes for providing required technical assistance to States and localities, and implement changes to make the system more responsive

¹⁵³ HHS Release—"Medical Reserve Corps Units," November 1, 2002, HHS Press Office.

Increasing Surge Capacity

The medical system lacks the surge capacity that might be needed in the event of a terrorist attack. Because of the financial realities of medical insurance and managed care, hospitals operate on tight budgets. Facilities have eliminated beds and pharmaceuticals and face substantial workforce shortages.¹⁵⁴ DHHS has not asked States to develop workforce surge capacity, *per se*, but is requiring each State to be able to staff 500 critical beds per region in 2002 and 1,500 by 2003. DHHS has not provided models, algorithms, or other guidance as to how and where to locate the beds and how to staff them: State and local governments need to figure out how best to achieve this. The exception is the guidance that DHHS recently provided to States regarding setting up and staffing smallpox mass vaccination clinics. The Smallpox Vaccination Clinic Guide, released in September 2002, provides specific guidance regarding the number and type of clinical staff needed given specific assumptions about the number of individuals who would seek vaccination following a known smallpox attack.¹⁵⁵

Some State public health officials are unclear about their role in assisting with planning for the staffing of hospital beds in the State and otherwise becoming involved in surge capacity issues, although they do work closely with some hospitals. One stressed that assessing and staffing needs, gaps, and issues in a large State are overwhelming at the State level and really needs to be addressed at the local/regional level. However, one State health department is playing a role by hiring an emergency room planner and pharmacist who will have primary responsibility for planning with hospitals around potential use of the National Pharmaceutical Stockpile (NPS).

Recommendation: That DHHS develop an electronic, continuously updated handbook on best practices in order to help States and localities more effectively manage surge capacity, the distribution of the NPS, and other preparedness goals¹⁵⁶

In addition to hiring new staff, States are implementing a wide range of preparedness activities but have had little opportunity to share this information with colleagues in other States. Most involve training activities to enhance health department employees' basic public health and emergency preparedness skills. For example, the second RAND survey found that nearly three-quarters of hospitals and more than 80 percent of local public health departments indicated that since September 11, 2001, they had trained personnel on emergency response and preparedness for bioterrorism and/or for WMD, in general (See Appendix D). In addition, the case study interviews found that one department is providing training to epidemiology staff at the local level and is strongly emphasizing infrastructure development. For example, State lab capacity is being fostered through funding of laboratory enhancement activities at the regional level. Another State started an intensive, five-day field epidemiology course, to which members of their new regional response teams were invited. The course covered surveillance, statistics, infectious disease, and enhancing communication skills and had a key goal of getting the new hires to "think the same way." Several interviewees noted unique aspects of their States' plans from

¹⁵⁴ Tucker, Jonathan, "What the Anthrax Attacks Should Teach Us," *Hoover Digest*, 2002, No. 1, available at <http://www-hoover.stanford.edu/publications/digest/021/tucker.html> accessed on November 6, 2002.

¹⁵⁵ *Smallpox vaccination clinic guide: logistical considerations and guidance for State and local planning for emergency, large-scale, voluntary administration of smallpox vaccine in response to a smallpox outbreak*, DHHS, September 16, 2002.

¹⁵⁶ This could be modeled after the DHHS database on best practices in retaining the long-term care workforce available at <http://www.directcareclearinghouse.org/practices/index.jsp>

which other States might draw ideas if they were aware of them. One State, home to a very large metropolitan area and well as very impoverished areas, is acutely aware of the need to develop preparedness capacities across the entire State, which is a major challenge. A lot of pressure comes from large communities to make preparedness efforts population-based, but the interviewee noted that attention must also be paid to the rural areas of the State—which are also potential sites of manmade and natural public health emergencies. Another noted that the level of collaboration with the veterinary community in their State is fairly unique. DHHS should leverage these State and local initiatives to develop the best practices.

Federal, State, and local agencies, as well as many private sector entities, have not articulated, and therefore do not share, a common understanding of the meaning of a “prepared workforce.” DHHS and other agencies should fund research and information sharing aimed at better understanding what a workforce “prepared” to address a range of health threats would look like in size, competencies, composition, and geographic distribution to allow implementation of best practices.

Providing One-Stop Shopping

Several respondents noted that there is still considerable uncertainty regarding the roles of the CDC and the Office of Public Health Emergency Preparedness (OPHEP) in coordinating DHHS bioterrorism preparedness activities. This uncertainty has led to a number of problems on the part of State and local public health officials, and this may be exacerbated as OPHEP moves from DHHS to DHS. Several officials expressed a high level of frustration with respect to the ability to gain access to, and communicate with, Federal officials who are in a position to render timely decisions on a range of issues. In other words, DHHS has not yet been able to offer cooperative agreement recipients “one-stop shopping.” As a result, State and local public health officials reported that they often find themselves in the position of searching for appropriate contacts in the OPHEP, CDC, OEP, and HRSA to have their questions answered and to obtain technical assistance. Finally, a number of key policymakers pinpointed information technology as an area in desperate need of a long-range vision and plan, with one observer noting that despite years of trying, CDC has been unable to create a unified public health information system. This individual went on to describe the current patchwork of such systems simply as “a mess.”

Enhancing Research

The National Institute of Allergy and Infectious Disease (NIAID) will be spending more than \$1 billion dollars on new and improved prophylaxis and treatment for bioterror agents. While this is a considerable sum of money it should be recognized that it could take up to \$800 million dollars and 10 to 15 years to develop one new vaccine. In addition to research on prevention, treatment, and cures, research is also required in applied public health to provide insight into the best way to get people to follow an antibiotic regimen, for example. In the aftermath of the anthrax attacks, only 44 percent of those instructed to complete a 60-day course of Cipro actually did

so.¹⁵⁷ This does not bode well for quarantine, isolation, vaccination, or other public health measures.

Recommendation: That NIH, in collaboration with CDC, strengthen programs focusing on both basic medical research and applied public health research, and the application of new technologies or devices in public health; and that DHS and OHS, in cooperation, prioritize and coordinate research among NIAID, other NIH entities, and other agencies conducting or sponsoring medical and health research, including DoD, DOE, and USDA, to avoid unnecessary duplication

Enacting Legal and Regulatory Changes

The Model Health Powers Emergency Act, a model law developed for the Federal Centers for Disease Control and Prevention and provided to State legislatures last year, would give authorities the right to enforce quarantines; vaccinate people; seize and destroy property without compensation; and ration medical supplies, food, and fuel in a public health emergency. It has been adopted by more than a third of States while being rejected by at least 22 States. This model law seeks to modernize outdated public health laws enacted before the development of modern medical technology and to incorporate civil liberties issues.

Many States that have adopted it are in a holding pattern, waiting for the Federal government to organize itself to deal with bioterrorism before operationalizing the legislation. The Federal Health Insurance Portability and Accountability Act (HIPAA) is in part designed to keep information about patients confidential and defines narrowly the information and the circumstances under which that information can be released. The public health community is exempt from these regulations, and therefore, during a public health emergency, medical information can be shared with public health agencies. However, during investigations into potential bioterror events, the goals and operating procedures of health and medical and public safety officials often conflicts. For instance, medical personnel are focused on identifying the cause of disease outbreaks and often are not familiar with preserving evidence using a chain of custody. Law enforcement officials gather evidence as the basis for criminal prosecution and may not consider the need for disease related testing. There are no mechanisms that encourage the integration of law enforcement and public health investigations, both of which may uncover evidence that ultimately can be presented in a court of law or may require disease testing. The relationship between the public health agencies and law enforcement in these situations—especially around the sharing of individually identifiable data—needs to be clarified. Although State and local involvement is critical, the Federal government needs to create and maintain some level of uniformity in dealing with these situations.

Recommendation: That each State that has not done so either adopt the Model Health Powers Emergency Act, as modified to conform to any single State’s special requirements, or develop legislation of its own that accomplishes the same fundamental purposes; and work to operationalize laws and regulations that apply to CBRN incidents—naturally occurring, accidental or intentional, especially those that may require isolation, quarantine,

¹⁵⁷ Altman, Lawrence, K. “Many Workers Ignored Pill Regimen,” *New York Times*, October 30, 2002, available at <http://www.nytimes.com/2002/10/30/health/30ANTH.html> accessed on November 6, 2002.

emergency vaccination of large segments of the population, or other significant emergency authorities

Recommendation: That the Congress clarify the conditions under which public health agencies, EMS, and hospitals can share information with law enforcement officials in special emergency circumstances under HIPAA

Such special circumstances would include instances, for example, where public health or medical providers have reason to believe that a person being treated for an illness may be involved in the intentional spread of a communicable disease or where it is necessary to provide law enforcement assistance in tracking relatives or other individuals who may have been exposed to an infected person.

Recommendation: As a prerequisite for receiving Federal law enforcement and health and medical funds from the Federal government, that States and localities be required to develop comprehensive plans for legally-appropriate cooperation between law enforcement and public health, EMS, and hospital officials

A carefully-crafted fusion center at the State level for the sharing of information between law enforcement, public health, medical officials, and other emergency responders, which has appropriate safeguards for ensuring confidential information to the maximum extent possible is a potential model.

Determining Who Is In Charge

The OHS is working to create an overarching National Incident Response Plan to consolidate and replace the Federal Response Plan and numerous other Federal plans that may be invoked during a terrorism or disaster response. This plan will serve to ensure better clarity of purpose and better understanding of responsibilities. The *National Strategy* provides that the Secretary of DHS will have the responsibility for “coordination and integration of Federal, State, local, and private” activities for critical infrastructure protection (CIP). It does not, however, provide any vision about the extent to which DHS will be “in charge” of executing a response during or after an attack on some CIP sector; nor does it specify which Federal agency is in charge for the Federal sector for other types of attacks, especially a biological one. Earlier in this report, we made specific recommendations that bear repeating here.

Recommendation: That the President and the Congress clearly define the responsibilities of DHS and other Federal entities before, during, and after an attack has occurred, especially any authority for directing the activities of other Federal agencies

That situation is especially problematic when it comes to a bioterrorism attack. No one in the Federal structure can currently identify who is or, after DHS is formed, will be in charge in the event of a biological attack.

Recommendation: That the President specifically designate the DHS as the Lead Federal Agency for response to a bioterrorism attack, and specify its responsibilities

and authority before, during, and after an attack; and designate the DHHS as the Principal Supporting Agency to DHS to provide technical support and provide the interface with State and local public health entities and related private sector organizations

Establishing Public Communications Strategies

Last year the panel recognized the critical role of a well-designed public affairs strategy in informing the public, minimizing psychological impacts, and preventing the spread of misinformation in the event of a public health emergency. The communications response to the anthrax attacks of last fall demonstrated that Federal, State and local officials were not coordinating their statements, and this led to mistrust among the public, especially postal workers in Washington, DC. The development of a clear Federal strategy in coordination with State and local medical, public health, and elected officials is not evident.

Recommendation: That DHHS, in coordination with DHS, develop an on-going, well coordinated strategy for education of the public on the prevention, risks, signs, symptoms, treatments, and other important health and medical information before, during and after an attack or large-scale naturally occurring outbreak occurs

The strategy should include elements at the national, State, and local levels. This campaign should be led by a person or persons with medical and/or public health expertise with guidance from experts in risk communications as well as State and local emergency management and elected officials.

Additionally, much is still not known about the most effective ways to treat people with mental or emotional problems following a terrorist attack.

Recommendation: That DHHS, through the National Institute of Mental Health, and in collaboration with CDC, enhance funding for research into the prevention and treatment of the short and long-term psychological consequences of terrorist attacks¹⁵⁸

This should include a special focus on biological terrorism and include agricultural terrorism as well as chemical and radiological terrorism and address strategies to be used before, during, and after an attack to minimize the negative psychological impacts. This research should also take into account the impact of public affairs and public communication strategies on various

¹⁵⁸ NIH issued a grant notice on July 24, 2002 for the Rapid Assessment Post-Impact of Disasters grants under the Traumatic Stress Research Program available at <http://grants.nih.gov/grants/guide/pa-files/PAR-02-133.html> accessed December 2, 2002. The Bioterrorism Preparedness and Response Act signed by President Bush in June of 2002 includes \$1.6 billion which does not cover research but includes some funding for mental health in the following areas: creation of a National Advisory Committee on Children and Terrorism within DHHS; enhanced strategies by the Department of Veterans Affairs for mental health counseling, including counseling to emergency response providers; addition of behavioral psychology experts to the Emergency Public Information and Communications Advisory Committee; educational grants for underserved professions to appropriate organizations for bioterrorism and emergency response; and creation of health professionals volunteer registry. M. Dittman available at <http://www.apa.org/monitor/sep02/bioterrorism.html>

segments of the population, including healthcare workers and other emergency responders. The panel notes that, in the past, research has emphasized such acute events as bombings, but little research has been conducted on the psychological consequences of ongoing events when people do not know when they are going to end.

Reconciling Interagency Issues

The Intelligence Community is not well equipped to assess threats that would have a direct impact on the public, especially as a result of bioterrorism. It is not well connected to health and medical experts and facilities involved in this field, in part because of a lack of security clearances held by those health and medical officials. In-house health and medical expertise in the Intelligence Community is not sufficiently robust to provide for continuing strategic assessments of bioterrorism cause and effect.

Recommendation: That the Intelligence Community improve its capacity for health and medical analysis by obtaining additional expertise in the medical and health implications of various terrorist threats

Enhancing Pharmaceutical Supplies and Distribution

The FY03 budget provides \$65 million in grants to States for the implementation of distribution systems for pharmaceuticals through the National Pharmaceutical Stockpile (NPS). States are concerned about their ability to receive and distribute products from NPS, which is composed of twelve 50-ton “Push Packages” of medical supplies placed throughout the country that can be deployed to any location within 12 hours. The NPS program is also responsible for storing and distributing smallpox vaccine. Once packages from the NPS arrive at an airfield, CDC transfers authority for managing the contents of the packages to State and local officials. Federal officials have indicated that a number of States came up short in their cooperative agreement proposals with respect to their plans for stockpile receipt and distribution. Federal technical assistance is needed on the part of State and local health officials to develop and exercise these plans. The panel acknowledges recent Federal efforts but suggests that additional enhancements as well as ways of measuring the ability of States to distribute the NPS are still in order.

Recommendation: That DHHS significantly enhance technical assistance to States to help develop plans and procedures for distributing the NPS, continue to require exercises that demonstrate the States’ ability to employ the NPS, and use specific metrics for evaluating States’ capabilities

The timely research, development, production, and distribution of certain critical vaccines and other medical supplies continue to be perplexing problems.¹⁵⁹ Vaccines and pharmaceuticals can cost hundreds of millions of dollars to develop, and little incentive exists for commercial manufacturers to produce pharmaceuticals with a potentially small or variable market. Moreover, private industry has become more risk-averse where vaccines are concerned because of the liability that they may incur. In addition, the Food and Drug Administration (FDA) must license vaccines and other pharmaceuticals after meeting standards for both safety and efficacy, which further delays their availability to the market. Human testing for efficacy is unethical, potentially unlawful, in the case of biological and chemical agents for which there is no known cure. FDA inspections are becoming increasingly stringent, making licensing even more challenging.

Recommendation: That DHHS, in collaboration with DHS and DoD, establish a national strategy for vaccine development for bioterrorism, which will be consistent with the nation's needs for other vaccines

The strategy may include tax incentives, liability protection, public-private initiatives such as the Government Owned Contractor Operated facility recommended in our previous report, and a guaranteed market.¹⁶⁰

Implementing a Smallpox Vaccine

There has been significant debate on the nation's smallpox vaccination policy. This debate focuses on the uncertain level of threat of a smallpox attack and the certainty of adverse reactions to the smallpox vaccine. Recently, Federal health officials recommended a multiphase smallpox vaccination program for at risk emergency medical personnel with the Federal government assuming liability for adverse events related to vaccination. CDC sent a manual to all 50 States and Washington, DC in September 2002 with instructions on how to vaccinate entire populations within a week of an outbreak. The panel recognizes the significant accomplishment of acquiring sufficient doses of smallpox vaccine to immunize the population of the United States. The panel concurs with the evolving plan to voluntarily vaccinate limited numbers of healthcare providers and emergency responders.

Recommendations: That the smallpox vaccination plan be implemented in incremental stages with careful analysis and continuous assessment of the risks of the vaccine; and that DHHS place a high priority on research for a safer smallpox vaccine

¹⁵⁹ Wyeth announced that it would stop producing flu and pneumonia vaccines in 2002, leaving only one major producer. Recent experiences of the Department of Defense in the timely acquisition of reliable anthrax and adenovirus vaccines, as well as civilian shortages of influenza vaccines in 2000 and an ongoing tetanus toxoid shortage, highlight the magnitude of the problem. According to the American Society of Health System Pharmacists, supply problems for drug products have been increasing due to challenges in all segments of the supply chain: raw material sources, pharmaceutical manufacturers, federal regulators, wholesalers and other distributors, health care facilities, and pharmacies available at <http://www.ashp.org/shortage/> accessed on October 12, 2001. In our second report, we noted that the TOPOFF exercise, conducted in May 2000, highlighted existing problems in the delivery and distribution of vaccines, antidotes, and prophylaxes. Unfortunately, as of the writing of this report, the Department of Justice has not yet released the TOPOFF After-Action Report, which was due in November 2000.

¹⁶⁰ At the time of the publication of this report, the enabling legislation for DHS contains liability protection issues for certain activities. Those provisions are, however, subject to modification when the new Congress convenes.

CHAPTER VII. DEFENDING AGAINST AGRICULTURAL TERRORISM

Agriculture and the food industry are critical to the economic, social and, arguably, political well being of the United States. One in eight people work in an occupation that is directly supported by the industry, which makes it the country's largest single employer. Cattle and dairy farmers alone earn between \$50 billion and \$54 billion a year through meat and milk sales,¹⁶¹ while roughly \$50 billion is raised every year through farm-related exports. In 2001, food production constituted 9.7 percent of the U.S. Gross Domestic Product (GDP), generating cash receipts in excess of \$991 billion.¹⁶² Agriculture's share of commodities sold overseas is also more than double that of other industries, which gives the sector major importance in terms of helping Washington's balance of trade.¹⁶³ Food imports valued at approximately \$32 billion entered the market in 1998. Foreign sources accounted for 62 percent of fish, fish products and shellfish, 34 percent of fresh fruit, and 10 percent of fresh vegetables that Americans consumed in 1997.¹⁶⁴

Although significant, these figures do not take into account allied industries and services, such as suppliers, transporters, distributors, and restaurant chains. According to the Department of Commerce (DoC), the economic multiplier effect of exported farm commodities alone is in the region of twenty to one.¹⁶⁵ The downstream effect of a major act of terrorism against this highly valuable industry would likely be enormous, impacting all of these sectors and ultimately, on the American consumer him/herself.¹⁶⁶ In addition, there is likely to be a major psychological impact on the producers, responders and the public more generally, and the psychological consequences of an act of agricultural terrorism are not well understood.

While there has been a focus in recent years in the United States on detecting, preventing and responding to terrorist threats and incidents, agriculture is one area that has received less attention. The antiterrorism focus, which has involved substantial financial outlays, has developed an increasingly well-protected public infrastructure in most sectors where, at a minimum, risk analyses have been used to expand contingency and consequence management responses to include terrorist incidents. In terms of accurate threat assessments and consequence management procedures, the agricultural sector continues to exist as an exception to the wide-ranging emphasis that has been given to infrastructure protection in this country in part because the sector was not included under the provisions of Presidential Decision Directive 63 (PDD-63),

¹⁶¹ Overall livestock sales in 2001 were in excess of \$108 billion. See "Agro-Terrorism Still a Credible Threat," *The Wall Street Journal*, December 26, 2001.

¹⁶² Bureau of Economic Analysis, "Gross Domestic Product: First Quarter 2002 (Advance)," available at <http://www.bea.doc.gov/bea/newsrel/gdp102a.htm>.

¹⁶³ Shell, Ellen, "Could Mad Cow Disease Happen Here?" *The Atlantic Monthly*, 282/3, 1998, p. 92; "Stockgrowers Warned of Terrorism Threat," *The Chieftain*, August 19, 1999.

¹⁶⁴ Cohn, Jeffrey, "The International Flow of Food: FDA Takes on Growing Responsibilities for Imported Food Safety," *U.S. Food and Drug Administration, FDA Consumer Magazine*, January-February 2001 available at http://www.fda.gov/fdac/features/2001/101_food.html accessed October 31, 2002.

¹⁶⁵ Parker, "Agricultural Bioterrorism: A Federal Strategy to Meet the Threat" 11

¹⁶⁶ Wilson et al., "A Review of Agricultural Terrorism, Biological Crimes and Biological Warfare Targeting Animal Agriculture," p. 22.

which specified critical nodes deemed to be vulnerable to terrorist attack or disruption.¹⁶⁷ The current administration recognized agriculture and food as critical infrastructures that among other things “provide the essential goods and services Americans need to survive.”¹⁶⁸ However, because agriculture and food have only recently been acknowledged as critical sectors, because terrorist threats against these infrastructures are uncommon, and because the *National Strategy* is focused on protection and not response, relatively little action has been taken to address the threat.

To address this shortcoming, the Advisory Panel is making a number of recommendations. These recommendations represent the beginning of a comprehensive strategy to address the threat of agriculture and food terrorism with a focus this year on agriculture. As the country begins to understand the scope and magnitude of the problem and begins to institute remedial measures, the panel is likely to have additional recommendations. It should be noted that, where appropriate, agriculture and food should be integrated into existing systems for planning, prevention, response, and information sharing. In addition, the dual use nature of some of these actions should be maximized. For instance, improved disease surveillance in animals will help to detect naturally occurring outbreaks as well as purposeful attacks, and food monitoring will prevent the spread of mistakenly contaminated as well as intentionally contaminated food.

Improving Resource Allocations

There has recently been recognition of the potential threat by the Congress and the Administration. President Bush proposed \$146 million in new spending in FY03 to protect the nation’s food supply from animal and plant pests and diseases, strengthen food safety programs, and support specific research activities. Several areas of funding relate to homeland security and the protection of agriculture:

- “\$48 million increase for animal health monitoring to enhance the ability to quickly identify potential threats. These additional resources will be used to improve the emergency management system that coordinates and implements rapid response to an animal or plant pest or disease outbreak.
- “\$19 million increase in the Agricultural Quarantine Inspection (AQI) program for improved point-of-entry inspection programs by providing additional inspectors, expanding canine teams and state-of-the-art high definition x-ray machines at high-risk ports of entry. This will bring staffing at ports of entry to 3,974.
- “\$12 million increase for programs to expand diagnostic, response, management and other technical services within the Animal Plant Health Inspection Services (APHIS).

¹⁶⁷ In May 1998, the Clinton administration passed into law PDD-63 on Critical Infrastructure Protection. The initiative designates nine physical and cyber-based systems essential to the minimum operations of the economy and government that are deemed vulnerable to possible terrorist attack. Such sectors are taken to include: banking and finance; transportation; electricity, gas and oil; telecommunications; emergency law enforcement; government services; emergency fire; public health service; and the water supply. Agriculture and Food Safety is included as one of eight subgroups of the National Security Council’s (NSC) Weapons of Mass Destruction Preparedness Group, which was established in 1998 under the auspices of Presidential Decision Directive 62 (PDD-62), “Combating Terrorism.” See Henry Parker “Agricultural Bioterrorism: A Federal Strategy to Meet the Threat” McNair Paper 65, Institute for National Strategic Studies, National Defense University (March 2002), 30. For details on PDD-63 see White Paper, The Clinton Administration’s Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998.

¹⁶⁸ *National Strategy*, p. 30.

- “\$28 million increase for the Food Safety and Inspection Service (FSIS). The increase will support FSIS food safety activities, including maintaining approximately 7,600 meat, poultry, and egg products inspectors. This funding would include \$14.5 million to improve the information technology infrastructure to improve risk management systems and \$2.7 million for slaughter epidemiological surveys and risk prevention activities.
- “\$34 million increase to support research aimed at protecting the nation’s agriculture and food system from attack by animal and plant diseases, insects, and other pests and to reduce the incidence of food-borne illness in humans due to pathogens and other threats to the food supply. These increases will emphasize development of improved detection, identification, diagnostic, and vaccination methods to identify and control threats to animal and plant agriculture.
- “\$5 million increase to strengthen the capability of APHIS to assess and monitor outbreaks of diseases in foreign countries that have the potential to spread to the United States.”

In addition, appropriations for 2002 provided an additional \$328 million in USDA funding for homeland security related protections. This includes \$105 million for APHIS pest and disease exclusion, detection, and monitoring; \$80 million for upgrading USDA facilities and operational security; \$50 million for an animal bio-containment facility at the National Animal Disease Laboratory; \$40 million for the Agricultural Research Service; \$23 million for the Plum Island Animal Disease Center; \$15 million for security upgrades and bioterrorism protection for the FSIS; and \$14 million for increased security measures at the National Veterinary Services Laboratories in Ames, Iowa.¹⁶⁹

Understanding the Threat

As noted in the updated threat assessment earlier in this report, the threat to agriculture has received relatively little attention in the national security arena and from State, local, and private sector entities involved in this critical infrastructure. For a variety of reasons, the U.S. agricultural sector remains acutely vulnerable to attack. Critical susceptibilities stem from six main factors:

- The concentrated and intensive nature of contemporary U.S. farming practices;
- The increased disease susceptibility of livestock;
- A general lack of farm/food-related security and surveillance;
- An inefficient passive disease reporting system further hampered by a lack of trust between regulators and producers;
- Veterinarian training that tends not to emphasize foreign animal diseases (FADs) or large-scale husbandry; and
- A prevailing focus on aggregate, rather than individual animal statistics.

During the past administration, the industry was not recognized in the nation’s efforts to protect critical infrastructure and was not included under the provisions of PDD-63. Agriculture and Food Safety is included as one of eight sub-groups of the National Security Council’s (NSC) Weapons of Mass Destruction Preparedness Group, which was established in 1998 under PDD-

¹⁶⁹ Release No. 0026.02 Alisa Harrison “President’s Budget To Provide \$146 Million Increase in Funding to Protect Agriculture and the Nation’s Food Supply,” USDA News Release available at <http://www.usda.gov/news/releases/2002/01/0026.htm>, accessed on November 6, 2002.

62, “Combating Terrorism.” The USDA serves as chair of this subgroup. However, the USDA lacks sufficient visibility and influence to champion greater Federal attention to countering biological attacks against agriculture.

The USDA’s Office of Crisis Planning and Management (OCPM) is responsible for coordinating USDA’s requirements to the Intelligence Community and sharing intelligence information among USDA offices and agencies.¹⁷⁰ However, an overarching appreciation of the true threat to America’s agriculture is lacking. Without a broad threat assessment it is difficult to prioritize resources to counter the terrorist threat.

Recommendation: That the President direct that the National Intelligence Council, in coordination with DHS, USDA and DHHS, perform a National Intelligence Estimate on the potential terrorist threat to agriculture and food

Enhancing Planning

As with other disasters and emergencies, the response to an act of agricultural terrorism would require participation by numerous local, State, and Federal agencies, as well as industry and other private organizations. The response should be coordinated through the emergency management system. The Animal Health Emergency Preparedness Plan, developed by the National Emergency Management Association with funds from the USDA provides a guide for comprehensive emergency management plans for the response to emergencies involving animals and the animal industry segment of production agriculture, and as a source of information on national trends for States already having such plans. The plan is designed for inclusion in State Emergency Operations Plans. It builds on existing concepts of operation and mutual aid agreements.¹⁷¹ The Emergency Support Function (ESF) in the Animal Health Emergency Preparedness Plan is not currently applicable to any ESF in the Federal Response Plan. Therefore the State agency or agencies with statutory authority will be responsible for the function.

Recommendation: That the Assistant to the President for Homeland Security ensure that an Emergency Support Function for Agriculture and Food, consistent with the intent of the ESF described in the Animal Health Emergency Preparedness Plan, be included in the Federal Response Plan and the National Incident Response Plan under development

There are many critical aspects to such a plan. These include understanding who is in charge; the laws and authorities governing response; information sharing among those involved including all levels of government and the private sector; a comprehensive communication strategy for the public and including the media, which takes into account the psychological dimension of the threat; and response capabilities. Each of these is discussed in some detail below.

¹⁷⁰“National Security: U.S. Department of Agriculture,” available at <http://www.usda.gov/da/ocpm/security.htm>, accessed on November 6, 2002.

¹⁷¹ NEMA, Model Emergency Support Function for Production Agriculture, Animal, and Animal Industry,” September 2002, available at http://www.nemaweb.org/library/documents/Model_Plan_for_Animal_ESF.pdf.

The *National Strategy for Homeland Security* specifies that infrastructure protection will be integrated and coordinated in the Department of Homeland Security with the Department of Agriculture acting as the lead agency with the primary responsibility for interacting with the agriculture and meat and poultry sectors. The Department of Health and Human Services will be the lead agency for all other food products. Other agencies involved in protecting agriculture and food include the U.S. Departments of State and Commerce, the Environmental Protection Agency, and the Office of the U.S. Trade Representative. States also play a significant role. This plethora of interests may make it difficult to respond efficiently to an attack on America's agriculture or food.

Currently, as with bioterrorism, it is unclear who is in charge in the event of an agricultural attack at the Federal level. Several agencies are involved in different parts of the agriculture chain. As examples:

- FSIS regulates meat, poultry, and egg products, which account for thirty percent of consumer spending for food, with an annual retail value of \$120 billion. FSIS maintains a system of import inspection and controls. Also, FSIS annually “reviews inspection systems in all foreign countries eligible to export meat and poultry to the United States to ensure that they are equivalent to those under U.S. laws.”¹⁷²
- The FDA monitors all food sold in interstate commerce, including shell eggs but not meat and poultry, bottled water, and wine beverages with less than seven percent alcohol.
- The CDC investigates with local, State, and other Federal officials sources of food-borne disease outbreaks and maintains a nationwide system of food-borne disease surveillance.
- The National Oceanic and Atmospheric Administration inspects and certifies fishing vessels, seafood processing plants, and retail facilities for Federal sanitation standards.
- The U.S. Marshals Service seizes unsafe food products not yet in the marketplace, as ordered by courts.¹⁷³
- The U.S. Customs Service works with Federal regulatory agencies to ensure that all goods entering and exiting the United States do so according to U.S. laws and regulations.

While clearly much of the agricultural and food products that cross State and international boundaries are subject to inspection, FDA and USDA do not have the resources to inspect all of the food entering the United States. Therefore, these organizations must coordinate with those who export food to America to ensure the safety of American citizens. One vehicle for cooperation is the Codex Alimentarius Commission, run by the World Health Organization (WHO) and the Food and Agricultural Organization (FAO). Codex's 165 member countries establish international standards for agricultural products and food commodities and set safety standards for food additives and contaminants and for veterinary drugs.¹⁷⁴

The lack of clarity in the responsibility for agriculture and food safety may create confusion in the event of an attack on agriculture or processed food. Reflecting the mandate in the *National Strategy for Homeland Security*, if an attack of agricultural terrorism occurred in the United

¹⁷² FSIS Backgrounders, “Protecting the Public from Foodborne Illness: The Food Safety and Inspection Service, April 2001, available at <http://www.fsis.usda.gov/oa/background/fsisgeneral.htm>, accessed on November 6, 2002.

¹⁷³ U. S. Food and Drug Administration, FDA Backgrounder, “Food Safety: A Team Approach,” September 24, 1998 available at <http://vm.cfsan.fda.gov/~lrd/foodteam.html>, accessed on November 6, 2002.

¹⁷⁴ Ibid.

States, DHS should be the lead agency and USDA should be the principal supporting agency for a newly developed Emergency Support Function in the developing National Incident Response Plan. As such the USDA should coordinate with FDA, Customs, Commerce, and others and with State emergency management agencies and other State, local and private responders. As with other emergency functions this response function should be included in interdisciplinary terrorism response exercises.

The legal and regulatory regime must be clear when developing a plan to respond to an act of terrorism. The Model State Emergency Health Powers Act, written by Lawrence Gostin, provides a blueprint for State legislation that gives governors and State health officials the authority to enforce quarantines, vaccinate people, seize and destroy property without compensation, and ration medical supplies, food, and fuel in a public health emergency. It has been adopted by a number of States; however, there is no comparable legislation for authorities to respond to an agricultural attack. To standardize laws and authorities across the country the USDA should commission a Model State Agricultural Disease Emergency Security Act in consultation with State authorities.

DHHS has supported efforts to better connect emergency management, public health, law enforcement, and other entities involved in combating terrorism through such initiatives as the Health Alert Network (HAN). The agricultural community is not well integrated into this and other systems. In fact, many veterinarians are not connected to the Internet. As part of the emergency response plan described above, the USDA, DHHS, and DHS should work to include the agricultural community in all developing communications strategies.

For many animal diseases, vaccines and treatments exist that can limit the spread and scope of an attack; however, for foreign animal diseases, the stockpiles in the United States either do not exist or the numbers are inadequate. As part of the agricultural response plan, the USDA, in consultation with DHHS, should store vaccines, pesticides, herbicides, and other needed equipment and supplies as a component of the National Pharmaceutical Stockpile.” These supplies would be available for response to a large-scale outbreak. To decide on the components of the Stockpile, the USDA, in consultation with other relevant Federal, State, and local officials, and the private sector should undertake a study to understand current stores of needed pharmaceuticals and supplies and assess shortcomings based on a risk assessment for the agriculture and food sector.

The United States has not faced a mass disease outbreak in the agricultural sector in the recent past. It is unclear the psychological impacts of such an attack and such a response as a mass culling operation. Individuals affected by the FMD outbreak in the United Kingdom experienced a range of psychological symptoms. The results of a survey in Great Britain showed that those seeking assistance commonly experienced tearfulness, lack of sleep, loss of appetite, increased consumption of alcohol and tobacco, increased anger, irritability, increased marital and domestic discord, and general feelings of depression. Health practitioners also reported seeing farmers and business owners with a range of mental health problems from stress, anxiety, and depression.¹⁷⁵ To minimize the psychological impact, as part of the agricultural response plan,

¹⁷⁵ Deaville J, Jones L. The Health Impact of the Foot and Mouth Situation on People in Wales—The Service Providers Perspective. A summary report to the National Assembly for Wales by the Institute for Rural Health. May 2001.

the USDA in concert with DHS, DHHS, and State and local officials should develop a public communications strategy for before, during, and after an attack that takes into account the potential psychological impacts of an agricultural attack.

The American veterinary community is only partially integrated into Federal disaster response systems. In 1993, the American Veterinary Medical Association (AVMA) became part of the National Disaster Medical System (NDMS). Veterinary health professionals are organized into Veterinary Medical Assistance Teams (VMAT), which respond to the needs of animals during disasters. In 1994, the VMAT role was expanded to assist the USDA in the “control, treatment, and eradication of animal disease outbreaks.” The veterinarians, technicians, and support personnel provide assistance if the local veterinary community is overwhelmed. Deployment is meant to occur to any State or United States territory within 24 – 48 hours when the State officials from the affected State request their assistance. The members can sustain themselves for three days. Team members are preprocessed for Federal employment and issued identification cards. These persons can then be called to Federal service for up to 14 days as “special needs” employees of the U.S. Public Health Service and as such are protected under the Federal Tort Claims Act against personal liability and are exempt from licensure, certification, or registration requirements. The AVMA and American Veterinary Medical Foundation (AVMF) were recognized in 1998 as the only national organizations representing licensed veterinarians and are solely responsible for the care of animals, including during periods designated as disaster relief. These organizations should be carefully integrated into the ESF in the National Incident Response Plan and also into planning by State and local officials.

As with other parts of the economy, the agricultural system has moved to “just in time” logistics, but the disease surveillance system has not kept pace. Animals in the United States travel long distances during their lifetime and tracking mechanisms are insufficient. For instance, a pound of meat generally travels about 1,000 miles on the hoof before it reaches the dinner table. Between 20 and 30 percent of cattle were regularly consigned to non-slaughter destinations at least 25 miles from their original point of purchase and in many cases had crossed several States within 36 to 48 hours of leaving the sales yard. To enable rapid response to an act of terrorism against agriculture or a natural outbreak, tracking products from the breeder to the table is critical. This will involve both government and private sector personnel and resources.

Improving Laboratory Capacity

There are only two existing civilian biosafety level 4 (BSL 4) laboratories for working with and diagnosing the most hazardous animal pathogens, the National Veterinary Services Laboratories in Ames, Iowa, and Plum Island, New York. Infectious animal diseases can only be studied and Foot and Mouth Disease testing is only allowed at Plum Island by law.¹⁷⁶ Samples must be shipped to this location for testing, wasting precious time before the diagnosis of an outbreak. To minimize the impact of any outbreak it is critical that laboratory tests be performed quickly. Having to send samples across the country (if an outbreak occurred in California) might delay appropriate responses. Recognizing this, Ken Foster, professor of agricultural economics at Purdue University noted, “If some state diagnostic labs were allowed to test for FMD, that would

¹⁷⁶ Plum Island Foreign Animal Disease Laboratory available at http://www.globalsecurity.org/wmd/facility/plum_island.htm on November 11, 2002.

reduce the time it takes to make the diagnosis.”¹⁷⁷ The Armed Forces Institute of Pathology (AFIP), Department of Veterinary Pathology, can also assist in identifying and diagnosing animals’ diseases. If an outbreak of a foreign animal disease occurs in the United States, early detection will be critical in the containment and elimination of disease. These would provide insufficient capacity in the event of a large-scale outbreak. Probabilities suggest that by the time an outbreak is detected, it will have already spread to more than one location, probably in more than one State. Capabilities at the State level would increase the ability to detect foreign animal diseases early. A pilot program currently tests for eight animal diseases including foot and mouth disease, hog cholera, and others at the State level.¹⁷⁸

Recommendation: That the President propose and that the Congress enact statutory provisions for the certification under rigid standards of additional laboratories to test for Foot and Mouth Disease and other highly dangerous animal pathogens

At the end of 2001, the U.S. Animal Health Association (USAHA) passed a resolution recommending that the Department of Agriculture enable State veterinary laboratories to perform tests and increase surveillance for foreign agricultural diseases.¹⁷⁹ In its response to USAHA, USDA said that “(l)aboratory test results can be ready within between eight hours to several days after receipt of samples” and that “(i)n an outbreak situation, where laboratory diagnosis would overwhelm Federal capacity, consideration to allow State diagnostic laboratories to test would be given.” But without advance training and the appropriate equipment and security in place prior to an outbreak, it is not likely that State labs will be adequately prepared to respond to a crisis. With the creation of the Department of Homeland Security, that department will now have certain specific authority in this area.

Recommendation: That the Secretaries of Homeland Security and Agriculture (consistent with the November 2001 resolution of the United States Animal Health Association) jointly publish regulations implementing a program to train, equip, and support specially designated, equipped, secure, and geographically distributed veterinary diagnostic laboratories to perform tests and enhance surveillance for agricultural diseases that are foreign to the United States

Compensating for Agricultural Losses

The United States does not have a national, standardized system of compensation in place for reimbursement to producers for losses stemming from an agricultural disease outbreak. This lack of clarity may prevent producers, and others in the agricultural community from coming forward when they suspect infected animals or food. Otto Doering, professor of agriculture at Purdue University, recommends that the USDA distribute a decisive statement alerting producers that if FMD were found in their herds, they would receive adequate reimbursement for any

¹⁷⁷ Purdue News Service, “Purdue experts propose ideas to deal with foot-and-mouth disease,” April 13, 2001 available at <http://news.uns.purdue.edu/UNS/html3month/010413.Doering.fmd.html> accessed on November 11, 2002.

¹⁷⁸ Powell, Charlie, “WSU Animal Disease Diagnostic Laboratory Awarded \$750,000 for Homeland Security,” News @ WSU, August 30, 2002 available at <http://www.wsunews.wsu.edu/detail.asp?StoryID=3234>, accessed on November 29, 2002.

¹⁷⁹ See Appendix G.

animals destroyed. “Such things as larger payments for breeding stock need to be made clear so as to encourage farmers to come forward if there is an outbreak,” Doering said.¹⁸⁰ USDA provides compensation on a case-by-case basis. To encourage reporting of diseases and to ensure the stability of the agricultural sector, it is critical that a consistent scheme of national compensation be in place to provide financial assistance to producers and other agribusiness interests affected by an animal disease outbreak.

Recommendation: That the Secretary of Agriculture, in consultation with State and local governments and the private sector, institute a standard system for fair compensation for agriculture and food losses following an agroterrorism attack; and that the Secretary of Health and Human Services should develop a parallel system for non-meat or poultry food

The Animal and Plant Health Inspection Service (APHIS) recently published a proposed rule, “Foot-and-Mouth Disease Payment of Indemnity,” on May 1, 2002,¹⁸¹ that changes indemnity requirements primarily related to FMD. This rule would make the compensation of producers more fair and transparent and enhance the likelihood that they would come forward to report potential infections. This rule should be broadened to encompass all diseases that threaten livestock. Once a compensation plan is in place, the USDA along with State and local officials should develop an information dissemination strategy so that those involved will be well informed. In addition, incentives for disease reporting at all facilities and levels should be provided.

Promoting Better Education and Training

While some States are preparing for the threat of agricultural terrorism, others have not begun to establish the information sharing channels, plans, and structures to adequately address the threat. A number of different persons or entities at the State level are in charge of the public agricultural sector for the State including lieutenant governors and State cabinet level officials. These and other State and local officials need to be educated on the threat and need to open communication lines with State, local, and Federal law enforcement officials and the Intelligence Community.

At another level, there is a lack of expertise and sheer numbers of personnel available to work to secure the U.S. agricultural infrastructure. Not enough appropriately trained veterinarians are capable of recognizing and treating exotic livestock diseases in the United States because fewer people are entering veterinary science, reflecting the lack of educational support and financial incentive given to the discipline in the country and because most veterinarians focus on domesticated pets rather than large-scale husbandry. Veterinary degree curricula should include courses on foreign animal diseases. The need for more large-animal veterinarians was recognized in a recent conference entitled “Food Animal Veterinarians: An Endangered Species.”¹⁸² According to the American Veterinary Medical Association, which represents

¹⁸⁰ Purdue News Service, “Purdue experts propose ideas to deal with foot-and-mouth disease,” April 13, 2001 available at <http://news.uns.purdue.edu/UNS/html3month/010413.Doering.fmd.html> accessed on November 11, 2002.

¹⁸¹ Federal Register (67 FR 21934-21959, Docket No. 01-069-1).

¹⁸² Held at Kansas State University’s College of Veterinary Medicine, October 25-26, 2002 available at http://www.fass.org/fasstrack/news_item.asp?news_id=745, accessed on November 6, 2002

82 percent of veterinarians in the United States, only 751 veterinarians declare themselves as bovine exclusive with another 3,000 declared as “mixed large animal” veterinarians.¹⁸³

In addition, college curricula do not emphasize foreign animal diseases, with most focus on diseases endemic to the United States. Therefore, a dearth of accredited State and local veterinarians have either a background in farm animal diagnostics or the necessary expertise to deal with “Class A” agents.

Other types of expertise required for dealing with agricultural diseases are lacking. For instance, entomology expertise is shrinking, presenting difficulties for understanding vectors and response.¹⁸⁴ In addition, government compensation in laboratories is weak compared to the private sector, making it difficult to attract experienced personnel. This leaves the agricultural sector ill-equipped to recognize and respond to a manmade or naturally occurring attack against agriculture.

Recommendation: That the Secretary of Agriculture develop and that the Congress fund programs to improve higher education in veterinary medicine to include focused training on intentional attacks, and to provide additional incentives for professional tracks in that discipline

That the Secretary of Agriculture, in coordination with States, improve education, training, and exercises between government and the agricultural private sector, for better understanding the agroterrorism threat, and for the identification and treatment of intentional introduction of animal diseases and other agricultural attacks

¹⁸³ Author interview, October 31, 2002

¹⁸⁴ For instance the article by W. C. Reeves. “Concerns About the Future of Medical Entomology in Tropical Medicine Research,” *Am. J. Trop. Med. Hyg.* 1989, 40:569-570, laments the shortage of medical entomologists and “Growing Pest Control Industry Faces A Shortage Of Entomologists,” Wendy McDowell, UF/IFAS Educational Media & Services, (352) 392-2411, Sources: Phil Koehler, (352) 392-2484; Bruce McCown, (352) 376-2661, Feb. 18, 1997.

CHAPTER VIII. IMPROVING THE PROTECTION OF OUR CRITICAL INFRASTRUCTURE

In our previous reports, we have focused our attention in the area of critical infrastructure protection (CIP) on matters of cyber security. The cyber piece of the CIP effort continues to be, in our view, the most problematic and challenging in that arena. Much work has been done to enhance the physical protection of certain critical infrastructures, but more remains to be accomplished. Little real success has been achieved in the cyber realm, perhaps because of its complexities or perhaps because its imperatives are less well understood.

In our *Third Report*, we recommended that “the Congress create an independent commission, tasked to evaluate programs designed to promote cyber security, to identify areas where requirements are not being met, to recommend strategies for better security, and to report its findings to the President and the Congress.” That recommendation has not yet received favorable consideration by the Congress. Later in this chapter, we will restate and expand that recommendation to include all aspects of CIP, with a comprehensive framework for the types of issues that should be comprehensively addressed by that commission.

We have concluded that the physical and cyber elements of CIP are so intertwined that it makes no sense to address them separately. We will also make additional recommendations for improving CIP that need to be addressed on an urgent basis, regardless of whether a new commission is established.

First, some discourse on the current nature of the CIP problem is in order.

Reconciling Definitional Terms

“Critical infrastructure” can mean different things to different people. But it is important that everyone has a common baseline of definitions or terms, so we are not talking past each other. Neither the Administration’s proposed legislation for establishing the Department of Homeland Security nor the Bill as passed define the term; nor does the *National Strategy*.

There is a useful definition, at least, in the 1997 report of the President’s Commission on Critical Infrastructure Protection:¹⁸⁵

Infrastructures so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security.

That definition, or something like it, should be adopted by all policymakers.¹⁸⁶

¹⁸⁵ President’s Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America’s Infrastructure*, October 1997.

¹⁸⁶ In response to the Commission’s report, President Clinton signed Presidential Decision Directive Number 63 (PDD-63) on May 22, 1998. The Directive defined critical infrastructures as “those physical and cyber-based systems essential to the minimum operations of the economy and government.” That, in our view, falls well short of a comprehensive and comprehensible definition. A more comprehensive definition is contained in Section 4. (2), S. 1456 Critical Infrastructure Information Security Act of 2001 (Introduced in the Senate); September 24, 2001: “The term ‘critical infrastructure’--

The *National Strategy* the following as the “Critical Infrastructure Sectors:

- Agriculture
- Food
- Water
- Public Health
- Emergency Services
- Government
- Defense Industrial Base
- Information and Telecommunications
- Energy
- Transportation
- Banking and Finance
- Chemical Industry
- Postal and Shipping

Interestingly, the *Strategy* does not list “hospitals and other medical care providers;” that system is different from “public health,” especially since most of it belongs to the private sector; not all medical care is an emergency service. Nor does it list “law enforcement” unless that sector is subsumed in emergency services; of course, not all law enforcement is an emergency service.

More importantly, many in government and the private sector do not make the necessary distinction between “critical infrastructure protection”—often abbreviated “CIP”—and “critical information infrastructure protection”—sometimes called CIIP, or perhaps more appropriately “cyber security.”¹⁸⁷ CIIP or cyber security challenges permeate all CIP sectors and, indeed, now most every aspect of American life.

Enhancing Resources and Establishing Appropriate Burden Sharing

In the weeks and months following September 11, 2001, State and local governments and private sector entities responded to the increased threat to the nation by taking measures to safeguard their critical infrastructures and protect their populations and workforces. These additional costs were necessary but burdensome, and these actors looked forward to fiscal support for reimbursement and other resources that they believed had been promised by the Federal

“(A) means physical and cyber-based systems and services essential to the national defense, government, or economy of the United States, including systems essential for telecommunications (including voice and data transmission and the Internet), electrical power, gas and oil storage and transportation, banking and finance, transportation, water supply, emergency services (including medical, fire, and police services), and the continuity of government operations; and

“(B) includes any industry sector designated by the President pursuant to the National Security Act of 1947 (50 U.S.C. 401 et seq.) or the Defense Production Act of 1950 (50 U.S.C. App. 2061 et seq.) as essential to provide resources for the execution of the national security strategy of the United States, including emergency preparedness activities pursuant to title VI of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5195 et seq.)”

¹⁸⁷ The terms are, unfortunately, often used synonymously or interchangeably. See testimony of John Tritak, Director, Critical Infrastructure Assurance Office, before the Senate Judiciary Committee Subcommittee on Technology, Terrorism and Government Information, October 6, 1999.

government. Much of these funds have not yet found their way to the intended recipients. In the case of State and local governments, this is a particularly onerous, because many State constitutions require a balanced budget. In these States in particular, but to some degree in almost every jurisdiction, other services have been cut to pay for increased security. This problem is exacerbated by the continuously elevated threat level (yellow), recurring periods of heightened alert (orange level), and targeted warnings for specific regions of the country or designated critical infrastructures.

That does not suggest that such warnings are not well intentioned or necessary; they are. While the concerns that led to the warnings have not resulted in any more attacks, the burden these warnings place on both public and private sector organizations charged with security missions have been significant. That situation has been further complicated by the absence of any set of substantive actions that should be undertaken by an entity when a warning is received.

This fundamental issue—homeland security burden sharing—deserves far more formal attention.¹⁸⁸ While the September 2001 attacks made the importance of homeland security starkly clear, it did not help define who should pay for what, and what measures give the greatest return on investment remains unclear. This is one of the fundamental public policy issues of the next decade, and one that will significantly affect such critical issues as the provision of homeland security and national defense, the maintenance of social well being, and the health and viability of U.S. commercial interests. The second of these is a first-order question that requires innovative thinking and solid economic analysis and a question that we believe can only be answered by a body of experts, sufficiently sheltered from the dynamics of the political process to permit it to conduct objective research and analysis.

Improving Information Sharing

The homeland security legal framework is relatively new and still developing. Many critical issues are being addressed by the Administration, the Congress, and State and local governments. One area of importance that crosses several boundaries, and one especially important in the context of CIP—especially cyber security—is information shared by private sector organizations with the Federal government. This can expose corporations to liability concerns as well as the potential for inadvertent disclosure of proprietary or other sensitive information.

There are provisions in the enabling legislation of the new Department of Homeland Security that provide certain protections for critical information provided *voluntarily* to the government by private sector entities.¹⁸⁹ That is an important step. It is reasonable to assume that, if such provisions are not deemed satisfactory by the government in terms of the quality or quantity of information provided, future legal or regulatory regimes may *demand* some types of information.

On the one hand, requiring that security related information be provided would force the private sector to implement better security practices to avoid liability, while on the other, failing to provide some liability protection would all but ensure that the private sector will not share

¹⁸⁸ Burden sharing implies the questions of public vs. private, and federal vs. State vs. local.

¹⁸⁹ Subtitle B, “Critical Infrastructure Information,” Pub. L. 107-296 (H.R. 5005, 107th Congress, 2nd Session), November 25, 2002, reproduced at Appendix M.

potentially critical information. This continues to create a conundrum for private entities and the government.¹⁹⁰

Determining Appropriate Identification and Access Control

The argument for a homeland security identification system for government employees performing critical or sensitive functions is not difficult to make. Indeed, all federal agencies currently have some form of identification system. More problematic is the concept of an identification system for private citizens who handle sensitive information or dangerous substances or otherwise perform functions critical to public health and safety. Examples of positions for which such a system might be desired range from the operators of nuclear power plants, to airline baggage handlers and drivers of HAZMAT trucks. Some of these positions will require nothing more than the ability to positively verify the identity of the person seeking access to a facility or information, while others may require some background checks or other information.

Concerns about privacy and misuse of personal data on the part of the government are prudent, and care must be exercised in examining the wisdom of such a system. Nonetheless, we feel that circumstances warrant examining the implications of such a system for certain jobs, as the implications for our collective security and individual health and safety are grave. Furthermore, any such system must be national in character if it is to be truly effective and may need to mesh with a future government identification system. However, meticulous care should be exercised in identifying what positions should be included in this scheme, what private information should be maintained on the holders of these positions, who should have access to that information, and how that information should be protected. All stakeholders must have their concerns considered, and have some form of representation in the deliberations on creating such a system.

Improving the Roles of the Public At Large

One component of the homeland security effort that has not gotten enough attention has been the role of the public as a critical component of the solution—indeed, as a critical infrastructure in and of itself. The Terrorism Information and Prevention System, generally referred to as Operation TIPS, was first introduced by President Bush as part of the USA Freedom Corps program in the January 2002 State of the Union address. It was envisioned as a voluntary reporting system to “enable American workers to report unusual and non-emergency issues that they observe in the normal course of their work.”¹⁹¹ Mail carriers, utility employees, truckers, and other workers were encouraged to report suspicious and potentially terrorist-related activity to the Operation TIPS website or telephone hotline, where it would be entered into a national database. However, the program came under intense opposition from Federal lawmakers, the American Civil Liberties Union (ACLU), and such government agencies as the U. S. Postal Service. The major concern was that it would infringe on the privacy rights of American citizens by encouraging millions of workers with access to private homes to spy on customers. As Rachel King, legislative counsel of the ACLU, argued, “The administration apparently wants to implement a program that will turn local cable or gas or electrical technicians into government-

¹⁹⁰ For a recent, excellent commentary on the nature of this problem, see the statement of Senator Robert Bennett, *Congressional Record*, November 19, 2002, pp. S11562-S11563, reproduced at Appendix N.

¹⁹¹ Statement of Barbara Comstock, Director of Public Affairs, Department of Justice, July 16, 2002.

sanctioned peeping toms.”¹⁹² Indeed, the Homeland Security Act of 2002 (H.R. 5005) included language that explicitly prohibited Operation TIPS from being implemented.

Despite the failed attempt of the TIPS program, there are tangible functions and responsibilities the public can and should take on, such as awareness of food and water safety issues, which do not which do not carry negative connotations.

But this issue is larger than that. In fact, “we should recognize that the government, alone, cannot always protect us from terrorists. Catching small, covert terror cells is not unlike catching spies—both seek to hide in and use our open society and the resources of our nation against us, and succeed by evading the government agencies established to protect society. History teaches that some will evade government detection.”¹⁹³

This topic is controversial on several levels. First, our very social fabric is founded on individual freedoms, and creating a situation in which neighbors spy on each other would not only be undesirable but almost certainly counterproductive. Furthermore, constructive involvement by the public would entail a significant education and training effort to make the general public aware of signs of terror (e.g., behavior patterns, suspicious materials, practices defined in terrorist training manuals) and not interpret religion, ancestry, or culture as terrorist indicators. Finally, a real reliance on public participation would involve a shift from a law enforcement/defense metaphor for homeland and national security, in which the government is responsible for our collective security, to a “wagon train” metaphor in which each member of society bears some responsibility for the collective security of the whole. That said, little hard analysis of this absolutely critical issue exists.

Enhancing Cyber Security

National coordination of cyber security policy has not significantly improved. The President’s Critical Infrastructure Protection Board (PCIPB) has not had a large affect on policymaking, apparently relying, instead, on the White House Office of Cyberspace Security. The *Draft National Strategy to Secure Cyberspace* presents a clear example. This document, introduced by a cover letter from the Chair and Vice Chair of the PCIPB, apparently has not been cleared by the full Board despite the appearance to the contrary in the introductory letter. Furthermore, the new governmental structure designated by Executive Order 13231 is in fact only marginally different than that put in place four years earlier by PDD 63. Moreover, recommendations in our earlier reports that key State and local government and private sector representatives be included on key policymaking entities, such as this Board, have not been acted upon.

In addition, the *Draft National Strategy to Secure Cyberspace* attempts to straddle the intellectual and policy gap represented by the power of the government to mandate certain actions that would have a salutary affect on the security of cyberspace with the tacit recognition that entrepreneurial forces are more efficient than government mandates. As a result, it continues and extends the policies in place for the past several years that rely on “public-private

¹⁹² Stacy Humes-Schulz, “Alarm Bells Ring Over Terrorism Reporting System,” *Financial Times*, July 23, 2002, p. 6.

¹⁹³ Terrence K. Kelly, “Vigilance is our Civic Duty,” *Pittsburgh Post Gazette*, September 11, 2002, available at <http://www.post-gazette.com/forum/comm/20020911edterr11p4.asp>.

partnerships”—meaning that it relies on private sector willingness to take certain security measures and bear their costs and chooses not to use government’s power to legislate, regulate, or otherwise require certain actions. As a result, the *Draft Strategy* poses what we view as voluntary, tactical responses to an inherently strategic problem of national importance. If it is adopted, it will be a step in the right direction but a small step indeed.

As we stated in our report last year, “This is an exceptionally complex topic, one that spans national security, law enforcement, civil [liberties], and commercial and other private-sector interests.”¹⁹⁴ If anything, cyber security, its importance, and the issue of who should bear the burden for providing it will increase in complexity and difficulty with the increasing complexity of the networks. It is our firm belief that the single most important step in developing good public policy for cyber security, and a step that is notably immature, is to develop an understanding of the problem. Other key background areas are an outline of the government approach to the problem, and private sector trends and concerns.

Earlier in this chapter we highlighted some concepts and analyses that must be undertaken, and which are critical to furthering our understanding of the general homeland security problem and development of cogent policy. But policy decisions by the Federal government are also hindering this maturation process. Key problems in the approach to date are defined by the following characteristics:

- Cyber security has been isolated and specialized, thus limiting its perceived relevance to day-to-day outcomes and even its relevance to what are viewed as clear and present homeland security threats.
- Creating a separate strategy and Executive Branch organizational structure for cyber and physical security has reinforced the isolated and add-on nature of cyber security to such an extent that it has drawn criticism from the private sector as burdensome bureaucratic layering, thereby significantly detracting from its relevance.
- In focusing on the need for public-private partnership so intensely, the government has failed to recognize the fundamental importance of market factors and largely failed to exercise any of its powers besides persuasion. As a result, there has been no change in the significant market disincentives to the adoption of cyber security measures necessary for ensuring the viability of critical functions performed by the information infrastructure that directly contribute to national needs (e.g., national security, public health, and safety).
- Applying this same standard to the public sector has produced the result that no one is clearly responsible for the security of information infrastructure “commons” or held accountable for cyber security lapses. The Federal government does not hold its leaders and managers responsible for cyber security. There are essentially little or no consequences for Federal government agencies and officials who do not take prudent steps to improve cyber security.

¹⁹⁴ *Third Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*, p. 41.

Accounting for Private Sector Concerns

The concerns expressed to us by key critical infrastructure stakeholders in the private sector are in certain respects divergent, but common themes exist. In general, extensive interviews conducted by supporting staff at RAND with representatives of key stakeholders indicate that

- The vast majority of security failures stem from poorly configured systems and workforce training issues, and are caused in part by poorly written software and the inability to understand the security implications of the increasingly complicated systems of systems that is the information infrastructure.
- Corporations are in the business of managing risk, of which cyber security risk is just one. If better risk models make clear that good cyber security is of greater value than previously acknowledged, businesses will invest in more of it.
- Rapidly changing technology, most prevalently in the form of mobile networks and embedded computing and communications devices, are likely to make the cyber security situation much worse if certain fundamental steps are not taken (e.g., establishment of security standards and improvements in software and hardware security engineering).
- Key reforms cannot be accomplished without fundamental changes in the information technology market that significantly increases the understanding of importance of cyber security.
- Mechanisms that could increase the market value of security include
 - statutes and regulation that require certain specified levels of security;
 - changes in insurance and auditing practices that reward good security practices;
 - increases in the availability of secure products and services brought about, for example, by demand from very large customers (e.g., the Federal government) and that significantly lower the cost of adopting more secure systems and practices by smaller customers and users; and
 - changes in liability law that assigns responsibility for security in both the enterprise and information infrastructure commons and limits the externalizing of cyber security risk.

The Need for an Independent Commission

Recommendation: That the Congress establish and that the President support an Independent Commission to suggest strategies for the protection of the nation’s critical infrastructures

The importance of such an Independent Commission is hard to overstate. This new area contains many very sensitive issues of great importance about which objective research and proposals are very difficult to conduct and develop within the political process. It is also important to realize that recommendations for resolving these issues cannot be based on the current make up of either the Executive or Legislative Branches of the Federal government and that issues requiring action by one branch or level of government (i.e., Federal, State and local governments) or the private sector, alone, do not in general require the special level of attention that makes an Independent Commission necessary. General categories of issues that might be appropriate for the Independent Commission include those that span different national equities—i.e., require actions by or changes in both the Executive and Legislative Branches of government; actions by or changes in multiple levels of government; government intervention in the conduct of private sector entities, and the internal and external relationships of entities in the private sector.

In line with our previous discussion of the central issues in critical infrastructure protection, it is our opinion that an Independent Commission must, at a minimum comprehensively address the following:

- **Burden sharing between public and private sector organizations responsible for homeland security, and among Federal, State and local governments, including basic principles and guidelines for these determinations. Such policies should be based on analysis of the effectiveness and efficiency of different types of programs and potential solutions.**
- **Liability protection for corporations that share information with the Federal government, taking into account compulsory and voluntary sharing considerations.**
- **The need for and impact of an identification system for private sector positions that have significant homeland security implications, including guidelines for such a system.**
- **Public participation in homeland security, including areas, if any, in which the government must have help from the public, how best to develop this capability, and the implications for civil liberties and effects on our culture.**
- **Critical social functions impossible to sustain without the information infrastructure, including options that would compel their security (e.g., regulations or statutes governing their security itself, audit standards or insurance provisions, and changes to liability laws that would place a reasonable share of the security burden on product/service providers).**
- **Information infrastructure “commons” and assigning responsibility for their security to appropriate public or private sector organizations or communities.**
- **In coordination with the President’s National Infrastructure Advisory Council, National Security Telecommunications Advisory Committee, and the President’s Committee of Advisors on Science and Technology and supported by comprehensive, expert economic analysis, examine the information technology market mechanisms to determine the information security market structure and competitiveness issues and make recommendations for changes that would accomplish the security goals established by the Independent Commission.**

If the Congress chooses not to create such an Independent Commission, these critical issues will, nevertheless, require the urgent attention of policymakers in a system of political pressure and other factors that have, to date, proven to be incapable of satisfactory resolution.

Regardless of whether the Independent Commission is created, are several additional CIP issues require immediate attention.

Developing Threat Assessments

The lack of a comprehensive assessment of threats to U.S. infrastructures significantly hampers defensive measures and preparedness activities. DHS will eventually establish the process for vulnerability assessment and “mapping” of the nation’s critical infrastructure. But that process must be informed by a clear articulation, on a continuing basis, of threats—strategically, operationally, and tactically. To the best of our knowledge, no comprehensive threat assessment exists to inform the process that DHS must manage.

Recommendation: That the President direct that the National Intelligence Council perform a comprehensive National Intelligence Estimate on the threats to the nation’s critical infrastructure

Creating More Effective Cyber Security Policy

DHS will be responsible for executing operations for CIP. But it will not, apparently—and logically so—be responsible for the development of all CIP policy. We assume that CIP strategic policy development will continue to be accomplished within the White House. But the continuing bifurcation of policy for the physical and cyber components of CIP has, as we have noted above, created confusion and resulted in less than effective policy formulation.

Recommendation: That the President direct the merger of physical and cyber security policy development into a single policy entity in the White House

Enhancing Aviation Security

Securing aircraft from all potential terrorist hazards is a very difficult task. In general, these hazards can be caused by passengers (i.e., the terrorists themselves) or cargo placed on the aircraft as baggage or non-passenger cargo (e.g., mail or general cargo). Progress in meeting airline passenger baggage-screening goals has been slow, and no screening technology will ever be foolproof. Perhaps equally important is the fact that much of the non-passenger cargo on commercial passenger aircraft is not being screened.¹⁹⁵ This task is hindered by physical (e.g., space for screening equipment) and technical limitations (e.g., a lack of screening equipment for large, bulky cargo). Furthermore, it is expensive and time consuming.

Recommendation: That DHS elevate the priority of measures necessary for baggage and cargo screening on commercial passenger aircraft, especially non-passenger cargo

Similarly, security of general aviation aircraft and facilities is thin, where it exists at all. Cargo aircraft, in particular, pose a significant danger that is not now adequately addressed, in that they have the potential to cause even greater damage than passenger aircraft if flown into a building or other ground target, because of the added kinetic energy provided by their substantially greater weight. Cargo flown on them is frequently not adequately screened for the reasons articulated above. Furthermore, measures to secure access to them are not nearly as rigorous as for passenger aircraft. Prudent measures can be undertaken at relatively low costs, especially controls on access to aircraft and ramp and hangar facilities where aircraft are parked or stored.

Recommendation: That DHS, in conjunction with the airline industry, develop comprehensive guidelines for improving the security of general aviation

¹⁹⁵ Greg Schneider, “Terror Risk Cited For Cargo Carried On Passenger Jets,” *Washington Post*, June 10, 2002.

Improving the Security of Dams

Hydroelectric and other dams on various watercourses present a significant hazard if terrorists find ways to exploit their controls. According to the U.S. Army Corps of Engineers National Inventory of Dams,¹⁹⁶ approximately 80,000 dams exist in the United States, of which approximately 24,000 would cause downstream loss of life if catastrophically breached. Of these, the Federal government owns approximately 2,100, with State and local governments and private sector organizations (e.g., utilities) owning the remainder.

The risks to dams varies, as does the ability of owners to provide adequate protection. No database currently contains the information needed to assess the risk to dams, and no national program exists for securing dams. This may stem from the fact that dams do not fall cleanly in any one infrastructure, but rather can be considered as part of the transportation, energy, and water infrastructures in different locations and circumstances. Threats to dams range from terrorist attacks to cyber intrusions. At least one recent incident has occurred of a teenage cyber “hacker” getting deep inside the control mechanisms for a series of dams in one State.

Recommendation: That DHS make dam security a priority, and consider establishing regulations for more effective security of dam facilities

Using Models and Metrics

One of the critical shortcomings in structuring programs and securing funds to protect critical infrastructures is the lack of risk-based models and metrics that help explain the value of protective measures in terms that public and private sector decisionmakers understand. Homeland security investment decisions are currently based on analysis of available information but the process for developing that information is far from rigorous. Many such investment decisions are based on partial descriptions of the problem and anecdotal evidence. However, by virtue of its enabling legislation, DHS will own the National Infrastructure Simulation and Analysis Center.¹⁹⁷ This asset provides DHS with a world-class modeling and simulation capability, expert analysts, and the opportunity to use these abilities and expertise to enhance CIP programs and guidelines.

Recommendation: That DHS use NISAC modeling and analytic capabilities to develop metrics for describing infrastructure security in meaningful terms, and to determine the adequacy of preparedness of various critical infrastructure components

¹⁹⁶ Available at www.crunch.tec.army.mil/nid/webpages/nid.cfm

¹⁹⁷ See <http://www.sandia.gov/CIS/NISAC.htm>.

CHAPTER IX. ESTABLISHING APPROPRIATE STRUCTURES, ROLES, AND MISSIONS FOR THE DEPARTMENT OF DEFENSE

A type of military motto has developed over time: “The mission of the U.S. Armed Forces is to fight and win the Nation’s wars.” For the past century, except for one incident, that has essentially meant fighting those wars on foreign soil. But the war on terrorism has come to our shores, and the actual as well as the perceived level of security we have historically enjoyed has been demonstrably challenged.

In light of what happened on September 11, 2001, and in the intervening months, it may now be necessary to return to some basic tenets on which the Republic was founded, and the Constitution of the United States of America is the appropriate starting point.

ARTICLE IV, Section 4. The United States shall guarantee to every State in this Union a Republican Form of Government, and shall protect each of them against Invasion; and on application of the Legislature, or of the Executive (when the Legislature cannot be convened) against domestic Violence.

Understanding the Proper Role of the Military in Homeland Security

Although our military forces have been designed to fight our Nation’s wars within a context of forward deployment and engagement, there is no question that some of the Department’s warfighting capabilities and resources are also applicable to homeland security.

At times, using the military domestically raises difficult issues about the division of State and Federal power. Unless they occur on a Federal reservation, and sometimes even then, homeland security responses will likely begin with the local and State responders. Within a State, the governor controls the National Guard and the State emergency management agency when an incident is controlled or managed by the State. When U.S. active duty and reserve forces become involved, they serve under the President. The President also has the Constitutional power to federalize the National Guard for various contingencies.

Using the military for homeland security inevitably has raised concerns about the proper roles and rules for use of the military domestically. There are several laws that proscribe the use of active duty forces domestically, the most widely known being the Posse Comitatus Act.¹⁹⁸ The existence of such laws is an indication of the concern within the country that the military not be misused. As the Advisory Panel has noted in a previous report, there is a significant problem in implementation of these laws caused by the widespread confusion about their interpretation and how they apply to specific situations. As a result, military response to many homeland security situations may be delayed in order to work through the legal issues.

¹⁹⁸ 18 U.S. Code, Section 1385. For a complete discussion of the laws for use of the military domestically, see our *Second Report*, Appendix R, and our *Third Report*, Chapter VI.

The new *National Strategy for Homeland Security* acknowledges the important role of the military in homeland security.¹⁹⁹ In this context, “homeland security” is an overarching term comprising two missions: “homeland defense” and “civil support.”²⁰⁰ According to the Department of Defense (DoD), the term homeland defense refers to military combat missions; that is, military sea, air, and, land operations wherein DoD leads and other Federal agencies may provide support. Operation Noble Eagle, which provides for air defense of U.S. territory against terrorist attacks, is a recent example.

Providing for the Defense of the Homeland

That the military has a clear mission to provide “homeland defense”—one in which it “would take the lead in defending the people and the territory of our country, supported by other agencies”—is a clear and sober fact recognized by the new *National Strategy for Homeland Security*.²⁰¹

In its *Second Report*, the members of this panel, with a single exception, made an explicit recommendation about the use of the military:

We recommend that the President always designate a Federal civilian agency other than the Department of Defense (DoD) as the Lead Federal Agency.

We made that recommendation in the context of the potential involvement of multiple Federal, State, and local entities being engaged in a response to a planned or potential terrorist attack. A word of clarification about our previous recommendation is, perhaps, now in order. We recognize that certain responses to attacks may be exclusively or at least primarily military missions. The attacks of September 11 of last year are instructive. After the two hijacked airliners crashed into the Trade Center towers and a third crashed into the Pentagon, it was quickly discovered that a fourth had also been hijacked and had turned toward the Nation’s Capital. We now know that, but for the courageous and heroic intervention of some of our fellow citizens, United Airlines Flight 93 may have been shot down by Air Force fighters launched to intercept it. We now acknowledge that, for certain actions by terrorists that may rise to the level of an “invasion”—from the air, from the sea, and potentially even from land external to the United States—the military may have to take the lead in responding. In certain circumstances, no other agency of government, at any level, will likely have the capability to respond to such attacks. That concept is firmly embedded in the formation of the new U.S. Northern Command, discussed in greater detail below.

Providing Military Support to Civil Authorities

The new *National Strategy* also recognizes that the Department of Defense has an additional significant homeland security mission—military support to civil authorities. This is not a totally new mission. The military regularly is called on to provide assistance to civil authorities to deal

¹⁹⁹ *The National Strategy for Homeland Security* (Washington, DC: The White House, Office of Homeland Security, July 16, 2002), p. 13, available at online at http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

²⁰⁰ In this report, we use interchangeably the terms “civil support” and “military support to civil authorities.”

²⁰¹ *National Strategy*, p. 13.

with natural disasters (e.g., hurricanes, floods, and fires), as well as manmade incidents (e.g., riots and drug trafficking).

The military is called on to perform these missions because it moves and organizes large numbers of trained personnel to provide a coordinated response to incidents at home and because the military has developed specialized capabilities (particularly medical, engineering, and chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) weapon response capabilities) that either do not exist at the State and local level or do not exist in sufficient quantities. In using the military domestically, a number of legal and political issues arise.

Increased homeland security concerns also have focused attention on the National Guard's domestic role. Given its nationwide disposition and connection to local communities, the Guard is arguably well suited to provide assistance when civilian capabilities are overwhelmed in an emergency. However, the National Guard is also an important part of the U.S. military's power projection capability. Therefore, devoting National Guard resources to homeland security and the potentially competing demands of foreign warfighting have consequences for both that need to be considered. We discuss the role of the National Guard in greater detail below.

DoD defines civil support as mutual support activities it undertakes with any civil government agency for planning or responding to the "consequences of civil emergencies or attacks, including national security emergencies." Civil emergencies include "any natural or manmade disaster or emergency that causes or could cause substantial harm to the population or infrastructure."²⁰² The 2002 deployment of military forces to assist Federal border security agencies is a recent example of a civil support operation.

For those missions involving military support to civil authorities, the Advisory Panel reaffirms the normal—and logical—sequence of commitment for response to a terrorist attack outlined in its *Second Report*, and for the appropriate place for employment of military forces. In this regard, response to terror threats or attacks will be led by first responders, those who serve the communities in which the incident has occurred. Responding second are those organizations mobilized under the leadership and authority of the State governors (including the National Guard of the several States), including requests for assistance from a full range of State and Federal law enforcement agencies. Within this context, a governor could request assistance from National Guard units from adjoining States under voluntary State compacts. At the point when response requirements exceed the State's capacity, a governor could request assistance from the President, who would designate a Lead Federal Agency to manage the U.S. response. The Advisory Panel has recommended in past reports that the Lead Federal Agency be a civilian agency, rather than the Department of Defense. The President's assistance might include the deployment of Federal military forces as a last resort.

The military has a long history of providing support to civil authorities to deal with natural and manmade disasters. This assistance is now common: between 1998 and 2000, the military

²⁰² Department of Defense, Directive 3025.15 (Washington, DC: Department of Defense, Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, 18 February 1997), sections E2.1.3 and E2.1.9.

supported an average of 73 events per year.²⁰³ Large-scale incidents can create significant demand for military forces. Notable examples of such incidents in the last decade, beyond the post – September 11 activities, include the Los Angeles Riots and Hurricane Andrew in 1992, the 1995 bombing of the Murrah Federal Office Building in Oklahoma City, Hurricane Floyd in 1999, the Western forest fires of 2000, and the 2002 Olympics in Salt Lake City.

Each homeland security incident that requires military support to civil authorities will involve a unique size and mix of forces. Specialized military capabilities are deployed as required and responding forces also typically include general-purpose units and military police; air transportation; engineers; signal operators with communication equipment; medical experts; and a command element with expertise in the law, public affairs, and intergovernmental coordination.

While the military participates in numerous missions to support civil authorities each year, the Department of Defense does not count this support as its primary mission. Warfighting is the Department's primary mission and takes priority unless the Secretary of Defense directs otherwise.²⁰⁴ Therefore, with the exception of a limited number of specially-trained units (e.g., the National Guard's Weapons of Mass Destruction Civil Support Teams (WMDCSTs), the forces DoD provides to support civil authorities are primarily trained to perform their warfighting missions. In addition, these forces may not always be available. While demand for military civil support operations may increase in the future, so might the military's warfighting commitments increase (e.g., for the global war on terrorism or a conflict in Iraq²⁰⁵). Therefore, we must consider what homeland security capabilities we are counting on DoD to provide, whether it is the most appropriate provider of those capabilities, and how to handle simultaneous demand for overseas warfighting and homeland security missions.

The President has recognized the challenges ahead in his *National Strategy for Homeland Security*. The *National Strategy* has identified three broad roles the military might be called upon to perform domestically, including executing homeland defense missions with support from other agencies, responding to emergencies to provide capabilities that other agencies do not have, and supporting the lead Federal agencies for "limited scope" missions such as national security special events. The strategy also provides details on potential DoD combating terrorism operations: "Military support to civil authorities pursuant to a terrorist threat or attack may take the form of providing technical support and assistance to law enforcement; assisting in the

²⁰³ LTC James Rice, United States Army, Deputy Special Assistant for Military Support, Office of the Secretary of the Army, remarks before the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, September 30, 2002, Arlington, Virginia.

²⁰⁴ An analysis of the Defense Department's combating terrorism directives has determined that "the military's non-MSCA [military support to civil authorities] operations take priority, unless the Secretary of Defense determines otherwise." This guidance on civil support is provided in Department of Defense Directive 3025.1, at A.2.-6. The analysis is presented in Barry Kellman, *Managing Terrorism's Consequences: Legal Issues* (Oklahoma City: Oklahoma City National Memorial Institute for the Prevention of Terrorism, March 2002), chap. 2, p. 14.

²⁰⁵ According to an official in the office of the Defense Department's Director of Military Support, a large-scale conflict abroad, with Iraq for example, could significantly reduce the military resources available at for civil support operations in the U.S. homeland. COL Ricki L. Sullivan, Chief, Military Support Division, Department of the Army, RAND staff interview, the Pentagon, Arlington, Virginia, November 7, 2002.

restoration of law and order; loaning specialized equipment; and assisting in consequence management.²⁰⁶

Reviewing the historical support that the military has provided to civil authorities can help us anticipate the kinds of support and level of effort that the military may be called upon to provide in the future to respond to terror attacks. After the Oklahoma City bombing, the U.S. military deployed about 800 active and reserve personnel, while the Oklahoma National Guard provided 465.²⁰⁷ The military support provided included medical and rescue teams, structural experts, and air and ground transportation. After the September 11 attacks, DoD provided 657 active duty personnel to support response operations at the Pentagon and the World Trade Center. DoD support deployed to the Pentagon included a defense coordinating element, logistics support, and engineers. Most of the active duty military support at the World Trade Center came from the 387 personnel manning the hospital ship *Comfort*, but it also included a defense coordinating element, a medical mobilization center, logistics support (airlift), and subject matter experts on demolitions and remote sensing operations.²⁰⁸ The National Guard provided the lion's share of the military forces responding to the crisis in New York City. At their peak, a total of 5,070 New York and 1,006 New Jersey National Guardsmen were committed to the effort.²⁰⁹

Given its size, nationwide disposition, and inherent capabilities, the Army, including the Army National Guard, can be expected to provide most of the military support in the event of future attacks with CBRN weapons. The Army's potential level of effort for such incidents has been estimated by extrapolating from past support operations. Using this approach, RAND estimates that an Army response could range from approximately 4,000 soldiers for a small biological or radiological attack, to more than 20,000 to respond to a large-scale anthrax attack in which more than 15,000 people have been exposed.²¹⁰

IMPROVING STRUCTURES FOR THE USE OF THE MILITARY DOMESTICALLY

New homeland security missions for combating terrorism warrant dedicated civilian and military organizational structures. Since the terrorist attacks of September 2001, the Department of Defense has restructured both the civilian oversight roles and the military organizations that deal with homeland security. In this report, we assess the progress in both organization and missions for providing military support to civil authorities, and recommend further improvements for military capabilities that may strengthen the Nation's ability to combat terrorism.

²⁰⁶ *The National Strategy for Homeland Security*, (Washington, DC: The White House, Office of Homeland Security, 16 July 2002), available at online at http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

²⁰⁷ "After Action Report for Oklahoma Bombing Incident of 19 Apr 95," completed by the Fifth U.S. Army and Fort Sam Houston, August 17, 1995.

²⁰⁸ Department of the Army, Office of the Director of Military Support, information paper, "DOD Support to the Events of and Subsequent to Sept 11th 2001," Undated.

²⁰⁹ Office of the Director of Military Support, information paper, "DOD Support."

²¹⁰ Richard Brennan, "U.S. Army Finds Its Role at Home Up for Grabs," *Rand Review*, Vol. 26, No. 2, Summer 2002 (Santa Monica: RAND, 2002), p. 47; and Eric V. Larson and John E. Peters, *Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options* (Santa Monica: RAND, 2001), p. 167.

Organizing the Defense Civilian Structure for Homeland Security

Decisions to deploy military forces for homeland security activities are not made by the uniformed military; such decisions are made by the Secretary of Defense, or his designated agent. The Department of Defense is reorganizing both the military command structure and the civilian oversight structure dedicated to homeland security. In November 2002, Congress approved the request from the Secretary of Defense to create a new Assistant Secretary position within the Office of the Secretary of Defense to oversee the support that the military provides for homeland security. We congratulate the Congress and the Administration for creating this new position. This office will formulate DoD homeland security policy and oversee the approval of military contributions to the national homeland security effort. In situations where the lead Federal agency (most likely either the Department of Homeland Security or the Department of Justice) determines it needs military assistance, it would direct a request to the Secretary of Defense. To expedite the process, decisional authority is anticipated to be delegated to the new Assistant Secretary for Homeland Defense; however, the Secretary of Defense will retain approval authority for responses to acts of terrorism, deployment of assets to deal with CBRNE, and military assistance for civil disturbances. The Assistant Secretary of Defense would review the request and, if it were determined that DoD can meet the request, would direct the Joint Staff to select the military assets that will be used and issue deployment orders.

In this arrangement, the Assistant Secretary of Defense for Homeland Defense will assume the role that the Secretary of the Army (i.e., as the Secretary of Defense's Executive Agent for civil support) and his Director of Military Support (DOMS) filled in the past. The ASD Homeland Defense will have a much broader portfolio than DOMS had, because he will be responsible for all DoD homeland security support to Federal, State, and local authorities as well. In most cases DoD would play a supporting role in homeland security; however, there are some cases when the President might order the military to take the lead to thwart a terrorist attack. Oversight of preparations for such activities to combat terrorism is vested by the Secretary of Defense in the Under Secretary for Policy and the Assistant Secretary for Special Operations-Low Intensity Conflict (SOLIC).

We have noted here important developments in DoD's organization. The panel reaffirms its view that command and control relationships must be very clear and practiced. Responsibilities and authorities must be clearly prescribed and exercised. However, it is also important for DoD to articulate the many changes it is making so that the American people understand how their government is moving to protect them from new threats. As such, the Advisory Panel applauds Congress for directing the Secretary of Defense to submit a detailed report describing DoD's homeland security responsibilities and how it is preparing to discharge them.²¹¹

Organizing the Military Structure for Homeland Security

In our *Third Report*, we recommended "that the National Command Authority establish a single, unified command and control structure to execute all functions for providing military support or assistance to civil authorities." A new geographic combatant command, U.S. Northern Command (NORTHCOM), has been established in the Unified Command Plan, effective October 1, 2002.

²¹¹ U.S. House, 107th Congress, 2nd Session, Conference Report on H.R. 4546, *Bob Stump National Defense Authorization Act for Fiscal Year 2003*, November 12, 2002, section 1404.

Based at Petersen Air Force Base in Colorado, the new command has been assigned the mission of defending the continental United States, Alaska, Puerto Rico, and the U.S. Virgin Islands and for providing military support to civil authorities.²¹² The Command describes its mission, inclusive of both its homeland defense and civil support responsibilities, as follows:

The command's mission is homeland defense and civil support, specifically:

- *Conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned area of responsibility; and*
- *As directed by the President or Secretary of Defense, provide military assistance to civil authorities including consequence management operations.*²¹³

NORTHCOM is in a transition between initial operational capability and full operational capability. In its initial structure, NORTHCOM has few permanently assigned forces, and most of them serve as part of its homeland security command structure. NORTHCOM's commander will exercise combatant command authority over his own headquarters in Colorado Springs, the Joint Force Headquarters Homeland Security (JFHQ- HLS), the Joint Task Force 6 (JTF-6) counterdrug headquarters, and the Joint Task Force Civil Support (JTF-CS), which provides command and control for all Federal military forces operating in support of a lead Federal Agency to manage the consequences of CBRNE incidents. Commander NORTHCOM may also exercise combatant command authority over the Cheyenne Mountain Operations Center.

The JFHQ-HLS, located in Norfolk, Virginia, was established by Joint Forces Command immediately after September 11, 2001 to coordinate the land and maritime defense of the continental U.S. as well as military assistance to civil authorities for "all hazards." At NORTHCOM's initial operational capability, combatant command over JFHQ-HLS was transferred to NORTHCOM. The ultimate role and status of this headquarters is pending design determination of NORTHCOM at full operational capability. The Commander of NORTHCOM also serves as Commander, U.S. Element NORAD, and currently as commander of NORAD, the U.S.-Canadian Aerospace Defense Command. In these, roles he conducts and coordinates North American air defense. NORTHCOM, at least initially, does not have control of any other units. As is the case with other regional combatant commanders, Joint Forces Command (JFCOM) will act as NORTHCOM's primary "force provider" if additional units or personnel are needed for any planned or contingency operations and for exercises. As such, NORTHCOM will only be given control of air, land, sea, and maritime forces when required to perform an assigned task.

Although NORTHCOM's mission statement implies that the Command could be directed to execute *counterterrorism* operations in support of civil authorities,²¹⁴ we are not aware of any deliberate planning by the Command to support such a contingency. Conceivable events (e.g., multiple, geographically dispersed terrorist operations within U.S. territory) might exhaust civil

²¹² U.S. Pacific Command has responsibility for Hawaii.

²¹³ NORTHCOM Mission Statement, available at

<http://www.northcom.mil/index.cfm?fuseaction=s.whoware§ion=3>, accessed on December 5, 2002.

²¹⁴ DoD defines counterterrorism as "offensive measures taken to prevent, deter, and respond to terrorism." It defines antiterrorism as, "Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces." See Department of Defense, *DoD Dictionary of Military and Associated Terms*, Joint Publication 1-02, as amended through August 14, 2002, available at on the internet at <http://www.dtic.mil/doctrine/jel/doddict/index.html>.

and other limited military resources envisioned for use in existing national plans. Moreover, scenarios exist within which NORTHCOM might then be directed to provide additional support to civil authorities *regardless* of its pre-incident focus on planning and training for the so-called “consequence management” mission. We have consistently noted in this and earlier reports that ample statutory authority already exists for use of the military to provide a wide range of support to civil authorities, including very specific types of support under special terrorism statutes,²¹⁵ as well as more general authority under such other provisions as the Insurrection Statutes.²¹⁶

Recommendation: That the Secretary of Defense clarify the NORTHCOM mission to ensure that the Command is developing plans across the full spectrum of potential activities to provide military support to civil authorities, including circumstances when other national assets are fully engaged or otherwise unable to respond, or the mission requires additional or different military support. NORTHCOM should plan and train for such missions accordingly

The creation of NORTHCOM is an important step toward enhanced civil-military integration for homeland security planning and operations and could result in an enhancement of homeland security response capabilities. NORTHCOM has the responsibility to plan for a number of critical military homeland security activities. NORTHCOM will need to train and exercise with civil authorities at all levels of government—Federal, State, and local. Given its command relationships, Commander NORTHCOM will be well positioned to ensure unity of command and effort when military units are employed for homeland missions under Federal authority.

In our *Third Report*, we recommended that a unified command be created “to execute all functions for providing military support or assistance to civil authorities”—an all-hazards approach. The Advisory Panel is pleased that NORTHCOM will apparently execute *most* of these functions, and adds the following:

Recommendation: That the NORTHCOM combatant commander have, at a minimum, operational control of all Federal military forces engaged in missions within the command’s area of responsibility for support to civil authorities

IMPROVING MILITARY CAPABILITIES FOR HOMELAND SECURITY

The Administration and Congress have improved the Federal government’s structure for the delivery of military support to civil authorities. However, the panel believes additional enhancements are possible and necessary. The President and Congress should clarify legal authorities for military activities within U.S. territory. Training for civil support operations should be increased across the armed forces. As the panel notes in Chapter V, Organizing the National Effort, and later in this chapter, the President and the Congress should initiate a rigorous assessment of national preparedness requirements. That assessment should be used to evaluate further enhancements to the military’s ability to deliver needed capabilities as part of the national homeland security effort. Finally, the National Guard’s homeland roles and missions must be reevaluated in light of the new security environment facing the Nation.

²¹⁵ 10 U.S. Code, Section 1282, and 18 U.S. Code, Section 831.

²¹⁶ 10 U.S. Code, Sections 331 et seq.

Clarifying Posse Comitatus and Other Relevant Statutes

Currently, there is a debate within the country on the authorities granted by the Posse Comitatus Act. Historically, Americans have been hesitant to use the armed forces for internal security. In general, the Posse Comitatus Act prohibits the Federal military's participation in front-line law enforcement activities, such as arrest, search, seizure, surveillance, or pursuit of convicted or suspected criminals. Some believe the laws governing the domestic use of the military should be modified to tighten restrictions on military law enforcement activities. But in the last year, the military has been used in new ways to support homeland security missions. For example, in October 2002 military reconnaissance aircraft were used in an attempt to locate the sniper terrorizing the Washington, DC area. Some leading members of Congress believe the time has come to re-examine the 1878 law in light of the new security environment the Nation faces.²¹⁷ In considering the role of the military in homeland security and its use in support of civil authorities, the Advisory Panel reviewed again the authorities granted in current law to assess its position on the debate.

The President's homeland security strategy calls for a "thorough review of the laws permitting the military to act within the United States in order to determine whether domestic preparedness and response efforts would benefit from greater involvement of military personnel and, if so, how." The panel previously noted that significant statutory and regulatory authority already exists for using the military inside the United States, especially under the insurrection statute.²¹⁸ However, there remains widespread confusion about Posse Comitatus and other statutes that address domestic use of the military. For that reason, the Advisory Panel supports the review proposed by the Administration in the *National Strategy* as a means to bring clarity to this important issue.

To achieve that clarity, the laws governing domestic use of the military should be consolidated and the Federal government should publish a document that clearly explains these laws.²¹⁹ In consolidating the laws, the legislation should clarify ambiguities about the authority to use the military to respond to terrorist acts involving chemical, biological, radiological and/or nuclear weapons as well as conventional or cyber attacks.

Recommendations: That the President and the Congress amend existing statutes to ensure that sufficient authorities and safeguards exist for use of the military across the entire spectrum of potential terrorist attacks (including conventional, chemical, biological, radiological, and nuclear threats as well as cyber); that the authorities be consolidated in a single chapter of Title 10; and that DoD prepare a legal "handbook" to ensure that military and civilian authorities better understand the

²¹⁷ These positions are detailed in Pat Towell, "Northern Command Stirs Issue of Military's Role in Security," *Congressional Quarterly Weekly*, 2 November 2002, p. 2867; and Harry Levins, "Loopholes in Law Give Military Ability to Play Role in U.S.," *St. Louis Post-Dispatch*, 21 April 2002.

²¹⁸ See *Second Annual Report*, page 27 and Appendix R. <http://www.rand.org/nsrd/terrapanel/>

²¹⁹ In April 2001 the Department of the Army's Center for Law and Military Operations published an "advisory" guide entitled *Domestic Operational Law Handbook for Judge Advocates*. Although its contents do not represent official DoD legal positions, the Army guide could serve as the basis for an official DoD handbook of the type we recommend. The Army's guide is available at on the internet at <https://www.jagcnet.army.mil/clamo/publications>.

legal authorities governing the use of the military domestically in support of civilian authorities for all hazards—natural and manmade

Identifying Requirements

Northern Command and supporting service and Joint Staff structures have the capability to identify purely military homeland defense requirements for land, maritime, and air combat missions. The problem, however, is that no process is clearly in place to identify among the full scope of participants the requirements for support to civil authorities. It is critical that States, cities, and municipalities define requirements beyond their current capabilities that should be met by Federal augmentation.

Recommendation: That the President direct the DHS to coordinate a comprehensive effort among DoD (including NORTHCOM) and Federal, State, and local authorities to identify the types and levels of Federal support, including military support, that may be required to assist civil authorities in homeland security efforts and to articulate those requirements in the National Incident Response Plan

The DHS should evaluate shortfalls and allocate augmentation responsibilities to other Federal agencies, including DoD. DHS should articulate those responsibilities in the National Incident Response Plan. The Defense Department, supported by NORTHCOM, should give DHS full cooperation in completing this effort.

Enhancing Training

Military personnel in the United States have long adhered to this principle: “train as you fight and fight as you train.” This principle is certainly valid for homeland defense and civil support operations. The panel is reasonably confident that NORTHCOM will develop adequate plans for its homeland defense, military-led mission and that most combat training and exercises for military units will have some application in that mission. Nevertheless, there will be special considerations for conducting military operations inside or over the United States and in adjacent waters—proximity to the civilian population, coordination with other governmental entities, and air or sea traffic issues, as examples—that will need significant attention in training and exercises. Moreover, States and localities should be provided information and definitive guidance on what to expect in the event of future homeland defense, military-led operations.

In addition, the panel is concerned that there is no assurance that specially trained forces will be available to NORTHCOM prior to a crisis, and that current civil support training across the armed forces in general is insufficient.

Although the military trains extensively for combat operations, training for homeland activities differs in essential ways. Compared to coordination within a purely military command structure, coordinating homeland operations with other Federal, State, and local authorities will require comparable skills but different applications. Liaison activities among the elements involved in planning, training, and exercising will take on greater importance. For response operations, command and control processes may be different. Requirements for joint training will take on a new meaning, as joint exercises with State and local responders will be very important. Finally, certain homeland missions will require support to civil law enforcement and the execution of law

enforcement tasks. Military personnel will require specific training to support local law enforcement agencies in performing law enforcement missions.

The *problem* has been that insufficient attention has been paid to and resources made available for civil support training. We now know the pervasiveness of the threat, the increased probabilities of terrorist acts, and the need for enhanced preparation for effective response. Therefore, the Advisory Panel suggests a significant increase in the emphasis on civil support missions for all hazards incidents, with special emphasis on response to acts of terror. Specifically, the Department of Defense should increase the planning, training, and exercising of Active, Guard, and Reserve forces to execute civil support missions.

Recommendation: That the Secretary of Defense direct that all military personnel and units under NORTHCOM, or designated for NORTHCOM use in any contingency, receive special training for domestic missions. Furthermore, in those cases where military personnel support civil law enforcement, special training programs should be established and executed.

Establishing New Capabilities for Military Support to Civil Authorities

As noted above, NORTHCOM's initial force structure will include few permanently assigned forces.²²⁰ The problem with this initial force structure is that it leaves unanswered questions about the scope and level of training and exercising of units and personnel that might be used for civil support missions. It is not clear that Commander NORTHCOM's pre-incident authorities have been aligned with the civil support responsibilities that he has been assigned. Indeed, there are no assurances that civil support training will be conducted unless NORTHCOM is given command of specific units, some other pre-incident authority over units, or specific units commanded by others are designated and trained for civil support missions.

²²⁰ The panel acknowledges that NORTHCOM is not unique with respect to the provision of assigned forces but argues nonetheless that NORTHCOM is unique among commands. For example, like NORTHCOM, U.S. Central Command (CENTCOM), the Unified Command in charge of military operations in an area including the Middle East, Central and Southwest Asia, and Northeast Africa, does not have permanently assigned forces. However, CENTCOM can be assured that forces temporarily assigned will be fully ready for combat missions that might occur in its area of responsibility. This is because military units have been notified that they are part of a CENTCOM operational plan and must train for that mission. NORTHCOM, on the other hand, if it is assigned forces temporarily when an incident occurs, cannot be assured that those forces will have been trained specifically for homeland security missions, especially civil support missions, because no formal contingency plans currently exist that would trigger a requirement for training. Forces provided to NORTHCOM will most likely be trained for warfighting not necessarily for homeland defense or for civil support missions.

Our understanding of the latest plan for NORTHCOM command authorities is that its commander will have a “combatant command”(COCOM)²²¹ relationship with the various service component commands (i.e., ARNORTH, NAVNORTH, NORTHAF, MARFOR NORTH). Its full implications are not yet clear. There is a question about this whether command relationship is only for the purpose of unity of *homeland defense* authority and responsibility or applies more broadly to all *homeland security* missions, including NORTHCOM’s civil support mission. Thus, at this writing, the extent to which the new command will be able to direct new and expanded civil support training and exercises remains unclear.

Recommendation: That the Secretary of Defense clarify NORTHCOM’s combatant command authority to ensure that Commander NORTHCOM can direct subordinate commands to conduct pre-incident planning, training, and exercising of forces required to conduct civil support missions

The Advisory Panel acknowledges that the U.S. military is rightly focused on warfighting. However, the panel believes many of its concerns related to pre-incident planning, training, and exercises could be rectified if NORTHCOM were assigned forces for civil support missions. Indeed, the possibility of a major attack on U.S. soil of a size that would overwhelm even the best-prepared cities and States warrants consideration of dedicating a small number of specialized, “rapid reaction” forces to NORTHCOM for civil support. The advantages of dedicated forces are that they can respond quickly and can be well trained to operate effectively at the scene.

Currently, DoD has several small, specialized units that are prepared to quickly deploy to support civil authorities in dealing with a terrorist attack. (Appendix P lists units and assets identified by the Office of the Secretary of Defense as having a homeland CBRNE response or other civil support mission.) The Department has, for example, units that, under certain circumstances, could respond to ongoing terrorist or hostage situations that exceed the capability of law enforcement agencies. The employment of these units within the United States is reserved for only the most severe circumstances. The National Guard has a dedicated but limited CBRNE response capability for homeland operations: the Weapons of Mass Destruction Civil Support

²²¹ As of August 2002, the Department of Defense had defined combatant command (command authority) as follows: “Nontransferable command authority established by title 10 (“Armed Forces”), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority). Also called COCOM.” *DoD Dictionary of Military and Associated Terms*, Joint Publication 1-02, as amended through 14 August 2002, available at on the internet at <http://www.dtic.mil/doctrine/jel/doddict/index.html>

Teams.²²² Several small active duty response teams have been specially designed to deal with CBRNE events. However, other than the WMDCSTs, those additional existing CBRNE response teams are deployable to theaters abroad.²²³ In addition, existing CBRNE response teams, including the WMDCSTs, are designed to provide a command capability, or specialized capability (e.g., chemical or biological agent decontamination), or technical advice and a communications channel to follow-on forces. They could not by themselves handle medium- or large-size events.

The Army has brigade-size elements (e.g., comprising roughly 3,500 airborne troops²²⁴) standing by for rapid deployment to trouble spots throughout the world. Similar capabilities for rapid deployment exist in the Air Force, Navy, and Marine Corps. Analogous rapid response-type capabilities should arguably be tailored to deal with homeland terrorist events that overwhelm State and local capabilities. Although the Advisory Panel fully understands the principle of forward defense, we believe military organizations should be established, trained, and dedicated to homeland defense *and* civil support missions if the *National Security Strategy of the United States of America* is to be meaningful—that “our military’s highest priority is to defend the United States.” Our belief is premised upon the fact that the territory of the United States is now a battlefield in the war on terrorism.

Recommendation: That the Combatant Commander, NORTHCOM, have dedicated, rapid-reaction units with a wide range of response capabilities such as an ability to support implementation of a quarantine, support crowd control activities, provide CBRNE detection and decontamination, provide emergency medical response, perform engineering, and provide communication support to and among the leadership of civil authorities in the event of a terrorist attack

²²² In the Fiscal Year 2003 Defense Authorization Act, Congress directed the Secretary of Defense to establish WMDCSTs in each of the remaining States and territories; thus, a total of 55 teams have been authorized, with two stationed in California. Each team has 22 personnel. U.S. House, 107th Congress, 2nd Session, Conference Report on H.R. 4546, *Bob Stump National Defense Authorization Act for Fiscal Year 2003*, November 12, 2002, section 1403.

²²³ According to an official in the Office of the Assistant Secretary of Defense for Reserve Affairs (OASD-RA), the WMDCSTs are dedicated to homeland operations in accordance with the Unified Command Plan. In Appendix P, numerous other military units and assets are also described. Most of these have varying levels of commitment to homeland operations and, depending on the level of effort demanded by concurrent incidents, at least some likely could perform missions at home and abroad simultaneously. According to OASD-RA, the Marine Corps’ Chemical Biological Incident Response Force, although deployable abroad, is in fact focused on homeland operations. The CBIRF maintains 90 Marines in a 24-hour readiness posture for immediate response and a follow-on force of 200 more personnel. In addition, OASD-RA says the Army’s Technical Escort Unit and 52nd Ordnance Group are deployable but maintain elements dedicated to supporting U.S. civil agencies (e.g., the FBI). Finally, in the event of a terrorist incident, commanders of military installations within U.S. territory are authorized to provide “immediate response” to requests from civil authorities “to save lives, prevent human suffering, or mitigate great property damage.” Therefore, communities in proximity to U.S. military installations could in most circumstances expect resident military personnel and civilian employees to render general assistance in a crisis; such assistance would be reasonably assured if pre-preplanned in the form of a civil-military mutual aid agreement. On installation commanders’ immediate response authorities, see Kellman, *Managing Terrorism’s Consequences*, chapter 2, p. 13.

²²⁴ Army light infantry, airborne, and air assault brigades typically have between approximately 3,200 and 3,500 soldiers. For details, see Federation of American Scientists, Military Analysis Network, “U.S. Army Table of Organization and Equipment,” available at:

<http://www.fas.org/man/dod-101/army/unit/toe/index.html>.

If NORTHCOM's Combatant Commander establishes the requirement, force "designers" and force providers should consider, in coordination with the States and local organizations, a mix of existing or specifically tailored rapid-reaction forces to meet civil support missions. Once designated, these rapid reaction forces should be under NORTHCOM's operational command. They could include forces (Active, National Guard, and Reserve) representing a full range of joint capabilities, such as military police, command and control, medical, engineering, CBRNE detection/decontamination, and liaison elements.

Improving the National Guard's Role

The National Guard's future role in homeland security activities has moved to the forefront of the debate on military support options. The Guard's history of service within the United States extends to its founding as a colonial militia during the Revolutionary War era. More recently its role in supporting the active force increased continuously during the Cold War and today is manifested in increasing numbers of deployments throughout the world, including long-term commitments in Bosnia and Kosovo.

In preparing to confront terrorists, the United States and its individual States must resolve difficult issues about the role of the States and the Federal government in protecting citizens. The National Guard's potential contribution to combating terrorism is an important dimension of the assessment of appropriate State and Federal roles because the National Guard is "dual missioned": it can serve directly both the State governor and the citizens of the State, as well as the President.

The National Guard Can Operate Under Three Authorities

In the event of a natural or manmade disaster, demand for National Guard support can escalate along a continuum that begins with a governor's call up of Guard personnel in *state active duty* (SAD) status and moves through a call to Federal service. Guard personnel in SAD status are controlled by their governor, typically compensated by their State, and perform their tasks—including assistance to law enforcement—in accordance with State statutes. If a governor believes the Guard is performing missions in support of Federal agencies, he can request moving Guard personnel to U. S. Code Title 32 status, which provides for continued State control but with Federal funding for the mission. National Guard forces in Title 32 duty status can, in accordance with State statutes, support civil law enforcement in operations to deter terrorist activities and prevent attacks.²²⁵ The National Guard can operate in a third status when the President decides it is necessary to assume control of military support activities and activates the Guard in any State for Federal active duty under USC Title 10. Such a move extends to Guard personnel Federal pay and benefits, permits Title 10 officers to command mobilized National Guard forces, and permits the President to order federalized guard units to move between States (or out of the country) as part of any national response effort.

Each of these legal authorities has strengths and weaknesses in relation to homeland security operations. States may have difficulty funding homeland security training and operations of the

²²⁵ As we note in our *Third Report*, "statutes and regulation in certain states . . . prohibit the use of the Guard for law enforcement activities." States can restrict the law enforcement activities of National Guard forces operating in state active duty or Title 32 status. See *Third Report*, p. 52.

Guard in SAD status, especially if their missions are conducted for extended periods. Commanders are not clearly authorized under Title 32 to expend Federal funds for training for civil support tasks.²²⁶ Guard personnel deployed in Title 32 status for national missions (e.g., to assist in border security operations) may therefore have varying levels of training and proficiency in their assigned tasks. Under Title 32, moreover, individual States can establish procedures and rules of engagement for Guard missions, potentially resulting in no comprehensive standards covering the activities of Guard personnel supporting a national mission. Military officers in Title 32 status cannot command Title 10 forces, which limits their ability to direct available Federal resources. Title 10 forces are limited by the Posse Comitatus Act, which restricts their activities and can thus limit their ability to perform critical homeland security tasks.

Recommendation: That the Congress expressly authorize the Secretary of Defense to provide funds to the governor of a State when such funds are requested for civil support planning, training, exercising and operations by National Guard personnel acting in Title 32 duty status and that the Secretary of Defense collaborate with State governors to develop agreed lists of National Guard civil support activities for which the Defense Department will provide funds

As the United States grapples with the role of the National Guard in homeland security missions, a fundamental issue that must be addressed is the degree to which past practices and informal and formal relationships (such as State emergency assistance compacts) will be effective in an environment in which our Nation, our cities, and our communities will potentially become the battlefield. Can effective response to the war on terrorism and major CBRNE incidents within our borders be met within the current structure, practices, and command and control arrangements? What is the appropriate balance between the responsibilities of State governors and Federal authorities? What is the most appropriate and acceptable concept to support unity of effort in local, State, and Federal response to such incidents as well as extremely grave national disasters? And, what is the appropriate relationship between NORTHCOM and the National Guard?

The National Guard's experience in responding to the September 2001 terrorist attacks illustrates some of the challenges associated with its dual State-Federal mission. The magnitude of the attacks compelled an immediate national response. New border and airport security measures were required. The President wanted a coordinated national effort; the National Guard offered organized military forces that could perform these missions.

²²⁶ Several National Guard officers interviewed by the panel's staff expressed the opinion that Title 32 was developed primarily for Guardsmen to train for warfighting missions and that Title 32 does not clearly authorize National Guard military support to civil authorities. The Adjutant General of Washington State, Maj. Gen. Timothy Lowenberg, expressed the view that this lack of clarity acts as a deterrent to commanders who wish to train their Guardsmen for civil support operations. Commanders might face criminal penalties under the 1906 Anti-Deficiency Act (31 USC, Section 1341) if they expend on civil support training funds appropriated by Congress to support training for warfighting missions. Indeed, the Congress had to expressly authorize the Guard's conduct of counterdrug missions while in Title 32 duty status to assure commanders that such missions would not risk a violation of the Anti-Deficiency Act. To review the legislation on National Guard counterdrug activities, see U.S. House of Representatives, Committee on Armed Services, 104th Congress, 2nd Session, *National Defense Authorization Act for Fiscal Year 1996*, House Conference Report, H. Rpt. 104-450, available at <ftp://ftp.loc.gov/pub/thomas/cp104/hr450.txt>.

For airport security augmentation, the President requested that governors stand up the Guard in the several States to perform the mission. The President could have mobilized the Guard for this national mission under his Title 10 authorities. Instead, he called them to duty under Title 32. Maintaining the Guard in this status allowed State units to deploy to airports within roughly one week of the order. States maintained control of their Guard resources and had greater flexibility to meet airport and other security requirements. The governors also had greater flexibility to rotate Guard personnel in and out of duty status to deal with family, business, or employment issues. Governors and Guard commanders had greater flexibility in tailoring missions, drawing from multiple units within a State rather than having total units activated under Title 10, thus placing all personnel in such units on full time duty status. Importantly, the 9,100 National Guard personnel manning airports performed their duties in accordance with State laws, policies, and rules of engagement. This led to significant variation in the Guards' activities in airports across the Nation.²²⁷ Indeed, the varied approach among the States suggests that other processes may be required and surely would be more effective.

Deploying the Guard for border security operations posed different challenges. In this case, President Bush approved 1,600 National Guard for duty in Title 10 status. The governors initially opposed the President's decision to federalize the Guard,²²⁸ but it was decided that the border security operation was a Federal not a State mission and the Guard had no law enforcement duties to perform. Even so, the Posse Comitatus Act undermined the Guard's utility as a Title 10 force in this mission. The Defense Department determined that Guard personnel carrying weapons within U.S. territory could only use them in self defense.²²⁹ Most personnel went unarmed and carried out their tasks under the protection of armed Customs and INS agents. Finally, in a complex intergovernmental and Federal interagency policy and decisionmaking process involving the States, the Defense Department, INS, Customs, and the Border Patrol, it took approximately six months to complete deployment of Title 10 Guard personnel for border security.²³⁰

The examples cited with the Federal, State, and city response to the September 11 terrorist operations in New York and at the Pentagon suggest the challenges all entities had in responding effectively to both the incidents as well as the pending threats. Since then, we have all learned of the pervasive and growing threat we face and, as the President states, the long-term nature of the war on terrorism. The *problem* we face is to determine the optimum way to employ all assets to protect the people of the United States and to respond effectively, efficiently, and decisively for consequence management in those cases when deterrence fails. Should the United States establish more formal association among the States so that the National Guard, and other committed assets, can be optimally trained, exercised, and sustained to meet future disasters in a national effort, covering multi-State regions, but where National Guard assets remain under the control of State governors? As noted earlier, Guard units and personnel deployed in Title 32 status under the control of State governors offer great advantage to the Nation and to the Guard and its individual personnel.

²²⁷ George Cahlink, "Identity Crisis: The National Guard Is Torn Between Two Missions," *Government Executive*, September 2002.

²²⁸ The governors' concerns are cited in, Adjutants General Association of the United States, Letter to the Governors and Legislators of the Several States, Territories and the District of Columbia and to the Congress and the President of the United States, February 25, 2002, p. 4.

²²⁹ Cahlink, "Identity Crisis."

²³⁰ Cahlink, "Identity Crisis."

We believe that an enhanced Federal-State partnership is required to support the National Guard operating in the homeland and assisting civil authorities. Experience indicates that State and Federal leaders must have options for Federal-State arrangements beyond those currently permitted in Title 32 and Title 10. Any new arrangement should permit federally-funded, multi-State activities by Title 32 Guard personnel operating under the control of State governors and with agreed Federal-State coordination mechanisms. In developing an enhanced partnership, a key objective must be to ensure that National Guard units can effectively respond to incidents of *national* significance and do so under *State* control, thus reducing the likelihood that such units will be federalized under Title 10, with all the associated disruptions and complexities such an action entails.

Key Objective = Maximum Flexibility

Develop ways to be able to utilize the National Guard to execute “national” missions requested by the President, but operating under a Governor’s control, funded with Federal funds, with an “opt out” at the State’s discretion. Then train and exercise National Guard units to the same standard so they can be utilized anywhere and with units from other States.

A Federal-State arrangement meeting these general requirements could be developed based on new Title 32 authorities and by building on the concept of existing multi-State assistance compacts that employ Guard resources. In this regard, the President should establish with the governors of the several States a process by which the States will deploy National Guard forces in Title 32 status to support national missions. This arrangement should include mechanisms for collaborative mission planning and execution in accordance with agreed-on standards. Such an arrangement will ensure an efficient deployment process and increased uniformity of operations by Title 32 Guard personnel.

Many States have participated in a long-standing mutual aid agreement: the Interstate Civil Defense and Disaster Compact.²³¹ In addition, forty-eight States and two territories have joined a congressionally-approved Emergency Management Assistance Compact (EMAC)²³² and other arrangements that permit them to provide State National Guard assets to neighboring States to deal with an emergency. However, existing compacts typically have certain limitations, which are important in the homeland security context. These compacts are designed primarily for responding to more localized events (e.g., natural disasters), as opposed to national, all-hazards incidents. States are responsible for providing funds to train their National Guard in civil support tasks. The compacts can require the State requesting assistance to fund any National Guard response effort and they do not uniformly ensure that units from outside States will have specialized or equivalent training. Finally, Guard units deployed outside their States under the

²³¹ For more information on interstate assistance agreements, see our *Third Report*, Appendix I.

²³² The EMAC is codified in Federal law. Participating States and territories duplicate the Federal law in their own implementing legislation. To review the public law, see U.S. House, 104th Congress, 2nd Session, Public Law 104-321, *Granting the Consent of Congress to the Emergency Management Assistance Compact*, available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ321.104.pdf.

terms of the EMAC are not permitted to engage in law enforcement tasks²³³ and require additional State or Federal authorization to use military force for any activity that is prohibited by the Federal Posse Comitatus Act (details on the legal restrictions cited here are provided in this footnote).²³⁴

Given the long-term threat environment, the States' existing National Guard military support arrangements must be enhanced to provide for more effective response capabilities in Title 32 duty status. A new construct must also include an improved Federal-State interface for military operations. To achieve these objectives a *regionally* organized system for providing National Guard military assistance to civil authorities should be developed. Such a system could be aligned with the 10 FEMA regions. If this were done, all assets within such regions could train, exercise, and coordinate response activities under the regional system's auspices, more broadly under NORTHCOM's leadership, or under both. A memorandum of understanding (MOU) providing key details on an improved National Guard response system could be developed by Federal and State participants. Through the MOU (or some other instrument) the governors in each region could, for instance, delegate operational control of their Guard forces—or any other agreed level of control—to a regional Guard commander, or the Adjutant General of the affected State, for crisis response activities.²³⁵

A regionally organized National Guard response system would, like most existing emergency assistance compacts, be voluntary. The arrangement would be a “coalition of the willing”: the system's founding MOU could stipulate that any governor may forgo participation in an individual response operation.

The States would have numerous incentives to participate in a regionally organized system for National Guard military support. Increased Federal funding could be committed for a previously agreed-on list of civil support missions and for regionally-organized training and exercises. The efficient and effective delivery of Guard resources during an emergency could enable States to manage even large-scale incidents while maintaining control of their Guard personnel. Finally, to bring specialized or additional military resources to bear, coordination arrangements could be established between DoD and the leadership of the National Guard's regional response system. These arrangements would also establish mechanisms for coordinated Federal-State-local

²³³ This is the opinion of John G. Hathaway, Acting Deputy Assistant Secretary of Defense for Military Assistance to Civil Authorities. John G. Hathaway, email communication to Panelist William Reno, November 18, 2002.

²³⁴ In accordance with the EMAC legislation, National Guard units may use military force outside their State if they have “express statutory authorization” (e.g., during any incident in which the governor of the State requesting aid has declared martial law or one in which the President exercises his authorities under the insurrection statutes). In the Public Law providing congressional consent to the EMAC arrangement, the restrictive article reads as follows: “Nothing in this compact shall authorize or permit the use of military force by the National Guard of a state at any place outside that state in any emergency for which the President is authorized by law to call into federal service the militia, or for any purpose for which the use of the Army or the Air Force would in the absence of express statutory authorization be prohibited under §1385 of Title 18 of the United States Code.” See U.S. House, 104th Congress, 2nd Session, Public Law 104-321, Article XIII.

²³⁵ A Federal-State arrangement exhibiting many of the characteristics recommended here has already been established for bringing military resources to bear for fire-fighting. Under this arrangement, 13 States have signed an MOU with the Secretary of the Air Force to provide for a mixed force of Title 10 and Title 32 assets in support of State fire-fighting operations. Brig Gen John E. Iffland, Commander, 146th Airlift Wing, Air National Guard, presentation to a panel member and staff, 14 November 2002, at the RAND Corporation, Arlington, Virginia.

planning, training, exercises, and operations activities by participating organizations, including such other Federal entities as the Federal Emergency Management Agency.

Recommendations: That the President and governors of the several States establish a collaborative process for deploying National Guard forces in Title 32 duty status to support missions of national significance at the President’s request

That the Congress provide new authority under Title 32 to employ the National Guard (in non-Title 10 status) on a multi-State basis, and with governors’ consent to conduct homeland security missions, and that the Secretary of Defense define clearly the appropriate command relationships between DoD and the National Guard

That Congress and DoD promote and support the development of a system for National Guard civil support activities that can deploy forces regionally--in coordination with DoD--to respond to incidents that overwhelm the resources of an individual State

In our *Third Report*, we recommended the following:

“--That the Secretary of Defense direct specific mission areas for the use of the National Guard for providing support to civil authorities for combating terrorism. Further, we recommend that the Secretary:

“-- In coordination with State governors, assess National Guard force structure, define appropriate roles and missions, and establish units with specific capabilities for homeland security missions.

“-- Increase the percentage of full-time personnel in Guard units designated for homeland security missions and ensure that pay and benefits parallel those of active-duty service members.

“-- Direct which National Guard units will be assigned homeland security missions as their primary missions with combat missions outside the United States as secondary missions and provide resources consistent with the designated priority of their homeland missions.

“-- Direct that National Guard units with priority homeland security missions plan, train, and exercise with State and local agencies.”

To the extent that we have not done so explicitly in this chapter, we reaffirm those recommendations but with one exception. We believe that, given the lessons learned during and after September 2001 and considering all the current circumstances and requirements, further enhancement of the National Guard’s civil support capability and responsibility is necessary. We therefore expand our recommendation on roles and missions of the National Guard contained in the third “bullet” above as follows:

Recommendation: That the Secretary of Defense direct that certain National Guard units be trained for and assigned homeland security missions as their *exclusive* missions (rather than primary missions as stated in our *Third Report*) and provide resources consistent with the designated priority of their homeland missions

Some people may suggest that organizing National Guard units with “exclusive” homeland security missions could mean that those units will be moved under the Department of Homeland Security. We disagree. Such a move is not only unlikely, it would not be prudent or consistent with the Constitutional underpinnings or historical precedents for use of the military generally and for the National Guard specifically. We have recommended a structure for using the Guard for “national” missions in a Title 32 status and for establishing certain Guard units with exclusive homeland missions—mutual goals. Nevertheless, the President could find it necessary, because of the magnitude of an attack or other circumstances, to bring National Guard units into a Title 10 status to serve with other Title 10 active and reserve forces under Federal command. For such a contingency, all National Guard forces, including those with exclusive homeland security missions, will need to continue to be trained and equipped through the Department of Defense.

Moreover, the governors of the several States should be consulted on the best possible structure and method to implement all of these recommendations that pertain to the National Guard.

TABLE OF APPENDICES

Appendix A—Enabling Legislation.....	A-1
Appendix B—Panel Chair and Members.....	B-1
Appendix C—Persons Interviewed.....	C-1
Appendix D—Survey Information and Analysis.....	D-1
Tab 1—The Survey Instrument.....	D-1-1
Tab 2—Sample Fire Services Survey.....	D-2-1
Tab 3—Fielding Procedures.....	D-3-1
Tab 4—Sample Design and Respondent Selection.....	D-4-1
Tab 5—Response Rates.....	D-5-1
Tab 6—Constructing the Survey Weights.....	D-6-1
Tab 7—Survey Comments.....	D-7-1
Appendix E—The Terrorist Threat to U.S. Agriculture.....	E-1
Appendix F—The Psychological Impact of U.S. Terrorism.....	F-1
Appendix G—United States Animal Health Association-USAHA 2001 Resolution No. 10.....	G-1
Appendix H—Defining a Public Communications Strategy for Counterterrorism.....	H-1
Appendix I—Programs of the Federal Emergency Management Agency and the Department of Justice.....	I-1
Appendix J—U.S. Department of Health and Human Services Initiatives to Support State and Local Terrorism Preparedness Programs.....	J-1
Tab 1—Interview Guide for DHHS Review.....	J-1-1
Tab 2—References.....	J-2-1
Appendix K—Medical and Public Health Workforce Preparedness.....	K-1
Appendix L—Protecting Critical Infrastructure Against Terrorist Attacks.....	L-1
Appendix M—Critical Infrastructure Information.....	M-1
Appendix N—Statement of Senator Robert Bennett on Critical Infrastructure Information.....	N-1
Appendix O—Status of Federal Budget Requests for Assistance to States and Localities.....	O-1
Appendix P—Department of Defense CBRNE Assets.....	P-1
Appendix Q—NORTHCOM Command Relationships.....	Q-1
Appendix R—List of Abbreviations.....	R-1
Appendix S—Panel Activities – Calendar Year 2002.....	S-1
Appendix T—RAND Staff Providing Support to the Advisory Panel.....	T-1

APPENDICES

APPENDIX A--ENABLING LEGISLATION

Following is an extract of the legislation, sponsored by Representative Curt Weldon of Pennsylvania, which created the Advisory Panel and provided its mandate.

An Extract of Public Law 105-261 (105th Congress, 2nd Session) (October 17, 1998)

SEC. 1405. ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION.

- a. **REQUIREMENT FOR PANEL-** The Secretary of Defense, in consultation with the Attorney General, the Secretary of Energy, the Secretary of Health and Human Services, and the Director of the Federal Emergency Management Agency, shall enter into a contract with a federally funded research and development center to establish a panel to assess the capabilities for domestic response to terrorism involving weapons of mass destruction.
- b. **COMPOSITION OF PANEL; SELECTION-** (1) The panel shall be composed of members who shall be private citizens of the United States with knowledge and expertise in emergency response matters. (2) Members of the panel shall be selected by the federally funded research and development center in accordance with the terms of the contract established pursuant to subsection (a).
- c. **PROCEDURES FOR PANEL-** The federally funded research and development center shall be responsible for establishing appropriate procedures for the panel, including procedures for selection of a panel chairman.
- d. **DUTIES OF PANEL-** The panel shall--
 1. assess Federal agency efforts to enhance domestic preparedness for incidents involving weapons of mass destruction;
 2. assess the progress of Federal training programs for local emergency responses to incidents involving weapons of mass destruction;
 3. assess deficiencies in programs for response to incidents involving weapons of mass destruction, including a review of unfunded communications, equipment, and planning requirements, and the needs of maritime regions;
 4. recommend strategies for ensuring effective coordination with respect to Federal agency weapons of mass destruction response efforts, and for ensuring fully effective local response capabilities for weapons of mass destruction incidents; and
 5. assess the appropriate roles of State and local government in funding effective local response capabilities.
- e. **DEADLINE TO ENTER INTO CONTRACT-** The Secretary of Defense shall enter into the contract required under subsection (a) not later than 60 days after the date of the enactment of this Act.
- f. **DEADLINE FOR SELECTION OF PANEL MEMBERS-** Selection of panel members shall be made not later than 30 days after the date on which the Secretary enters into the contract required by subsection (a).
- g. **INITIAL MEETING OF THE PANEL-** The panel shall conduct its first meeting not later than 30 days after the date that all the selections to the panel have been made.
- h. **REPORTS-** (1) Not later than 6 months after the date of the first meeting of the panel, the panel shall submit to the President and to Congress an initial report setting forth its findings, conclusions, and recommendations for improving Federal, State, and local domestic emergency preparedness to respond to incidents involving weapons of mass destruction. (2) Not later than December 15 of each year, beginning in 1999 and ending in 2001, the panel shall submit to the President and to the Congress a report setting forth its findings, conclusions, and recommendations for improving Federal, State, and local domestic emergency preparedness to respond to incidents involving weapons of mass destruction.
- i. **COOPERATION OF OTHER AGENCIES-** (1) The panel may secure directly from the Department of Defense, the Department of Energy, the Department of Health and Human Services, the Department of Justice, and the Federal Emergency Management Agency, or any other Federal department or agency information that the panel considers necessary for the panel to carry out its duties. (2) The Attorney General, the Secretary of Defense, the Secretary of Energy, the Secretary of Health and Human Services, the Director of the Federal Emergency Management Agency, and any other official of the United States shall provide the panel with full and timely cooperation in carrying out its duties under this section.

An Extract of Public Law 107-107, December 28, 2001 (107th Congress, 1st Session)

SEC. 1514. TWO-YEAR EXTENSION OF ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION.

(a) EXTENSION OF ADVISORY PANEL.—Section 1405 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (50 U.S.C. 2301 note) is amended—

- (1) in subsection (h)(2), by striking “2001” and inserting “2003”; and
- (2) in subsection (l), by striking “three years” and inserting “five years”.

APPENDIX B--PANEL CHAIR AND MEMBERS

NAME AND AFFILIATION	EXPERTISE
James S. Gilmore, III, Attorney at Law, and former Governor of the Commonwealth of Virginia, Chair	State government
L. Paul Bremer, Corporate Executive, and Former Ambassador-at-Large for Counter-Terrorism, U.S. Department of State	Terrorism, counter-terrorism
George Foresman, Deputy Director, Office of Commonwealth Preparedness, Commonwealth of Virginia	Emergency response—State
Michael Freeman, Chief, Los Angeles County Fire Department	Emergency response—local
William Garrison (Major General, U.S. Army, Retired), Corporate Executive, and Former Commander, U.S. Army Special Operations Command's Delta Force	Military special operations
Ellen M. Gordon, Administrator, Emergency Management Division, Department of Public Defense, State of Iowa, and Past President, National Emergency Management Association	Emergency response—State
James Greenleaf, Independent Consultant, and Former Associate Deputy for Administration, Federal Bureau of Investigation	Law enforcement—Federal
William Jenaway, Independent Consultant, and Chief of Fire and Rescue Services, King of Prussia, Pennsylvania	Emergency response—local
William Dallas Jones, Director, Office of Emergency Services, State of California	Emergency response—State
Paul M. Maniscalco, Past President, National Association of Emergency Medical Technicians, and Deputy Chief/Paramedic, City of New York Fire Department, EMSC	Emergency response—local
John O. Marsh, Jr., Attorney at Law, former Secretary of the Army, and former Member of Congress	Government structure, interagency coordination, cyber, and legal
Kathleen O'Brien, University Executive, and former City Coordinator, City of Minneapolis, Minnesota	Municipal government
M. Patricia Quinlisk, M.D., Medical Director/State Epidemiologist, Department of Public Health, State of Iowa	Health—State
Patrick Ralston, Executive Director, Indiana State Emergency Management Agency; Executive Director, Department of Fire and Building Services; and Executive Director, Public Safety Training Institute, State of Indiana	Emergency response—State
William Reno (Lieutenant General, U.S. Army, Retired), Corporate Executive, former Senior Vice President of Operations, American Red Cross	Non-governmental organizations

Joseph Samuels, Jr., Chief of Police, Richmond, California, and President, International Association of Chief of Police	Law enforcement—local, terrorism preparedness
Kenneth Shine, M.D., Policy Analyst, and former President, Institute of Medicine, National Academy of Sciences	Health—Federal
Alan D. Vickery, Deputy Chief, Special Operations, Seattle Fire Department	Emergency response—local
Hubert Williams, President, The Police Foundation	Law enforcement/civil liberties

NON-VOTING PARTICIPANTS

John Hathaway, U.S. Department of Defense Representative

Michael A. Wermuth, Senior Policy Analyst, RAND, Executive Project Director

Jennifer Brower, Senior Policy Analyst, RAND, Co-Project Director

FORMER MEMBERS

The Honorable Donald Rumsfeld, Secretary of Defense

James R. Clapper, Jr. (Lieutenant General, U.S. Air Force, Retired), Director, National Imagery and Mapping Administration; former Director, Defense Intelligence Agency, and former panel Vice Chair

James Q. Wilson, Ph.D., former Harvard and UCLA professor; Member, board of trustees, American Enterprise Institute; former member, President's Foreign Intelligence Advisory Board

Richard Falkenrath, Office of Homeland Security; former Associate Professor, John F. Kennedy School of Government, Harvard University

Ronald S. Neubauer, Chief of Police, St. Peters, Missouri, and Past President, International Association of Chiefs of Police

Raymond Downey, Deputy Chief, and Commander, Special Operations, Fire Department of the City of New York

John Gannon, Executive Office of the President, former Deputy Director of Central Intelligence, and former Chairman, National Intelligence Council

APPENDIX C--PERSONS INTERVIEWED

An “interview,” for the purpose of this list, includes a formal presentation to members of the Advisory Panel, a formal interview by a panel member or support staff, the written submission or exchange of information, or discussions about the issues addressed in this report with a panel member or support staff.

Lawrence Adams Critical Incident Analysis Group University of Virginia	U.S. House of Representatives
Patrick Alguire, M.D. American Society of Internal Medicine	Jarrett Clinton U.S. Department of Health and Human Resources
Graham Allison, Ph.D. Harvard University	Deborah Colantonio General Accounting Office
Larry Ankrom Federal Bureau of Investigation	Christina Crayton National Association of Counties
Joselyn Baker Office of the Governor of Georgia	Dean D'Amore Office of Representative Sherwood Boehlert
Lonice Barrett Georgia Department of Natural Resources	John Daugirda U.S. Northern Command
Ann Beauchesne National Governors Association	Charles Dawson Georgia Emergency Management Agency
Scott Becker Association of Public Health Laboratories	Raymond Decker General Accounting Office
Paul Blake Georgia Department of Human Resources	Scott Deitchman, M.D. American Medical Association
Eugene Bowman, J.D., LL.M. Federal Bureau of Investigation	Rebecca Denlinger Cobb County Fire Department Georgia
Sam Brinkley Department of State	Cherie Drenzek Georgia Department of Human Resources
Stephen L. Caldwell General Accounting Office	Edward Edens Committee on Armed Services United States Senate
Barry Cardwell U.S. Northern Command	William W. Ellis Congressional Research Service
Joni Charme Captain, U.S. Army Joint Task Force-Civil Support	Charley English Georgia Emergency Management Agency
Frank Cilluffo Executive Office of the President	Thomas W. Eres (Maj. Gen., USAF) California National Guard
Tim Clancy Committee on Science	John Erickson Washington State Department of Health

Alan Essig
Office of the Governor of Georgia

Paul Fay
FEMA Region IV

Jack Fenimore
Major General, U.S. Army (Ret.)

Jose Fernandez
Georgia Department of Defense

Michael Fowler
Georgia Department of Defense

Stephen Flynn, Ph.D.
Council on Foreign Relations

John Frank
InterAgency Board for Equipment
Standardization and Interoperability

Richard Friedman, J.D.
National Strategy Forum

Archie Galloway
Office of Senator Jeff Sessions

Kristine Gebbie, RN, DrPH
Columbia University School of Nursing

Vicky Gilner
Georgia Department of Public Safety

Lawrence Gostin, J.D., LL.D (Hon.)
Georgetown University

Buddy Gratton
Georgia Department of Transportation

Everett Gregory
Headquarters, First U.S. Army

Don Hamilton
Memorial Institute for the Prevention of
Terrorism

David Hamon
Defense Threat Reduction Agency

John Hamre
Center for Strategic and International Studies

Francis Hartmann
Harvard University

Seth Hassett
Substance Abuse Mental Health Services
Administration

Jerome Hauer
U.S. Department of Health and Human Services

Jeff Haverty
Federal Bureau of Investigation

Gary Hlady
Georgia Department of Human Resources

Krister Holladay
Office of Representative Saxbe Chambliss

Arnold Howitt, Ph.D.
Harvard University

Holly Idelson
Office of Senator Joseph Lieberman

Mark Jackson
Georgia Bureau of Investigation

Jay Jakub
House Permanent Select Committee on
Intelligence
U.S. House of Representatives

Bruce Jeffries
Georgia Department of Human Resources

Thea Jones, DVM
American Veterinary Medical Association

Dan Kaniewski
House Republican Conference

Donald Kauerauff
Illinois Department of Public Health

Vernon Keenan
Georgia Bureau of Investigation

Juliette Kayyem, J.D.
Harvard University

Timothy Lampe
Defense Threat Reduction Agency

Susan Lance-Parker
Georgia Department of Human Resources

John Landry
National Intelligence Council

Bert Langley
Georgia Department of Natural Resources

Peter LaPorte
Emergency Management Agency
District of Columbia

Scott Layne, M.D.
University of California at Los Angeles

Marcelle Layton, M.D.
New York City Department of Health

Scott Lillibridge, M.D.
Centers for Disease Control and Prevention
Department of Health and Human Services

Harold Linnenkohl
Georgia Department of Transportation

Mickey Lloyd
Georgia Department of Public Safety

Timothy Lowenberg
Adjutant General
State of Washington

Barbara Martinez
Federal Bureau of Investigation

Gene Matthews, J.D.
Centers for Disease Control and Prevention
Department of Health and Human Services

Gary McConnell
Georgia Emergency Management Agency

M. Allen McCullough
Fayette County, Georgia

Alan McCurry
Office of Senator Pat Roberts

Stanley M. McKinney
Office of Domestic Preparedness
U.S. Department of Justice

Howard Mead
Office of the Governor of Georgia

Andy Mitchell
Office of Domestic Preparedness
U.S. Department of Justice

Paul Monroe, Jr.
Major General
California National Guard

Darrell Morgeson
Executive Office of the President

Stephen Morse
Columbia University

Kenneth Mortisugu, M.D.
Deputy United States Surgeon General

Karl Musgrave, DVM, MPH
Wyoming Department of Health

Timothy Nank
Executive Office of the President

Marion Nelson
Georgia Department of Natural Resources

Terry Nesbitt
Georgia Department of Defense

Robert Newberry
Office of the Secretary of Defense

Robert Newman
National Guard Bureau

Gary Noesner
Federal Bureau of Investigation

Terry Norris
Georgia Police Academy

Phillip Oates
Major General
Alaska National Guard

Frank Ochberg, MD
Michigan State University,
and Dart Foundation

James P. O'Neal
Georgia Department of Human Resources

R. Nicholas Palarino,
Subcommittee on National Security
Veterans Affairs, and International
Relations
U.S. House of Representatives

Matthew Payne
U.S. Department of Health and Human Services

Kathryn Peppe
Association of State and Territorial Health
Officials

Raphael F. Perl
Congressional Research Service

Dennis Perotta
Texas Department of Health

Ann Petersen, J.D.

Cheryl Peterson
American Nurses Association

Hugh Peterson
Office of the Governor of Georgia

William Pollack
Department of Energy

David Poythress
Georgia Department of Defense

Charles Ramsey
Metropolitan Police Department
Washington, DC

Dennis Reimer
National Memorial Institute
for the Prevention of Terrorism

James Rice
Office of the Secretary of the Army

John Roland
New York City Police Department

Deborah Rosenblum
Office of the Secretary of Defense

Mitchel Rothholz
American Pharmaceutical Association

Gregory Saathof, MD
University of Virginia

Robert Salesses
Office of the Secretary of Defense

The Honorable Jeff Sessions
United States Senate

Brendan Shields
House Republican Conference

Donald Starry
Georgia Police Academy

C.H. Straub II
Office for State and Local Domestic
Preparedness Support
Department of Justice

Kenneth J. Stillely
California National Guard

David Studstill
Georgia Department of Transportation

John Sullivan
Los Angeles Sheriff's Department

Patrick J. Sullivan
Arapahoe County (CO) Sheriff's Department

Ricki L. Sullivan
Department of the Army

Janice Taylor
Washington State Department of Health

James P. Tierney
National Guard Association of the United States

Walter Tong
Georgia Technical Authority

Kathleen Toomey, MD, MPH
Georgia Department of Human Resources

David Trachtenberg
Committee on Armed Service
U.S. House of Representatives

John Tritak
U.S. Department of Commerce

Stanley Tuggle
Georgia Homeland Security Task Force

Owen Ulmer
Georgia Department of Defense

Michelle Van Cleave
Office of the Secretary of Defense

Michael Vatis
Institute for Security Technology Studies
Dartmouth College

Peter Verga
Office of the Secretary of Defense

David M. Wall
City of Morrow, Georgia

Jeremiah Walsh
Office of the Secretary of Defense

Jon Watson
Federal Bureau of Investigation

Michelle E. White
Federal Emergency Management Agency

James Woolsey
Attorney at Law

Frank Young
Georgia Department of Public Service

Lee Zeichner
LegalNetWorks

The Honorable James Ziglar
Commissioner
Immigration and Naturalization Service

APPENDIX D—SURVEY ANALYSIS AND INFORMATION

2002 SURVEY OF STATE AND LOCAL RESPONSE ORGANIZATIONS: WHAT HAS CHANGED SINCE 9/11 IN TERMS OF PLANNING FOR RESPONSE TO WMD INCIDENTS?

Introduction

Just prior to the 9/11 terrorist attacks, RAND undertook on behalf of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (WMD) (also known as the Gilmore Commission) a nationwide survey of state and local response organizations likely to be involved in the initial stages of the detection and response in the event of a domestic incident involving weapons of mass destruction (WMD). The specific focus was “to elicit state and local response agencies’ assessments of Federal programs intended to improve state and local preparation and readiness to respond to a WMD terrorism incident.” Given when the survey was conducted, it provided us with a good baseline of where state and local organizations stood in addressing planning for emergency response to WMD incidents prior to 9/11.

In 2002, we undertook a second, follow-up survey to the respondents of the initial survey to assess what has changed since 9/11 in terms of threat experience, planning activities, joint preparedness activities, and training of these organizations. In addition, we were interested in learning how organizations were resourcing these new activities. This appendix presents a summary of the results from the first and second *Surveys of Federal Weapons of Mass Destruction (WMD) Preparedness Programs (FWMDPPS I and II)*.²³⁶

The second survey instrument contained two sections: (1) Organizational Experience and Perceptions (included questions about threat experience since 9/11), and (2) Emergency Response Planning Activities (included questions about planning, joint preparedness activities, training, and resourcing). To ensure comparability between the first and second surveys (Waves I and II), we kept the questions as similar as possible between the two survey instruments and, in addition, added some new questions in Wave II.

The second survey was completed by those organizations that responded to the initial survey, which was constructed by first randomly selecting 200 counties throughout the United States and then one of each type of local responder organization (law enforcement, fire--paid, volunteer, and combination--departments; emergency medical service, EMS agencies; public health, hospital, and Offices of Emergency Management, OEMs) was randomly chosen within each county. All the relevant state-level organizations (public health, OEMs, EMS) were surveyed, including those in Washington, DC. In addition, regional EMS entities were surveyed that contained one or more of the 200 counties in the sample.²³⁷

Table 1 shows the current status of the first and second surveys. For the first survey (Wave I), our overall response rate was 65 percent, with some performing considerably better (e.g., state public health) and some not performing as well (e.g., local/regional EMS). In each case, however, the response rates were exceptional when compared to rates in other survey efforts. For the second survey (Wave II), we followed up with organizations that had responded in Wave I, achieving an overall response rate of

²³⁶ This summary is derived from a forthcoming RAND report by Lois M. Davis, et al. The full text of the survey results will be available at in the early Spring of 2003 at <http://www.rand.org>.

²³⁷ In addition to the random sample of counties, 10 counties were also handpicked for inclusion based on past WMD terrorist incidents or upcoming events that might have heightened their sensitivity to WMD terrorism (e.g., the Olympics). The most prominent of each type of response organization within each of these counties was then also surveyed.

69 percent, with response rates of 60 percent or better across the different types of organizations. Unless otherwise indicated, results have been statistically adjusted to represent the entire population in that discipline (e.g., law enforcement).²³⁸ Table 2 provides the margins of error for the second survey percentages presented in this chapter. The margin of error for local organizations ranged between 8 – 11 percent; for state organizations between 6 – 10 percent. Margins of error are useful for judging the likely range of the true value: The actual value for the entire population is highly likely to lie within the observed survey percentage plus or minus the margin of error.²³⁹

In this summary, we organize the findings below around three research questions: (1) what has been the experience of state organizations and local responders with terrorist incidents (or hoaxes) since 9/11? (2) what has changed since 9/11 in terms of planning, joint preparedness, and training? and (3) how are organizations resourcing these additional activities?

Table 1. Current Status of the Surveys and Response Rates for Waves I and II

Response Organizations	WAVE I (2001)		WAVE II (2002)	
	Number of Organizations Surveyed	Response Rate	Number of Organizations Surveyed	Response Rate
Local Organizations				
Public Health	199	74%	149	67%
Law Enforcement	208	71%	148	70%
OEM	202	71%	145	73%
Fire Department*	443	68%	300	69%
Hospital	208	51%	114	67%
Local/Regional EMS	230	48%	124	66%
State Organizations				
OEM	51	78%	40	85%
EMS	51	63%	41	61%
Public Health	51	80%	42	60%
TOTAL/OVERALL RATE	1,643	65%	1,096	69%

*Includes paid, combination, and volunteer fire service organizations.

**Wave I response rate includes completed surveys returned prior to September 11, 2001. Adjustments were made to the total number surveyed in Wave II to include the 29 organizations that returned their Wave I survey just after September 11, 2001.

²³⁸The exception is local/regional EMS organizations. These organizations represent a convenience sample and so the results are unweighted: Findings pertain to the sample only and are not generalizable to the entire population of EMS organizations.

²³⁹ Also note that, even though all State-level organizations were surveyed—a census rather than a sample—calculation of the margin of error is still relevant, since not all State-level organizations replied to the survey.

Table 2. Survey Margins of Error Rounded to the Nearest Percent

	Organization	Margin of Error (Percent)
Local	Public Health	8
	Law Enforcement	8
	OEM	8
	Fire Departments	
	Paid only	11
	Combination only	9
	Volunteer only	10
	Hospitals	9
	Local/Regional EMS*	---
State	OEM	7
	EMS	10
	Public Health	6

*Since convenience sampling was used to select Local/Regional EMS organizations, no margin of error can be calculated.

What Has Been the Experience of State Organizations and Local Responders with Terrorist Incidents since 9/11?

As shown in Table 3, more organizations have experienced terrorist incidents and/or hoaxes in the one-year following 9/11 than in the previous five years. Local first responders experienced an increase since 9/11, with, for example, an additional 10 percent of paid/combination fire departments indicating this to be the case. Volunteer fire departments were the exception; however, the decline was not statistically significant.

Local health organizations experienced a more dramatic increase in terrorist incidents and/or hoaxes following 9/11, moving from less than 20 percent of health organizations in the five years prior to 9/11 to approximately 50 percent and 33 percent, respectively, for local public health departments and hospitals after 9/11. State OEM and EMS also saw an increase after 9/11 in the percentage of organizations that reported incidents of terrorism and/or hoaxes within their state or jurisdiction, although rates were high to begin with.²⁴⁰

²⁴⁰State public health departments were not asked this question.

Table 3. Percentage of Organizations That Experienced Terrorist Incident/Hoaxes Within the Past Five Years Before 9/11 and Following 9/11

Organizations	Percent of Organizations	
	Within Past 5 Years	Since 9/11
Local First Responders		
Law Enforcement	19%	34%
Fire (paid and combo)	40%	51%
Volunteer Fire	20%	6%
Local/Regional EMS	37%	48%
Local OEM	33%	42%
Local Health		
Public Health	15%	50%
Hospitals	13%	33%
State		
OEM	55%	64%
OES	44%	52%

The type of incidents involved changed over time, with conventional explosives incidents predominant prior to 9/11 and then chemical, biological, or radiological (CBR) incidents predominating following 9/11. This is true for local first responders and even more so for local health organizations. However, for state organizations CBR incidents/hoaxes were fairly common even before 9/11.

Not surprisingly, most of the CBR incidents/hoaxes were anthrax-related, as reported by all state and local organizations, except for volunteer fire departments, where two-thirds reported the incidents were chemical-related and only a third indicated they were anthrax-related. This finding may represent the fact that volunteer fire departments tend to be in smaller communities, whereas paid/combination fire departments tend to be in larger cities where one might expect more incidents/hoaxes to have occurred.

What Has Changed Since 9/11 in Terms of Planning, Joint Preparedness, and Training?

Planning

In the planning area, since 9/11, local first responders--particularly paid/combination fire departments and law enforcement agencies--have been more involved in interagency task forces that specifically address planning for WMD-related incidents. The story is similar but even more extreme for local health organizations. Whereas only about a third of local public health departments and hospitals participated in WMD task forces prior to 9/11, this more than doubled following 9/11. For state organizations, participation rates in interagency task forces that address planning for WMD were high to begin and increased even more so following 9/11.

Since 9/11, less than half of local first responders have updated or newly established mutual aid agreements, with most of the updating or establishing occurring for disaster and emergency response in general, rather than for WMD-related incidents specifically. The rates were higher for local health organizations, and while there was a similar focus on disaster and emergency response in general, 14 percent of public health departments and 9 percent of hospitals indicated they updated their agreements for both disasters and WMD-related incidents. Finally, state organizations were even more likely to have updated or established new mutual aid agreements following 9/11, with at least two-thirds having done so. And although most focused on disaster or emergency response in general, about 20 percent of state organizations updated their agreements to address both disasters and WMD.

Prior to 9/11, most organizations already had written emergency response plans in place. Following 9/11, a number of organizations that did not have a response plan subsequently added one, bringing the rates up even higher. However, a more specific question is whether state and local organizations updated or newly developed plans since 9/11 to address WMD in particular. Table 4 shows the percent of organizations that updated their response plans to address one or more types of WMD incidents. Among first responders, local OEMs (49 percent) were most likely to have updated their response plans to address WMD and they did so across the entire spectrum (i.e., chemical, biological, radiological, conventional explosives). About a quarter of law enforcement agencies and paid/combo fire departments also updated or newly developed response plans to address WMD.

Table 4. Percentage of Organizations That Updated Their Emergency Response Plans to Address WMD by Type of Incident*

Organization	Percent Orgs. Updating Plans to Address WMD	Percent Updating by Type of WMD Incident				
		Bio.	Chem.	Radiol.	Conv. Expl.	Cyber
Local First Responders						
Law Enforcement	23%	18%	13%	9%	10%	3%
Fire (paid/combo)	26%	22%	15%	11%	12%	5%
Volunteer Fire	8%	3%	4%	1%	3%	0%
Local/Regional EMS	34%	29%	21%	18%	14%	3%
Local OEM	49%	43%	39%	31%	30%	9%
Local Health Organizations						
Public Health	51%	46%	32	29%	22%	4%
Hospitals	73%	60%	50%	32%	26%	4%
State Organizations						
OEM	76%	68%	50%	41%	50%	21%
EMS	68%	64%	44%	40%	20%	16%
Public Health	68%	64%	20%	12%	---	---

*State public health departments were not asked about incidents involving cyber-terrorism or conventional explosives.

In comparison, between half and three-quarters of local health organizations updated their emergency response plans following 9/11 to address WMD-related incidents. Hospitals, in particular, were more likely to update their response plans, especially for biological or chemical incidents. Two-thirds to three-quarters of state organizations updated their response plans following 9/11, especially to address biological incidents. State OEMs and EMS agencies also updated their plans to address other types of WMD-related incidents.

Joint Preparedness

In terms of joint preparedness--by which we mean participation in such activities as planning, training, or exercises with at least one other organization that also has responsibility for emergency response or ensuring the preparedness of a community within a locale or region--we again see increases since 9/11. Prior to 9/11, less than half the first responders indicated they participated in joint preparedness activities. However, one year following 9/11, most first responders have become involved in joint activities. Even more local health organizations initiated joint preparedness activities following 9/11, with participation rates doubling over the period surveyed. Almost all state organizations were undertaking some form of

joint preparedness activities prior to 9/11; one year following 9/11, rates had increased to nearly 100 percent.

State and local responders not only are more involved in joint preparedness activities, they also increased the number of partners they participate with in doing planning, training, or exercises. On average, the number of partners for local first responders and health organizations participated with more than doubled since 9/11. State organizations had more partnerships in place to begin with than did first responders or local health organizations (an average of 4-6 versus 1-2 for local organizations). After 9/11, their increases were more modest.

Training

Since 9/11, most first responders have increased the percentage of personnel on average trained in incident command/management and even more so for WMD awareness and response. Yet despite these increases, percentages trained still remain somewhat low (e.g., only 31 percent of law enforcement personnel on average are trained in incident command or incident management), suggesting room for improvement. We see a similar story with respect to training for local health organizations and state organizations; however, the latter also started higher and ended up higher than the local organizations. On average two-thirds of state organizations' personnel had been trained in WMD awareness or response since 9/11.

As for what organizations are actually doing about training, since 9/11, about two-thirds of first responders have trained their personnel on emergency response for WMD incidents, another 10-15 percent who had not yet trained their personnel were in the process of identifying training opportunities or had training scheduled, and between 10 and 20 percent indicated they had increased (or shifted over) the number of staff dedicated to addressing WMD preparedness. Compared to the first responders, state organizations (excluding state public health) had trained more and increased their staff more to address WMD. Since 9/11, almost all state OEM and EMS agencies had either trained their personnel on WMD emergency response or were in the process of identifying or scheduling training opportunities, and most had increased (or shifted over) the number of staff dedicated to addressing preparedness for WMD-related incidents. State and local health organizations were asked a similar set of questions and, in general, most have trained their personnel since 9/11 on emergency response to bioterrorism and other WMD-related incidents; about two-thirds of local health organizations (hospitals and local public health departments) and over 80 percent of state public health departments indicated that following 9/11 they had increased (or shifted over) the number of staff dedicated to addressing emergency preparedness for bioterrorism and/or other types of WMD-related incidents.

A majority of first responders (between 50 and 80 percent) have taken part in field or tabletop exercises since 9/11 that cover the spectrum of WMD-related incidents, as well as emergency response to natural disaster. Similarly, a majority of local health organizations have participated in a range of different types of exercises, particularly for chemical or biological incidents and for natural disasters. Nearly all state organizations have participated in a full range of different types of exercises, particularly related to bioterrorism or chemical incidents.

Finally, some first responders (about 1 out of 5) and state organizations (about 1 out of 10) are also developing specialized WMD units since 9/11. Local health organizations were asked a somewhat different question than the above organizations. Instead of units, local public health departments and hospitals were asked whether they had personnel (or access to personnel) specially trained to respond to WMD incidents. Approximately three-quarters of local health organizations indicated they had personnel (or access to personnel) specially trained to respond to WMD incidents. All the organizations had a focus on CBR incidents, but two-thirds of hospitals and one-third of public health departments also indicated they had personnel who were trained to address incidents involving conventional explosives.

How Are Organizations Resourcing These Additional Activities?

The above results indicate that state organizations and local responders are doing more since 9/11 in the areas of planning, joint preparedness, and training. A key question is, how are they resourcing these additional activities? Table 5 shows that a number of organizations have increased their spending since 9/11. Among the first responders, approximately 25-30 percent of paid/combination fire departments and local OEMs had increased spending or shifted resources internally, and (although not shown here) did so predominantly to undertake additional training and to support planning activities specific to WMD response. Only 15 percent of law enforcement agencies indicated they had increased spending or shifted resources following 9/11, similarly focusing on additional training and on planning for WMD. Very few volunteer fire departments (less than 1 percent) increased spending or shifted resources following 9/11. Local health organizations increased spending or shifted resources even more than first responders. Nearly half the hospitals and three-quarters of local public health departments increased spending or shifted resources following 9/11 to address WMD emergency preparedness.

By far, more state organizations increased spending or shifted resources following 9/11 to address WMD emergency preparedness. Over 80 percent of state OEMs and EMS agencies indicated they had done so. Two-thirds focused on additional training of personnel and roughly three-quarters of state organizations also increased spending to cover planning activities specific to WMD response.

Table 5. Percentage of Organizations That Increased Spending and/or Shifted Resources Following 9/11 to Address WMD Preparedness

Organizations	Percent
Local First Responders	
Law Enforcement	15%
Fire (Paid/Combo)	24%
Volunteer Fire	0%
Local/Regional EMS	41%
Local OEM	32%
Local Health Organizations	
Public Health	71%
Hospitals	48%
State Organizations	
OEM	82%
EMS	86%
Public Health	74%*

*State public health departments were only asked whether since 9/11 had they shifted resources internally to address bioterrorism and/or other WMD preparedness.

However, few first responders have received an increase in funding and/or resources following 9/11 to address WMD preparedness, with the exception of local OEM. For example, only 1 percent of law enforcement agencies and 7 percent of paid/combination fire departments indicated they had received additional funding and/or resources, as compared to a third of local OEM. Whereas, a greater percentage of local health organizations received an increase in funding and/or resources following 9/11 to address WMD preparedness: One out of 5 hospitals and 8 out of 10 local public health departments. State organizations by far were the most likely to receive additional funding and/or resources to address WMD preparedness following 9/11, with two-thirds of state EMS agencies and nearly all state OEMs and state public health departments reporting an increase in funding and/or resources.

As to whether these organizations expected any additional increases in their total budget to address WMD preparedness with the start of the new fiscal year (FY03),²⁴¹ there was variation among first responders. Only 1 out of 10 law enforcement agencies and 2 out of 10 paid/combination fire departments expected additional increases compared with one-third of local OEMs. More health organizations expected an increase in their total budget in FY03: a third of hospitals and half of local public health departments. Finally, even more state organizations expected additional increases, with 64 percent of state EMS agencies and over 80 percent of state OEMs indicating this to be the case. Since all state public health departments have received Federal funding for bioterrorism preparedness, we asked whether they anticipated any additional increases in funding from their *state government* for WMD preparedness. Only 13 percent expected additional funding from their state government to improve preparedness. Finally, when we asked the organizations about resourcing issues, we received a number of responses from the different organizations. A sample of comments received is shown in Table 6.

Table 6. Comments Received About Resourcing Issues

Organization	Sample Comment
Law Enforcement	“Being a part of the chief law enforcement agency in the county, I have observed an increase of 100 percent Federal Officers/agencies. Our budget is being cut with no increased funding for manpower or equipment. Doesn’t it make sense to give additional dollars to the agency that knows the needs, vulnerabilities, and people of the area?”
Local EMS	“We have personnel who want to take the training, but we lack the funding to complete this training. We do not have any equipment to combat this threat or protect our personnel. I am sorry to report that we are no better prepared than before Sept. 11, 2001.”
Fire (paid/combo)	“Training is an integral part of WMD. Funds need to get down to the less populated areas as well for equipment and training. Most funding so far seems to be centered around our population centers; however, areas approximately 50 to 75 miles outside these population areas are not well trained and the potential for WMD is still high but with the possibility of more disastrous consequences.”
Local OEM	“Federal, state guidance and planning remain fragmented. Federal and state agencies are starting to do a better job of integrating their efforts but they are too slow to extend the integration down to the county level. Funds must reach the county level.”
Local Public Health	“Staff time remains an issue in planning preparedness. Most positions funded by categorical grants. So far, state and federal dollars prohibit expenditures for staff overtime for training.”
State OEM	“All the ‘billions’ supposedly coming? Of course, we ‘anticipate.’ But state budgets are going down.”
State Public Health	“We have a great plan to move forward and prepare the entire state health care system--we just need the staff to carry out. Local health departments are frustrated and feel money would best be directed at them. At this time, fragmented local planning will not build a State system of preparedness.”

These selected comments provide an overview of some of the recurring themes we heard from respondents. At the local level, organizations are concerned about whether funding and resources being made available at the Federal and state-levels will actually reach their communities. Further, as one respondent noted, the push to improve preparedness for WMD comes at a time when state budgets and

²⁴¹For a number of organizations, the new fiscal year (Fiscal Year 2003) began July 1, 2002.

county budgets are being strained due to the downturn in the economy. At the state-level, having enough staff to focus on WMD preparedness is also a concern.

Conclusions

Overall, these survey results suggest that since 9/11, state and local response and health organizations are doing more in the areas of planning, joint preparedness, and training for WMD. For example, we saw increases in the percentage of personnel being trained and in the participation of organizations in joint planning and preparedness activities. Local health organizations, in particular, have shown some important gains in these areas. Whereas, state organizations, in general, tended to have been more engaged in planning and preparedness activities for WMD prior to 9/11 than local organizations and became even more so following 9/11.

Although organizations increased spending and/or shifted resources to address WMD preparedness following 9/11, the degree to which they have received funding and/or resources to help support these activities vary. Not surprisingly given the initial emphasis at the Federal-level on addressing bioterrorism preparedness, more health organizations at the local and state levels have received funding and/or resources to address WMD preparedness than have first responders and health organizations anticipate additional support to be forthcoming. Whereas, first responders appear to be less optimistic about what type of support in terms of funding and/or resources may be forthcoming.

The tabs to the appendix contain detailed information on all aspects of the State and Local Responder Survey.

TAB 1— THE SURVEY INSTRUMENT

TAB 2— FIRE DEPARTMENT SURVEY

TAB 3— FIELDING PROCEDURES

TAB 4— SAMPLE DESIGN & RESPONDENT SELECTION

TAB 5— RESPONSE RATES

TAB 6—CONSTRUCTING THE SURVEY WEIGHTS

TAB 7—SURVEY COMMENTS

TAB 1—THE SURVEY II INSTRUMENT

This tab contains a description of the Federal Weapons of Mass Preparedness Survey II (FWMDPPS II). The tab following is an example of one particular variant of the instrument.

Instrument Format

The information collected across the various local and state response organizations followed a similar format, as shown in the survey outline in Figure 1. The survey questions were organized into two sections: (1) Organizational Experience and Perceptions, and (2) Emergency Response Planning Activities. The second survey's main objective was to measure what has changed in the one-year since September 11, 2001 with respect to states' and locals' threat experiences and emergency response planning activities. In addition, the second survey asked questions about how these activities were being resourced. Because we wanted to compare changes over time, we attempted to keep the same wording of those questions that were included in both the Wave I and Wave II surveys. The primary difference being that the question in Wave II, in some instances, a question started with the phrase, "since September 11th, 2001" has your organization...."

For the Wave II survey, we elected to create fewer versions of the survey instrument given the similarity of the questions and response sets across the different groups and between the two waves. So instead of 10 different versions of the survey instrument, in Wave II we had four different versions: (1) first responders (law enforcement, fire service, local/regional EMS); (2) emergency responders (local and State OEM, state EMS); (3) health organizations (local public health departments, hospitals); (4) state public health departments. Organizations were combined based on similarities in their roles and scope of missions. Survey variations were primarily limited to differences in question phrasing and specific response sets (e.g., list of areas personnel are trained in) specific to the respondent group. For example, when referring to an organization's area of responsibility, the word "State" was used for State public health departments, "region" or "jurisdiction" for most local organizations, "region" for state and local OEM and state EMS, and "area" for hospitals and local public health departments.

Section Descriptions

The second survey contained only two major sections (see Figure 1) and was purposely kept shorter than the initial survey that had five major sections. This was done to reduce respondent burden given that this was a follow-up survey to the initial set of respondents and the fact that we planned to conduct a third, lengthier survey in the Spring of 2003 using the original sample. Because we surveyed the respondents to the initial survey, we already had available information on organizational characteristics (e.g., size of department, size of population served) and so decided not to ask these organizations to complete this information again thereby helping to reduce the length of the second survey. We also decided not to ask about Federal programs in the second survey, since the panel felt that not enough time had passed since September 11, 2001 for changes occurring at the Federal-level to have reached the state and local levels. For state departments of public health, we also asked about state-level plans to improve bioterrorism preparedness.

The two sections in the second survey were the following:

Section 1. Organizational Experience and Perceptions. Respondents were asked to give their opinion regarding the likelihood of different types of terrorist incidents occurring within their jurisdiction or region within the next five years. They also were asked whether since September

11, 2001 had any incidents of terrorism (including hoaxes) occurred, been attempted, or threatened within their jurisdiction or region that required a response by their organization. If so, they were asked to indicate what type of agents (e.g., chemical, biological) were used in these incidents, type of perpetrator, target of the attack, and whether these incidents resulted in fatal or non-fatal injuries. We also asked about whether their jurisdiction or region had conducted a needs and threat assessment, and what type of support their organization required to conduct future threat assessments.

Section 2. Emergency Response Planning Activities. This section focused on planning, training, and interagency coordination activities. For example, respondents were asked if they had personnel assigned specifically to do emergency management or response planning in general and for WMD. We also asked questions about participation in interagency task forces, committees, or working groups to address disaster preparedness in general and specifically preparedness for WMD-related incidents. Respondents too were asked about changes made to mutual aid agreements and emergency response plans since September 11, 2001. Similar to the initial survey, respondents were presented with the same four narrated scenarios²⁴² and asked to rate their organization's preparedness along a number of different dimensions based on the scenario they considered to be most important for their department to prepare for. In addition, we asked about joint preparedness activities, protocols used for command and control, and communications interoperability. Also included were questions about percentage of personnel trained in particular areas of emergency response; access to special equipment for use in response to WMD incidents; information related to any special units (personnel) trained to respond to WMD incidents. Lastly, we asked about since September 11, 2001 what changes in spending and/or reallocation of resources were made to address preparedness for WMD incidents; whether their organization had received an increase in funding and/or resources and if so, source of increase; and their expectations in terms of future funding and/or resources to address WMD preparedness.

Figure 1. Survey II Instrument Outline

<i>SECTION 1. ORGANIZATIONAL EXPERIENCE AND PERCEPTIONS</i>
<ul style="list-style-type: none">• Expectation of a terrorist incident within their jurisdiction within the next five years• Organizational experience since September 11, 2001 with actual terrorist incidents and/or hoaxes• Whether needs and threat assessment had been conducted for their region or jurisdiction
<i>SECTION 2. EMERGENCY RESPONSE PLANNING ACTIVITIES</i>
<ul style="list-style-type: none">• Organizational participation in emergency response planning activities• Changes made to emergency response plans and mutual aid agreements since September 11, 2001• Self-assessed level of preparedness based on ability to respond to scenario selected by respondent as being most important to prepare for• Joint preparedness activities• Communications interoperability• Relevant training• Resourcing of new activities

²⁴² For information on the scenarios and their development, please refer to Appendix G-1, Third Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, December 15, 2001.

In addition to the above two sections, a final section collected information on the individual completing the survey, and provided an opportunity for the respondent to share additional, open-ended comments and suggestions regarding WMD-related issues of importance to their organization that the survey had not addressed.

Pretesting the Survey Instrument

The second survey instrument was largely comprised of questions that had been included in the initial instrument, modified only slightly in some instances to ask about changes made since September 11, 2001. These questions had been previously pretested with selected experts.²⁴³ Therefore, we did not feel it was necessary to pretest these questions again, but instead had the full panel review the draft instruments for the second survey. Different experts on the panel had suggestions for adding response categories, clarifications, and in the case of the state public health survey on new questions to be added. These changes were incorporated and for the most part did not substantially alter the original wording.

²⁴³ Specifically, a draft questionnaire had been mailed to participating field experts with instructions to take the survey as a responder would, start-to-finish, timing their completion of each section. Pretesting was used to pinpoint and fix instrument problems, streamline questions, adjust wording to match appropriate vocabulary for each responder group, test and expand organization lists, and reduce the survey length. Each version of the survey was tested on two to four subject matter experts. The comments of each pre-tester were incorporated into discussions with subsequent pre-testers to allow for the possibility of agreement or disagreement between pretesters on their suggestions. In each case, pretesters comments were found to be crucial to the development of the survey.

TAB 2—SAMPLE FIRE SERVICES SURVEY

BAR CODE LABEL

**SURVEY II OF FEDERAL
WEAPONS OF MASS DESTRUCTION (WMD) PREPAREDNESS
PROGRAMS**

Conducted by

RAND

on behalf of

The Advisory Panel to Assess Domestic Response Capabilities
for Terrorism Involving Weapons of Mass Destruction

INSTRUCTIONS

1. Please use a dark colored pen to fill out the survey.
2. Mark only **one box** or circle **one number per item**, unless otherwise instructed.
3. As the designated representative of your organization, please fill out all questions, to the best of your ability, from the perspective of your organization as a whole.

FORM:

BATCH:

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
----------------------	----------------------	----------------------	----------------------

Acronyms Used in this Survey

EMS	Emergency Medical Services
FBI	Federal Bureau of Investigation, Department of Justice
FEMA	Federal Emergency Management Agency
HAZMAT	Hazardous Materials
ICS	Incident Command System
LEPC	Local Emergency Planning Committee or Commission
SARA	Superfund Amendments and Reauthorization Act passed by the U.S. Congress in 1986; also known as the Emergency Planning and Community Right-to-Know Act (EPCRA)
WMD	Weapons of Mass Destruction
2-PAM	Pralidoxime chloride

DEFINITIONS

For the purposes of this study, we ask you to keep the following definitions and their scope in mind when answering the remainder of the survey.

- ◆ ***Weapon of Mass Destruction (WMD)*** – A weapon of mass destruction is typically defined as a chemical, biological, radiological, or nuclear device. However, as used in this survey, it may also be any device capable of producing large-scale physical destruction, widespread disruption and / or mass casualties. Thus, a weapon of mass destruction may also be:
 - A conventional explosive device of sufficient magnitude to inflict massive damage or casualties, such as with the Murrah Federal Building in Oklahoma City
 - A device capable of disrupting critical societal infrastructure (for example, contaminating drinking water or agricultural products, or destroying or manipulating fuel or power distribution systems)
 - An attack on an industrial facility (not necessarily involving an actual explosive device) where the purpose is to engineer the hazardous release of a toxic substance to kill and injure surrounding populations.
- ◆ ***Terrorism*** – A criminal act of violence, or threat of violence, designed to create an atmosphere of fear and alarm and to achieve maximum publicity in order to coerce others into actions they otherwise would not undertake, or into refraining from actions that they desire to take. Terrorists are motivated by political aims, may be either lone actors or members of a group, and seek to produce effects beyond the immediate physical damage that they cause.
- ◆ ***Cyber-Terrorism*** – A criminal act involving computer systems or networks designed to cause massive disruption of physical or electronic services in order to intimidate or coerce others. Examples of cyber-terrorism include:
 - An attack against an industrial facility's communications or control systems, resulting in the release of a toxic substance
 - An attack against local responder communications and other computer systems that impairs response, in coordination with a conventional weapons attack
 - Infiltration or corruption of critical data systems (at a hospital or bank, for example) in order to impair normal operations resulting in a lack of public confidence and societal disruption.

Section 1:
ORGANIZATIONAL EXPERIENCE AND PERCEPTIONS

In this questionnaire, the acronym WMD is used as shorthand for “weapons of mass destruction.” The previous page of definitions explains all that we are including in this category for the purposes of this study.

Also, please keep in mind that in the following questions, “cyber-terrorism” is defined as the disruption of critical infrastructure or key information systems for more than one day.

1. How would you rate the likelihood of the following types of major terrorism incidents (e.g., more than 30 individuals with serious injuries) occurring within your jurisdiction or region in the next 5 years?
(Mark One Box on Each Row)

		<i>Very Unlikely</i>	<i>Somewhat Unlikely</i>	<i>Somewhat Likely</i>	<i>Very Likely</i>
a. WMD chemical incident	1 <input type="checkbox"/>		2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>
b. WMD biological incident	1 <input type="checkbox"/>		2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>
c. WMD radiological incident	1 <input type="checkbox"/>		2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>
d. Conventional explosives terrorism incident	1 <input type="checkbox"/>		2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>
e. Cyber-terrorism incident	1 <input type="checkbox"/>		2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>
f. Terrorism incident involving the use of military-grade weapons (e.g., automatic weapons, rifles, mortars)	1 <input type="checkbox"/>		2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>

2. Since September 11th, have any incidents of terrorism (including hoaxes) occurred, been attempted, or threatened within your jurisdiction or region that required a response by your organization?

1 Yes (briefly describe): _____

2 No → Skip to Question 7, page 4

3. Since September 11th, did any of these terrorist incidents involve the use (or threat of use) of the following?

(Mark All That Apply)

- 1 Anthrax
- 2 Other biological weapon
- 3 Chemical weapon
- 4 Radiological weapon
- 5 Conventional explosives
- 6 Cyber-terrorism
- 7 Military-grade weapons (e.g., automatic weapons, rifles, mortars)
- 0 **None of the above**

4. Since September 11th, were any of these terrorist incidents thought to have been associated with the following?

(Mark All That Apply)

- 1 Right-Wing (militias, secessionists, etc.)
- 2 Left-Wing (socialist revolutionary, Weathermen, etc.)
- 3 Race / ethnicity / hate-related (anti-Semitic, anti-homosexual, anti-immigrants, white supremacists, etc.)
- 4 Single issue / special interests (environmental, animal rights, anti-abortion, etc.)
- 5 Millennial / doomsday cults / (Y2K, religious cults, etc.)
- 6 Other *(please specify)*

- 0 **None of the above**

5. Since September 11th, please indicate the type(s) of targets involved in these terrorist incidents.
(Mark All That Apply)

- 01 Nuclear power plant
- 02 Military personnel or installation
- 03 Telecommunications system
- 04 Airport
- 05 Subway
- 06 Other transportation system (e.g., train, bus, rail)
- 07 Banking / financial establishment
- 08 Other private company, firm, or business
- 09 Large public gathering (e.g., stadiums, malls, theater complexes, arenas)
- 10 Government representative (e.g., governor, assemblyman)
- 11 Other public agency personnel (e.g., police officer, fireman)
- 12 Private citizen(s)
- 13 Other *(please specify briefly)* : _____

6. Since September 11th, did any of these incidents result in fatal or non-fatal injuries to:
(Mark All That Apply)

- 1 the perpetrator(s)?
- 2 emergency response, medical, or health personnel?
- 3 other individuals known (or presumed) to be the target(s) of the attack?
- 4 bystanders (i.e., not the intended target(s) of the attack)?
- 0 None of the incidents resulted in injuries**

The following questions are about needs and threat assessment.

7a. Has your jurisdiction conducted a needs assessment?

- 1 Yes
- 2 No
- 3 Don't know

7b. Was this needs assessment conducted specifically as part of the Department of Justice's Office of Domestic Preparedness (ODP / DOJ) Equipment Program in order to receive funding?

- 1 Yes
- 2 No
- 3 Don't know

7c. Since September 11th, has your organization conducted, or is it in the process of conducting, a threat assessment?

- 1 Yes
- 2 No, a threat assessment had already been conducted prior to September 11th
- 3 No → *Skip to Question 7e*

7d. Who conducted the threat assessment?

(Mark All That Apply)

- 1 Our organization
- 2 Inter-agency task force
- 3 Another agency or organization within our jurisdiction
- 4 Other *(please specify)* _____

7e. What type of support does your organization need in order to conduct future threat assessments?

(Mark All That Apply)

- 1 Protocols for conducting threat assessments
- 2 Training on how to conduct threat assessments
- 3 Better intelligence and threat information from the Federal government
- 4 Access to outside consultant expertise to assist with threat assessment
- 0 **No additional support is needed**

Section 2:

EMERGENCY RESPONSE PLANNING ACTIVITIES

Please keep in mind that for the purposes of this survey, WMD includes *any* device capable of producing large-scale physical destruction, widespread disruption and / or mass casualties, as described inside the front cover.

8. Does your organization have any individuals specifically assigned (full-time or part-time) to do emergency management or response planning?

1 Yes

2 No

9. Does your organization have any individuals specifically assigned (full-time or part-time) to do planning for WMD incidents?

1 Yes

2 No

10. Does your organization *currently* participate in a SARA Title 3 Emergency Planning Committee or Commission (LEPC) in your area?

1 Yes

2 No

11. Does an interagency disaster preparedness committee, task force, or working group (not including an LEPC) exist in your jurisdiction or region (whether or not your agency is a participant in it)?

1 Yes → *Continue with Question 11a*

2 No → *Skip to Question 12*

11a. Does your organization participate in this group?

1 Yes

2 No

11b. Does this interagency disaster preparedness committee, task force, or working group address planning for WMD incidents specifically?

1 Yes

2 No

11c. Please indicate which organizations in your region regularly participate in this interagency disaster preparedness committee, task force, or working group:

(Mark All That Apply)

Local Organizations (city or county)

- 01 Board of supervisors or other elected government officials
- 02 Law enforcement organizations
- 03 Other fire departments
- 04 HAZMAT (free-standing organizations)
- 05 Local hospitals or other medical institutions
- 06 EMS (3rd-service, hospital-based, fire department-based, or private ambulances)
- 07 Local health departments
- 08 Utilities (public or private – e.g., water and power)
- 09 Transportation (public or private organizations)
- 10 OEM (office of emergency management or preparedness)
- 11 Surrounding mutual aid response organizations
- 23 Local military installation
- 12 Other *(please specify)*: _____

State Organizations

- 13 State OEM (office of emergency management)
- 14 State EMS (state-level office of emergency medical services)
- 15 State law enforcement organizations
- 16 State public health department
- 17 State office of fire control
- 18 National Guard
- 19 Other *(please specify)*: _____

Federal Organizations

- 20 Federal Emergency Management Agency (FEMA)
- 21 Federal Bureau of Investigation (FBI)

22 Other (please specify): _____

11d. Since September 11th, have any new organizations (i.e., non-traditional partners) joined the interagency disaster preparedness committee, task force, or working group in your region?

(Mark All That Apply)

New Organizations:

1 Health or medical organizations (e.g., hospitals, public health agencies)

2 Local businesses

3 Private security firms

4 Academic institutions (e.g., colleges, universities)

5 Citizens' groups / public interest groups

6 Other (please specify): _____

0 No new organizations

Now we want to ask your opinion about your organization's overall approach to addressing WMD preparedness.

Please indicate how much you agree or disagree with the following statements.

12. To our organization, WMD incidents are crises like any other emergency and our efforts to prepare for WMD are, with few exceptions, the same as our efforts to prepare for any large-scale incidents (e.g., natural disasters or other hazards in our jurisdiction).

*Strongly
Disagree*

*Neither Agree
nor Disagree*

*Strongly
Agree*

1

2

3

4

5

13. The resources (e.g., equipment, training, exercises) used to prepare for WMD incidents are specialized and distinct from the resources needed to prepare for other large-scale incidents (e.g., natural disasters or other hazards in our jurisdiction).

*Strongly
Disagree*

*Neither Agree
nor Disagree*

*Strongly
Agree*

1

2

3

4

5

14. Since September 11th, has your organization updated existing mutual aid agreements or established new ones with other city, county, state, or regional organizations for disaster and emergency response?

(Mark All That Apply)

- 1 Yes, for disaster and emergency response in general
- 2 Yes, for WMD incidents specifically
- 3 No new changes have been made to such agreements since 9/11
- 0 No mutual aid agreements exist

The following questions ask about your organization's planning activities for emergency response in general.

15. Does your organization have a written emergency response plan?

- 1 Yes
- 2 No → *Skip to Question 19*

16. Does your organization's written emergency response plan . . .

(Mark One Box Per Question)

- a. Address operational areas and jurisdictional boundaries? 1 Yes 2 No
- b. Include mutual aid agreements to provide additional resources? 1 Yes 2 No
- c. Include a response plan for communicating with the public and / or the media? 1 Yes 2 No
- d. Address how your organization would communicate with other first responders (e.g., law enforcement, fire, EMS, HAZMAT organizations) within your jurisdiction? 1 Yes 2 No
- e. Address how your organization would communicate with health responders (e.g., hospitals, public health agencies) within your jurisdiction? 1 Yes 2 No
- f. Address procedures for mass decontamination of victims? 1 Yes 2 No
- g. Address procedures for decontamination of an area or site? 1 Yes 2 No
- h. Address how your organization would coordinate with other agencies outside your jurisdiction? 1 Yes 2 No

17. Is your organization's written emergency response plan integrated with . . .

(Mark All That Apply)

- 3 Federal response plans?
- 4 State response plans?
- 5 Response plans of other local organizations in your jurisdiction?
- 0 None of the above

18. Since September 11th, has your organization updated or newly developed a written emergency response plan to specifically address . . .

(Mark All That Apply)

- 1 Biological incidents?
- 2 Chemical incidents?
- 3 Radiological incidents?
- 4 Conventional explosives terrorism incidents?
- 5 Cyber terrorism incidents?
- 0 None of the above

19. Of the following four types of WMD incidents, which is the most important for your organization to prepare for?

(Mark ONE Box Only)

- 1 Biological
- 2 Chemical
- 3 Conventional explosives
- 4 Radiological

On the following page are listed four scenarios for: conventional explosives, biological, chemical, and radiological WMD incidents. Please read the one scenario that corresponds to the type you selected above in Question 19, and answer questions 20 - 26 in reference to this scenario.

SCENARIO 1: CONVENTIONAL EXPLOSIVES INCIDENT

One weekday morning, a major explosion occurs in a large office building downtown, with hundreds of people reportedly inside at the time of the blast. First responders report the following:

- The blast caused major structural damage to the office building, with some floors collapsed in upon each other
- Firefighters, police, and emergency medical personnel find dozens of people stumbling from the building with mild to severe physical injuries
- Buildings as far as a 5-block radius suffered blown-out windows
- Within an hour, 337 individuals require transport for medical treatment, with an unknown number still inside
- Hundreds of lookers-on, family, co-workers, and media personnel have congregated in the area, awaiting information.

As local responders attempt to enter, they find evidence of other explosive devices in the building, forcing them to exit and fall back from the scene. As the full magnitude of the incident becomes known, first State, and then Federal agencies are called on to assist in the response. As a suspected act of terrorism, collecting and preserving evidence from the scene immediately becomes a major concern.

SCENARIO 2: CHEMICAL INCIDENT

An explosion in a building with 200 people inside results in numerous injuries and some fatalities, but minimal structural damage. As first responders arrive on the scene, they observe the following:

- Twenty-five individuals have been killed by the blast
- There are more casualties than would be expected for an explosion alone
- Unlikely symptoms among the survivors include sweating, disorientation, muscle tremors, convulsions and eye pain exhibited by 145 individuals.

Soon, some of the responders also start to experience similar symptoms. A highly toxic and persistent chemical agent is suspected of having been released by the explosion. Both state and Federal emergency management officials are immediately notified. Cross-contamination becomes a major concern as victims find their way to local hospitals and responders operate in an area potentially covered with an active chemical agent. As the media quickly picks up on the story, panic begins to spread among the large crowd that has formed outside the building and in the nearby vicinity.

SCENARIO 3: BIOLOGICAL INCIDENT

During a three-day period in July, 20 individuals present to a local hospital's emergency room complaining of fever, night sweats, headaches, coughing and joint pains. Initially, an untimely flu epidemic is suspected. However, after the third day, concern grows more acute:

- Additional patients are admitted with more severe symptoms
- Laboratory personnel who analyzed patient blood samples begin reporting similar symptoms

Several days later, ERs and physicians have seen enough cases to alert local and state public health authorities, who immediately undertake large-scale surveillance and dispatch an investigation team. The state health department also notifies the CDC at which point other Federal agencies are also alerted. It is quickly determined that all patients had visited a regional airport in the past 10 days. The Governor orders the airport closed and quarantined. Fire and HAZMAT teams report to the scene to investigate and determine if there is a continuing threat. The National Guard is called to assist police with airport closure and crowd control.

- Days later, 7 of those affected die
- All victims' blood specimens test positive for brucellosis.

A statewide and international alert is activated urging anyone who passed through the airport to contact their local health department. News agencies report that brucellosis can be fatal, creating panic. Local ERs are flooded with patients complaining of flu-like symptoms.

SCENARIO 4: RADIOLOGICAL INCIDENT

An explosion downtown on the top of a multi-storied building causes significant structural damage and starts a major fire on the upper levels. Fire and EMS personnel arrive and attempt to suppress the fire, rescue people trapped inside, and treat and transport the injured. Ambulances carry the first victims to local hospitals, while police cordon off the area.

- Hundreds were reportedly in the building at the time of the blast
- A local radio station receives a call claiming responsibility on behalf of a terrorist group, stating that the bomb released radioactive materials
- A HAZMAT team with detection capability is dispatched and confirms the bomb was a radioactive dispersion device.

Police begin to evacuate a 10-block radius around the incident site, asking residents in adjacent areas to remain indoors. News agencies quickly pick up on the story. People in and around downtown panic and flee, causing traffic gridlock and a mass exodus from the town. Since initial responders transported the first rescued victims directly to hospitals, spread of radioactive contaminants becomes a serious concern.

Considering the type of WMD incident and scenario you selected in Question 19, please rate your organization’s level of readiness on a scale of 1 to 5, with 1 being INADEQUATE and 5 being EXCELLENT.

Please answer questions 20 - 26 carefully, considering the scenario you selected on the opposite page. Circle one number for each question on the 5-point scale given below.

20. Your organization’s **written emergency response plan** to be used during a response to an event similar to the one selected above is:

INADEQUATE					EXCELLENT
1	2	3	4	5	

21. Your organization’s **knowledge and expertise** about response to this type of event are:

INADEQUATE					EXCELLENT
1	2	3	4	5	

22. Your organization’s **equipment** to respond to this type of event is:

INADEQUATE					EXCELLENT
1	2	3	4	5	

23. Your organization’s **training** to respond to this type of event is:

INADEQUATE					EXCELLENT
1	2	3	4	5	

24. Your organization’s ability to **communicate and coordinate** with other organizations likely to be involved in a response to this type of event is:

INADEQUATE					EXCELLENT
1	2	3	4	5	

25. Your organization’s plan for **communicating** with the media and/or public is:

INADEQUATE					EXCELLENT
1	2	3	4	5	

26. How would you rank your organization’s **overall preparedness to respond** to this type of event?

INADEQUATE					EXCELLENT
1	2	3	4	5	

Now we would like to ask you a few questions about joint preparedness activities.

27. In the table below, please mark the appropriate boxes to indicate whether, since September 11th, your organization has participated in joint preparedness activities for natural disasters and / or WMD incidents with each of the organizations listed.

NOTE: By joint preparedness activities, we mean joint planning, training, or exercises.

Since September 11th, has your organization participated in joint preparedness activities with . . .
(Please Mark All That Apply)

	<i>FOR NATURAL DISASTERS AND EMERGENCIES:</i>	<i>FOR WMD INCIDENT RESPONSE:</i>
A. LAW ENFORCEMENT ORGANIZATIONS?	1 <input type="checkbox"/>	2 <input type="checkbox"/>
B. FIRE DEPARTMENTS?	1 <input type="checkbox"/>	2 <input type="checkbox"/>
C. HAZMAT (FREE-STANDING ORGANIZATIONS)?	1 <input type="checkbox"/>	2 <input type="checkbox"/>
D. LOCAL HOSPITALS OR OTHER MEDICAL INSTITUTIONS?	1 <input type="checkbox"/>	2 <input type="checkbox"/>
E. EMERGENCY MEDICAL SERVICES (EMS)?	1 <input type="checkbox"/>	2 <input type="checkbox"/>
F. LOCAL HEALTH DEPARTMENTS?	1 <input type="checkbox"/>	2 <input type="checkbox"/>
G. UTILITIES (PUBLIC OR PRIVATE – E.G., WATER & POWER)?	1 <input type="checkbox"/>	2 <input type="checkbox"/>
H. TRANSPORTATION (PUBLIC OR PRIVATE ORGANIZATIONS)?	1 <input type="checkbox"/>	2 <input type="checkbox"/>
I. OEM (OFFICE OF EMERGENCY MANAGEMENT OR PREPAREDNESS)?	1 <input type="checkbox"/>	2 <input type="checkbox"/>
J. SURROUNDING MUTUAL AID RESPONSE ORGANIZATIONS?	1 <input type="checkbox"/>	2 <input type="checkbox"/>

Since September 11th, our organization has not participated in joint preparedness activities with any of the above agencies.

Now we'd like to ask you some questions about communications interoperability.

By interoperability, we mean the ability of police or emergency response teams involved in an emergency to communicate in real-time across agencies and / or jurisdictions via radio or telephone, in order to mount a well-coordinated response.

28. What formal protocol for command and control does your organization use for large-scale incidents?

- 1 Incident Command System (ICS)
- 2 Other standardized incident command and control or management system
- 0 None of the above

29. In the event of a large-scale emergency involving multiple agencies or jurisdictions, how would you rate your organization's ability to communicate with other responding organizations?

INADEQUATE EXCELLENT

1 2 3 4 5

30. Has your organization had communications interoperability problems in the past 5 years with any of the following agencies in your jurisdiction?

(Mark All That Apply)

- 1 Fire departments
- 2 Police
- 3 EMS
- 4 Health / medical organizations
- 5 County agencies
- 6 Military agencies
- 7 State agencies
- 8 Federal agencies
- 9 Other *(please specify)* _____

31. Please rate how big a problem communications interoperability is for your organization during a response to a large-scale incident that involves multiple agencies.

<i>No Problem <u>at All</u></i>		<i>Somewhat of <u>a Problem</u></i>		<i>Very Much <u>a Problem</u></i>
1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>

32. What factors, if any, limit current efforts to improve the interoperability of your organization’s communications system?

(Mark All That Apply)

- 01 Aging communications system and hardware
- 02 Lack of information or guidance on what technologies to purchase
- 03 Uncertainty surrounding the availability of spectrum for public safety use
- 04 Frequency incompatibility between emergency response organizations in our region
- 05 Lack of funding
- 06 Inter-agency politics / disagreements
- 07 Differences between jurisdictions in rules and regulations
- 08 Differences between jurisdictions or agencies in resource priorities
- 09 Other *(please specify)* _____
- 00 **No efforts are underway to improve the interoperability of our organization’s communications system**

Now we would like to ask you a few questions about training and equipment.

33. What percentage of your response personnel are trained in the following areas?

(Please give your best estimate)

	Percent of Response Personnel Trained
a. Incident Command or Incident Management	<input type="text"/> <input type="text"/> <input type="text"/> %
b. Personal Protective Equipment Levels A or B	<input type="text"/> <input type="text"/> <input type="text"/> %
c. Personal Protective Equipment Level C	<input type="text"/> <input type="text"/> <input type="text"/> %
d. Hazardous Materials Technician / Specialist	<input type="text"/> <input type="text"/> <input type="text"/> %
e. WMD Awareness or Response	<input type="text"/> <input type="text"/> <input type="text"/> %
f. Certified Emergency Medical Technician – Intermediate	<input type="text"/> <input type="text"/> <input type="text"/> %
g. Certified Emergency Medical Technician – Paramedic	<input type="text"/> <input type="text"/> <input type="text"/> %

34. Since September 11th, has your organization . . .

(Mark One Box for Each Item)

- a. Increased (or shifted over) the number of staff dedicated to addressing emergency preparedness for WMD incidents? 1 Yes 2 No
- b. Scheduled training for WMD incidents? 1 Yes 2 No
- c. Trained personnel on emergency response for WMD incidents (or are personnel in the process of being trained)? 1 Yes 2 No
- d. Identified training opportunities for emergency response to WMD incidents? 1 Yes 2 No

34a. Since September 11th, has your organization participated in tabletop or field exercises? If so, please indicate for what type(s) of incidents?

(Mark All That Apply)

- ₁ Chemical
- ₂ Biological
- ₃ Radiological
- ₄ Cyber-terrorism
- ₅ Conventional explosives
- ₆ Natural disasters
- ₀ **No, our organization has not participated in any exercises since September 11th**

35. Does your organization stock or have access to any of the following types of equipment for WMD incidents?

(Mark All That Apply)

- ₁ Monitoring and detection equipment for chemical agents
- ₂ Monitoring and detection equipment for biological agents
- ₃ Monitoring and detection equipment for radiological agents
- ₄ Personal Protective Equipment (PPE) Levels A or B
- ₅ Personal Protective Equipment (PPE) Level C
- ₉ Equipment for decontamination of victims and / or sites
- ₆ Medical caches and/ or antidotes for chemical agents
(e.g., atropine sulfate autoinjectors, 2-PAM, cyanide antidote kits)
- ₇ Medical caches and/ or antidotes for WMD biological agents
- ₈ Medical caches and/ or antidotes for WMD radiological agents
- ₀ **None of the above**

36. Since September 11th, has your organization developed, or are you in the process of developing, any unit(s) specially trained and equipped to respond to WMD incidents?

1 Yes

2 No → *Skip to Question 38, next page*

37. What types of WMD incidents are these units trained to respond to?

(Mark All That Apply)

1 Chemical

2 Biological

3 Radiological

4 Cyber-terrorism

5 Large-scale conventional explosives

Now we'd like to ask you some questions about resource changes to address WMD preparedness made by your organization since September 11th.

38. Since September 11th, has your organization increased its spending, or shifted resources internally, to address WMD emergency preparedness?

- 1 Yes
- 2 No → *Skip to Question 40*

39. If so, for what purpose(s)?
(Mark All That Apply)

- 1 Additional security for your organization
- 2 Staff overtime
- 3 Additional training specific to WMD response
- 4 Purchase of personal protective or other equipment specific to WMD response
- 5 Planning activities specific to WMD response
- 6 Other (please specify) _____
-

40. Since September 11th, has your organization received an increase in its funding and / or resources (e.g., new equipment) for WMD preparedness?

- 1 Yes → *Continue with Question 41*
- 2 No → *Skip to Question 43*

41. If so, which of the following best describes how the increases in funding and / or resources for WMD preparedness have become available?
(Mark All That Apply)

- 1 Our organization's total budget was increased → *Continue with Question 42*
- 2 Our organization internally reallocated funds and / or resources from other areas and redirected them to WMD preparedness activities → *Skip to Question 43*

42. If your organization’s total budget was increased post-9/11 specifically to address WMD preparedness, what was the source(s) of this increase?

(Mark All That Apply)

- 1 From the City or County
- 2 From the State Office of Emergency Management (or equivalent in your state)
- 3 From other State agencies
- 4 From the Federal government
- 5 Other *(please specify)* _____
- 0 **Our organization’s total budget was not increased**

43. With the start of the new fiscal year, does your organization anticipate any additional increases in its total budget to address WMD preparedness?

- 1 Yes
- 2 No

44. Compared with other needs that may be facing your organization, would you consider applying for Federal funding to prepare for WMD as a low, medium, or high priority – were such Federal preparedness funding to become available specifically for organizations like yours?

- 1 High priority
- 2 Somewhat of a priority
- 3 Low priority
- 0 **Not at all a priority**

45. If your organization reallocated funds and / or resources to address WMD preparedness, to the best of your knowledge, was this reallocation of funds directly related to the events of September 11th?

- 1 Yes, this reallocation was related to the events of 9/11
- 2 No, this reallocation was unrelated to the events of 9/11

Our organization did not reallocate funds and / or resources

46. From what areas did your organization have to shift resources (including staff) to meet increased demands associated with September 11th?

(Briefly describe) _____

Point of contact for matters related to this survey:

Your Name: _____

Position Title: _____

Title of organization: _____

Address: _____

Street

City

State

Zip Code

E-Mail: _____

Phone: (_____) _____ - _____

Fax: (_____) _____ - _____

Thank you for completing this important survey. Please return your completed survey in the business reply envelope provided. If you have any questions regarding this study, please call Dr. Lois Davis at RAND, tel. 888-855-7263, or feel free to e-mail her at (Lois_Davis@rand.org).

TAB 3—FIELDING PROCEDURES

This tab describes the procedures to field the second Federal Weapons of Mass Destruction Preparedness Programs Survey (FWMDPPS II). The second survey was to be predominantly a mail survey without telephone follow-up (except was for state departments of public health). In addition, the second survey differed from the initial survey by having a much shorter fielding period. These parameters were chosen due to time and budget constraints. Despite these constraints, as noted in the section on response rates, we achieved a high rate of response for all groups largely we believe due to the fielding of this survey just prior to the anniversary of the September 11, 2001 attacks.

An outline of major fielding steps that were implemented includes the following: a letter sent one week in advance of the survey mailing; inclusion of a motivating cover letter and certificate of appreciation with the survey mailing; establishing a toll-free 800 number to field respondent questions; follow-up postcard reminders post survey mailing; the mailing of a second, replacement survey; and lastly, telephone follow-up only for state public health departments. In addition to further improve response rates, the second mailing of the survey was sent via Federal Express to the most challenging of the respondent populations, hospitals and state departments of public health.



Survey research has shown that incentive gifts mailed along with a survey instrument can increase response rates by elevating the perceived importance of the study and conveying both appreciation and recognition of the respondent's time.²⁴⁴ For the initial survey, we included in each survey packet a commemorative coin that was imprinted with the title of the first survey and the name of the panel. For the second survey, we created certificates of appreciation for each organization that had responded to our initial survey that included the name of the organization and that was signed by the Panel Chairman, James S. Gilmore, III, and by RAND project leaders.

Survey Mailing

To better manage the fielding process, the organizations to be surveyed in Wave II were divided into several groups or “waves”. In addition, the survey instrument for state departments of public health took longer to develop and so were fielded later than the other organizations' instruments. Table 1 gives the timeline for the fielding of the second survey for each wave. Each survey wave opened with an advance letter to the respondent indicating the importance of the survey and alerting them to its imminent arrival. Advance letters were printed on RAND stationery and signed by the RAND survey director. About a week following the advance letter, the survey was sent out with a cover letter and certificate of appreciation. Cover letters were printed on panel stationery and were signed by Panel Chairman James S. Gilmore, III, former Governor of Virginia.

²⁴⁴ Fowler, F. Jr. *Survey Research Methods* (2nd ed.), Newbury Park, CA, Sage Publications, 1993.

Table 1.
Final Survey Operations Timeline for FWMDPPS II

<i>Wave 1: Samples 1, 2, & 3</i>		Wave 2: State Public Health Sample	
			
Task	Timeline	Task	Timeline
Advance letter	7/30/2002	Advance letter	8/15/2002
1 st survey mailing	8/6/2002	1 st survey mailing	8/16/2002
Postcard reminder	8/13/2002	Postcard reminder	8/21/2002
2 nd survey mailing (Hospital sample via FedEx)	9/3/2002	2 nd survey mailing	9/3/2002
N/A		Phone reminders (N=26)	9/30/2002 -10/11/2002
N/A		FedEx a 3 rd surveys to non-responders	10/4/2002
Survey operations closed	10/2/2002	Survey operations closed	10/18/2002

Instructions to Respondents

In the survey cover letter, respondents were asked to complete the survey and return it to RAND in the enclosed postage-paid, business reply envelope. They were told that the survey would take about one-half hour to complete. They were instructed to complete the survey as the designated representative of their organization, i.e., from the perspective of their organization as a whole. Respondents also were given specific definitions for “weapons of mass destruction”, “terrorism,” and “cyber-terrorism” in the body of the survey, and were asked to keep these definitions and their scope in mind when answering each question.

Follow-Up

Approximately seven days following the initial survey mailing, reminder postcards were sent out to all survey recipients. The postcard thanked respondents if they had already filled out and returned the survey, but also prodded those to complete the survey who had not already done so (again citing the importance of the study and their participation in it).

Approximately four weeks following the initial mailing of the survey packet, a replacement survey was mailed to all candidates for whom a returned survey was not on file. As an added measure for the more challenging sample to survey, hospitals, the second mailing was sent via Federal Express. Based on our prior experience with this sample, we found that using Federal Express to draw their attention and underscore the importance of the survey was helpful in increasing response rates.

Telephone Follow-Up with State Departments of Public Health

Telephone follow-up was conducted only for state departments of public health in order to increase their response rates. The timing of the second survey coincided with deadlines for these organizations to complete state-level plans to receive Federal funding to improve bioterrorism preparedness and other planning activities. For this reason, this group in particular was a challenge to survey. Telephone follow-up was conducted by RAND's Survey Research Group (SRG) staff. Interviewers spoke either with the person to whom the packet was mailed or, in cases where that was impossible, to that person's assistant or secretary. The purpose was to reiterate the importance of the respondent's participation in the study and to answer any questions or concerns that the respondent might have. Eliminating questions and encouraging participation makes survey response more likely. Upon contacting each organization, a copy of the survey instrument was sent via Federal Express. The result was an improved response rate from 31 percent just prior to telephone follow-up being conducted to a final response rate of 60 percent for this respondent group.

TAB 4-SAMPLE DESIGN AND RESPONDENT SELECTION

The initial Federal Weapons of Mass Destruction Preparedness Programs Survey (FWMDPPS I) conducted in 2001 was designed to allow inference to the nationwide community of state and local emergency response and health organizations. The second survey (FWMDPPS II) conducted in 2002 was a follow-up to those organizations that initially responded to the first survey. The purpose of the second survey was to assess what changes these organizations had made in terms of emergency response planning since September 11, 2001 and to assess changes in their threat experience. To understand how the original sample was constructed, we summarize here the sample design and respondent selection process used for FWMDPPS I. The reader also is referred to the next Appendix Section “Construction of Survey Weights” for a discussion of the statistical adjustments made to represent the entire population in each discipline surveyed in Waves I and II (i.e., FWMDPPS I and II).

Sample Design and Respondent Selection

The original sample consisted of three tiers of state and local emergency response and health organizations — county, regional, and state—as shown in Table 1 below, with sampling strategies tailored to each. Surveys were sent directly to the individual in each organization most familiar with the organization’s participation in federal program and WMD preparedness activities, or, if no such individual could be identified, to the individual responsible for emergency response planning. The names and contact information for these individuals were requested from the head of each organization—for example, the chief of a fire or police department, or the ER or medical director of a hospital. In many cases, the organizational heads elected to complete the survey themselves. In all, surveys were initially sent to 1,687 organizations, including 150 at the state level and 1,526 at the local and regional levels.²⁴⁵

Table 1
Organizations Included in the FWMDPPS Surveys I and II

<i>Local (City/County)</i>	<i>Regional</i>
<ul style="list-style-type: none"> • Law enforcement • Fire departments <ul style="list-style-type: none"> ○ Paid ○ Volunteer ○ Combination 	<ul style="list-style-type: none"> • EMS
<ul style="list-style-type: none"> • Hospitals • Emergency Medical Services (EMS) • Offices of Emergency Management (OEM) • Public health departments 	<p><i>State</i></p> <ul style="list-style-type: none"> • EMS • OEM • Public health departments

Sampling County-level Organizations

The survey followed a multi-level cluster design for local and regional response organizations, first sampling counties and then sampling local and regional organizations that serve the sampled

²⁴⁵ Washington, DC was also sent all three State-level surveys, and State-level OEM and public health surveys were sent to the U.S. territories of Puerto Rico, Guam, Virgin Islands, and Northern Mariana's Islands.

counties. Two factors motivated the decision to sample by county. First, lack of comprehensive nationwide registries for some of the organizations listed in Table 1 makes it cost-effective to first choose counties and then identify all response organizations within the subset of counties selected. Second, from a substantive perspective, counties provide the most consistent unit of geographic organization for emergency response services throughout the U.S., particularly when both urban and rural areas are the object of study. Whereas, service areas and jurisdictions for response organizations tend to follow political boundaries, with counties playing a central role between local or city areas and the state. Of course, counties are not *always* the most relevant units of emergency response. Service catchment areas for hospitals and EMS organizations, for example, do not always respect county boundaries, as is true for the formal emergency response regions established by many states. Nonetheless, clustering by county provided the most cost-effective and consistent geographic unit for obtaining a nationwide sample of local organizations.

Ensuring the Inclusion of “Sensitized” Counties

In addition to the randomly sampled of counties, 10 counties were hand-picked for inclusion based on past WMD terrorist incidents or upcoming events that might have heightened their sensitivity to WMD terrorism (e.g., the Olympics).²⁴⁶ The most prominent of each type of response organization within each of these counties was then selected to receive a survey. This allowed comparisons between “average” U.S. counties and those most likely to have invested in preparedness efforts or sought federal support to do so.

Selecting the County-level Sample

The county sample followed a two-stage design that used counties as the primary sampling unit and then type of response organization as the secondary sampling unit. In the first stage, 200 counties out of the 3,105 counties in the contiguous United States, Alaska, and Hawaii were selected with a probability proportional to the size of their 1998 population, as estimated in the Department of Health and Human Services (DHHS)’s 2000 Area Resource File. The choice to give more populous counties a greater chance of selection was based on the fact that urban areas have been the foremost recipients of federal WMD preparedness support; they are perceived to be more likely targets for terrorism; and, as Table 2 illustrates, without such a selection scheme it is likely that rural counties would have comprised nearly half of the sample simply because about half of U.S. counties are rural.

²⁴⁶ The selection of sensitized counties was made prior to the attacks on New York City and the Capital on September 11th of this year. They are: Cook County, Illinois; Dade County, Florida; Fulton County, Georgia; King County, Washington; Los Angeles, California; Multnomah County, Oregon; New York County, New York; Oklahoma County, Oklahoma; Salt Lake County, Utah; and San Francisco County, California.

Table 2
Comparison of Sampled Counties and All Counties in the United States

Comparison by Region				
	All U.S. Counties (N=3,105)		Sampled Counties (N=200)	
	N	%	N	%
Northeast	217	7	31	16
Midwest	1,055	34	60	30
West	442	14	33	17
South	1,391	45	76	38
Rural	1,410	45	43	22

Comparison by Population				
	All U.S. Counties		Sampled Counties	
	Mean	Median	Mean	Median
Population	87,053	24,080	398,037	65,745

However, rural organizations are not excluded altogether. Though the probability of selection is based on county population, the sampling scheme ensures that a sufficient number of rural counties are also included in the sample so that rural views on federal assistance may enter into the analysis. Weighting proportional to population provides the balance required to ensure an adequate selection of urban counties without sacrificing the ability to give rural counties a voice in the panel’s deliberations.

In the second survey, we also had representation from all 200 counties from our initial sample. Recall that the second survey was sent to only those organizations that had responded to the initial 2001 survey. For each county, at least one or more organizations responded to the follow-up survey.

Selecting Organizations Within Counties

Within each county, one organization from each of the respondent groups listed in Table 1 above (local law enforcement; paid, volunteer, and combination fire departments; hospitals; EMS organizations; OEMs; public health departments; and regional EMS organizations) was randomly selected to receive a survey. When no organizations within a county from a particular respondent group could be identified, it was determined which surrounding organizations served the county, and the sampling was done from these.

Sampling Regional Organizations

Often, emergency response or health organizations are located apart from the counties they serve. For example, a public health department may reside in one county, but have a number of neighboring counties under its jurisdiction, especially in sparsely populated or rural areas. The term “regional” as used here refers to such organizations, whose jurisdiction or service area falls between the county and state level. In each county, the sample was drawn first from local

organizations residing within the county; if no local organizations were found to serve the county, regional organizations serving the county, but residing elsewhere, were searched for and sampled. This “first local, then regional” rule guaranteed that the most local relevant provider of services to a county was properly identified and surveyed, even when that provider resides outside the county.

Regional EMS organizations, in particular, are unique in that they often serve a county population that is already served by a local EMS provider. That is, a number of counties are served by both local EMS organizations based within the county, and regional EMS organizations based outside the county. To ensure that the perspectives of both local and regional EMS organizations on federal programs and WMD awareness were captured in the survey, both local and regional EMS organizations were sampled for each county.

Census of State-level Organizations

In addition to local and regional responders, state-level EMS, OEM, and public health departments in each of the 50 states, Washington, DC, and the U.S. territories of Puerto Rico, the Virgin Islands, Mariana's Islands, and Guam were also surveyed. “State-level” signifies the single focal point, coordinating, or administrative body in each state for a particular response community (e.g., public health) that has the state as its jurisdictional mandate. These state-level entities are important for their statewide response and policy-making activity, but also as intermediaries between Federal agencies and local response organizations.

Sample Size Calculations

The sample size calculations for the initial survey were used to determine the number of required respondents to achieve a desired accuracy in the final survey results. The calculations for the survey were based on a desired eight percent margin of error for each type of county-level responder organization and an assumed 70 to 80 percent survey response rate. Based on a dichotomous (i.e., yes/no) question, an initial sample of 200 of each type of responder organization will yield approximately 140 responses, which will result in the desired margin of error under the additional conservative assumption that 50 percent of the population would answer yes to the question.

Planning the sample size for such a relatively large margin of error reflected the intended use of the survey as a means of checking and evaluating the general conclusions of the Advisory Panel and as a way of ensuring that a wide cross-section of the local response community had input into the Advisory Panel’s deliberative process.

For the census of State-level organizations, calculation of the margin of error, under the assumption that not all organizations replied to the survey, is still relevant. With a dichotomous question and an assumed 70 to 80 percent response rate, and correcting for the finite size of the population (there are only 50 states), the resulting margin of error is very similar to the county-level organizations’ - between 7 and 10 percent.

TAB 5—RESPONSE RATES

This appendix presents the number of surveys sent in Waves I and II, the number of surveys returned in each wave, and the resulting response rate for all respondent groups, including local, regional, and state respondents.

Current Status of the Surveys

As shown in Table 1, the organizations surveyed in Waves I and II included at the local-level law enforcement agencies, fire departments, emergency medical services, offices of emergency management, public health departments, and hospitals; at the state-level, the organizations surveyed included state emergency medical services agencies, state offices of emergency management, and state public health departments.

Table 1 also shows the current status of the first and second surveys. For the first survey (Wave I), in all 1,687 organizations were surveyed including 150 at the state-level and 1,526 at the local and regional levels.²⁴⁷ Our response rate for these organizations was high. Two of every three organizations that received the initial survey completed and returned it for an overall response rate of 65 percent. A few performed considerably better, including state public health departments and combination fire departments, whose response rates exceeded 80 percent. A few of the more difficult to survey populations, with additional effort, only exceeded 50 percent response rates: volunteer fire departments, hospitals and local/regional responding EMS. In each case, however, the response rates were exceptional when compared to rates achieved with these organizations in other survey efforts.

The resulting sample of survey respondents in Wave I was representative of local and state responders both geographically and across the different emergency response and health disciplines. Surveys were received from every state in the union and the District of Columbia. Each region of the country was well represented and the final results can be generalized to all state and local response organizations nationwide.²⁴⁸

²⁴⁷ Washington, DC was also sent all three State-level surveys, and State-level OEM and public health surveys were sent to the U.S. territories of Puerto Rico, Guam, Virgin Islands, and Northern Mariana's Islands.

²⁴⁸ For more detailed information regarding the initial sample and response rates, please refer to Appendix G-5, Third Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, December 15, 2001.

Table 1.
Current Status of the Surveys and Response Rates for Waves I and II

Local Response Organizations	Wave I (2001)		Wave II (2002)	
	Number of Organizations Surveyed	Response Rate	Number of Organizations Surveyed	Response Rate
Public Health	199	74%	149	67%
Law Enforcement	208	71%	148	70%
OEM	202	71%	145	73%
Fire Department*	443	68%	300	69%
Hospital	208	51%	114	67%
Local/Regional EMS	230	48%	124	66%
State Organizations				
OEM	51	78%	40	85%
EMS	51	63%	41	61%
Public Health	51	80%	42	60%
Total/Overall Rate	1,643	65%	1,096	69%

*Includes paid, combination, and volunteer fire service organizations.

**Wave I response rate includes completed surveys returned prior to September 11, 2001. Adjustments were made to the total number surveyed in Wave II to include the 29 organizations that returned their Wave I survey just after September 11, 2001.

For the second survey (Wave II), we followed up with those organizations that had responded in Wave I. Table 1 lists the number of organizations surveyed in Wave II and their response rates. In all, 1,096 organizations were surveyed in Wave II with an overall response rate of 69 percent. Note that the number of organizations surveyed in Wave II also included the 29 organizations that had sent their Wave I survey just after September 11, 2001. Across the different types of organizations, the response rates were 60 percent or better, with State offices of emergency management achieving a very high rate of 85 percent. Given that the second survey (Wave II) had a much shorter fielding period and was primarily a mail survey with no telephone follow-up, the high response rates achieved in Wave II we believe were largely related to the survey being conducted just prior to the anniversary of 9/11. The resulting sample of survey respondents in Wave II was representative of local and state responders geographically and across the different emergency response and health disciplines.

TAB 6-CONSTRUCTION THE SURVEY WEIGHTS

Survey weights account for differential probability of being sampled among strata and for nonresponse. These statistical adjustments allow the analysis to properly infer back to the correct local response population.

The overall survey weight applied to any respondent can be expressed as $W_{igj} = \frac{1}{P_{igj}}$, where P_{igj} is the probability that respondent i in group g (e.g., hospitals) in county j was selected and completed the survey. Because organizations were selected from within counties, this overall probability is really threefold: it depends on

- (1) the probability county j was selected in the first stage;
- (2) the probability organization i was selected from among the eligibles in group g in the second stage, given county j was selected in the first stage; and
- (3) the probability organization i completed and returned the survey, given organization i was selected.

If we call these probabilities π_j , π_{igj} , and π_{igj}^R , respectively, then the overall probability of response, which is all that is needed to calculate a particular respondent's survey weight, is just their product:

$$P_{igj} = \pi_j * \pi_{igj} * \pi_{igj}^R \quad (1)$$

The first terms above, π_j , π_{igj} , are referred to as the “probabilities of selection” and their derivation depends only on the sampling methodology employed for each group of respondents. The final term, π_{igj}^R , is an adjustment to account for the fact that some organizations asked to complete the survey were more likely than others to complete and return it. π_{igj}^R is referred to as the “probability of response”: it accounts for observed patterns of response that can be determined only after all surveys have been returned and processed. For example, we observed that, on average, hospitals in rural counties were less likely to complete and return the survey than their urban counterparts; in this case, the adjustment is necessary to ensure that rural hospitals' views are not underemphasized—simply because of differences in response rates—when results from both urban and rural hospitals are aggregated.

Please refer to Appendix G (pages G-6-1 thru G-6-5), third report of the Gilmore Commission,²⁴⁹ for a detailed description of how the right-hand side probabilities in equation (1) were derived separately for each respondent group. The separate derivations are necessary because differences in organizational structure between groups and in the data available to construct sampling frames necessitated different sampling rules. In the Appendix, Table G-6-1 provides a summary of the impact of these differences on each term in equation (1).

Note, weights were not constructed for EMS respondents, since the sample of EMS organizations is a convenience sample. Therefore, findings from the local and regional EMS samples cannot be generalized to the larger EMS population.

²⁴⁹ Third Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, December 15, 2001.

Weights also were not constructed for State-level respondents, since the state surveys are censuses, rather than randomly selected samples, and because state respondents exhibited no observable patterns of non-response.

As in Wave I, the survey weights for Wave II must reflect the probability that an organization from the larger population of organizations was selected and responded. The sampling frame for Wave II consisted of those organizations that responded to Wave I of the survey. Thus, the probability of selection for Wave II is identical to the probability of selection and response to Wave I, which is just P_{igj} from equation (1).

The overall survey weight for Wave II, is then

$$W_{igj}^{(2)} = \frac{1}{\pi_j * \pi_{igj} * \pi_{igj}^R} * \frac{1}{\pi_{igj}^{R(2)}} \quad (2)$$

where $\pi_{igj}^{R(2)}$ is the probability of response to Wave II, given selection into Wave II's sampling frame. One convenient result of the definition of the sampling frame for Wave II is an alternative interpretation for $W_{igj}^{(2)}$: it is just the probability that an organization in the general population was selected and responded to both waves of the survey.

The only additional computations required to develop survey weights for Wave II, are the non-response adjustments, $\pi_{igj}^{R(2)}$. In Wave I, our investigation of systematic patterns of non-response was limited to the set of variables available in the membership lists used to construct the original sampling frame, the only data available for both respondents and non-respondents. In Wave II, we have the additional benefit of Wave I survey data. For example, one might anticipate that Wave I respondents who indicated a "low priority" on terrorism preparedness may have been less likely to respond to Wave II. Details of this analysis appear below.

Updating the Survey Weights for Late Responders to Wave I

Twenty-nine organizations that received a Wave I survey responded to the survey after September 11, 2001. For purposes of developing estimates of the π_{igj}^R , these organizations were classified as non-respondents under the assumption that they were indeed non-respondents up until 9/11 and would have remained so absent the events of that day. The P_{igj}^R and initial set of weights for Wave I thus reflect the probability that an organization in the larger population was selected and completed a survey *prior to September 11th*. However, we anticipate that a weight that reflects the probability of responding, regardless of whether the survey was returned before or after 9/11, may be desired for certain classes of analyses, although almost certainly not analyses probing for pre/post 9/11 differences.²⁵⁰ Four sets of non-response weights were developed to accommodate this:

1. Wave I, excluding late respondents, π_{igj}^R

²⁵⁰ Analyses comparing differences between Waves I and II should use weights that count the late respondents as non-respondents. Such analyses should exclude the late respondents' Wave I responses entirely, but may include the late respondents' Wave II responses if the analysis does not rely on matched pairing of Wave I and Wave II responses.

2. Wave I, all respondents, $\pi_{igj}^{R'}$
3. Wave II, excluding late respondents to Wave I, $\pi_{igj}^{R(2)}$
4. Wave II, all respondents to Wave I, $\pi_{igj}^{R(2)'}$

The corresponding survey weights, calculated by substitution of the appropriate version of π_{igj} into equations (1) and (2) are W_{igj} , W_{igj}' , $W_{igj}^{(2)}$, and $W_{igj}^{(2)'}$.

Analysis of Non-Response to Wave II

As mentioned previously, we draw on responses to the Wave I survey to detect systematic patterns of non-response to Wave II. We do not examine all items in the Wave I survey, but instead examine those we hypothesize were correlated with the organization’s underlying interest in WMD prior to 9/11, under the assumption that this in turn is related to willingness to participate in a WMD-related research effort after 9/11. Obviously, the events of 9/11 may have increased willingness to participate in WMD research, but perhaps not differentially, conditional on prior willingness.

The following items from the Wave I questionnaire were hypothesized to be related to the probability of response to Wave II. For each variable below, we tested whether the variable and response were statistically independent. If a Chi-squared/Mann-Whitney test gave evidence of a relationship, the variable was included in the prediction equation.

- Q10:²⁵¹ likelihood of a terrorist incident in respondent’s jurisdiction or region
- Q12: occurrence of a previous terrorist incident (or hoax) in jurisdiction or region
- Q12a: occurrence of a previous terrorist incident (or hoax) involving CBRN or conventional explosives
- Q14: individual assigned specifically to WMD planning
- Q16a,c: participation in an interagency working group that addresses WMD
- Q24: organization has units specifically for WMD response
- Q25, Q28, Q31, Q36: organization’s written response plan addresses WMD
- Q40: priority rating for preparing for a WMD incident
- Q54: receipt of federal material or financial support for WMD preparedness

Coding of variables:

Q#	Variable name	CODING	Description of coding	Binary?	Groups excluded
Q10	chem., bio, rad, expl, cyber, mil	sum(I[X=3 or X=4]) /6	Fraction of incidents deemed either somewhat or very likely	No	None
Q12	inc_resp	I[inc_resp=1]	An incident did occur	Yes	None
Q12a	inc_cbr inc_expl inc_cyber inc_mil	sum(I[X=1])/4	Fraction of types of CBRN incidents that occurred	No	None
Q14	ass_wmd_plan	I[ass_wmd_plan=1]	Someone at org. is assigned to WMD planning	Yes	None
Q16a,c	grppart	I[grppart=1 and iaplan=1]	Participates in an	Yes	None

²⁵¹ Question numbers refer to the Wave I survey instrument for fire departments.

Q#	Variable name	CODING	Description of coding	Binary?	Groups excluded
	iaplan		interagency group that addresses WMD		
Q24	unitchem, unitbio, unitrad, unitycybr, unitlrg	$\text{sum}(I[X=1])/5$	Fraction of types of CBRN incidents for which special units are trained	No	Hospitals
Q25,28, 31,36	esop, esop, rsop, bsop	$I[X=1]$ (four separate measures)	Organization has a written response plan that addresses the WMD scenario	Yes	esop: hospitals, pubhlth rsop: hospitals
Q40	priority	$I[\text{priority}=1 \text{ or } \text{priority}=2]$	Spending resources to prepare for WMD is a 'high' or 'somewhat high' priority	Yes	None
Q54	<i>OEM:</i> recfedsf, recfedot , recfedn o <i>Others:</i> recfed	<i>OEM:</i> $I[\text{recfedsf}=1 \text{ or } \text{recfedot}=1]$ <i>Others:</i> $I[\text{recfed}=1]$	Received federal support for WMD preparedness	Yes	None

Unfortunately, many of these variables are missing for some respondents that completed a survey. So they could not be used as covariates since they must be present to predict each organization's probability of non-response. Therefore, for purposes of the non-response analysis only, in order to allow the variables above to be used in this analysis, a missing item was coded as 0. Our assumption is that a missing value in these variables indicates a lower level of interest in WMD in a similar way as a "negative" response to each item.

Variable Selection

Univariate tests (either chi-squared or Mann-Whitney) were used to select items from the Wave I questionnaire as candidates for inclusion in the non-response prediction equations. The Chi-Squared test was used for discrete variables and Mann-Whitney for continuous variables, none of which were normally distributed.

Tests that rejected the null hypothesis of independence from response, at a "forgiving" confidence level of 20%, are included in the prediction equation. The high confidence level was chosen because sample size is small and in light of the goal of including any variable that could potentially improve the prediction.

Discrete variables: Chi-Squared test

P-values and significance

	N	Q12	Q14	Q16ac	Q25	Q28	Q31	Q36	Q40	Q54
Fire	301	0.06	0.06	0.33	0.01	0.50	0.90	0.13	0.27	0.34
Hosp	114	-- ^a	0.08	0.09	--	0.89	0.11	--	0.18	0.69
Law	148	0.05	0.19	0.06	0.47	0.63	0.46	0.90	0.66	0.35
OEM	145	0.03	0.86	0.80	0.18	0.80	0.34	0.16	0.91	0.24
PubHlth	152	0.07	0.26	0.79	--	0.21	0.86	0.68	0.11	0.83

* = p-value ≤ 20%

^a No variation: no hospital reported a previous incident

Continuous variables: Mann-Whitney two-sample test for difference of medians between responders and non-responders)

P-values and significance

	N	Q10	Q12a	Q24
Fire	301	0.05	0.04	0.51
Hosp	114	0.22	0.01	--
Law	148	0.96	0.23	0.30
OEM	145	0.11	0.37	0.24
PubHlth	152	0.70	0.05	0.89

* = p-value ≤ 20%

All variables included in the non-response estimation for Wave I were tested using similar methods and included non-response estimation for Wave II using the same criteria described above. Model results are shown below.

Prediction Models

The Hosmer-Lemeshow test statistic for goodness-of-fit of the prediction equation is presented in the tables shown on the following two pages.

Estimated Coefficients for Nonresponse Models, Wave II(Dependent Variable is Response=1)

Including Late Respondents to Wave I

	Law Enforcement	Fire Departments	Hospitals	Public Health Departments	OEMs
County-level variables:					
<i>region1</i>	--	--	1.04	0.40	--
<i>region2</i>	--	--	--	-0.69	--
<i>region3</i>	--	--	--	--	--
<i>region4</i>	--	0.38	1.04	-0.35	0.55
<i>pop</i>	--	0.00	0.00	--	--
<i>pop_small</i> [†]	--	--	--	--	--
<i>pop_med</i>	-0.79	-0.22	--	--	-1.03
<i>pop_big</i>	--	--	--	-0.46	--
<i>dens_small</i>	--	--	--	--	--
<i>urban</i>	-0.41	-0.29	0.66	-0.04	-0.83
Organizational variables:					
<i>vol</i>	--	-0.70	--	--	--
<i>combo</i>	--	0.39	--	--	--
<i>hospital beds</i>	--	--	-0.001	--	--
Wave I Questionnaire variables:					
Q10	--	--	0.01	--	-1.51
Q12	0.80	0.28	--	-0.05	-0.91
Q12a	--	--	5.25	-1.58	--
Q14	0.03	0.13	--	--	--
Q16ac	0.52	--	0.35	--	--
Q24	--	--	--	--	--
Q25	--	0.60	--	--	0.73
Q28	--	--	--	--	--
Q31	--	--	--	--	--
Q36	--	--	0.42	--	0.42
Q40	--	--	0.31	0.75	--
β_{g0}	1.29	0.87	-0.43	0.56	2.48
N^*	148	301	114	152	145
Pseudo-R ²	0.05	0.07	0.13	0.07	0.12
Hosmer-Lemeshow	0.76	0.68	0.65	0.72	0.99
p-value					

[†] *pop_small* and *dens_small* are indicators set to 1 when the county's population, or population density, respectively, are less than the 25th percentile. *pop_med* is set to 1 when the county's population is less than the median county population.

*Observations in the nonresponse model include organizations drawn from the two-stage random sample and purposively added "sensitized" organizations; a small number of observations were excluded from some models due to incomplete data in the datasets used to construct the sampling frame.

^{a)}--" indicates that the variable was excluded from the model.

Excluding Late Respondents to Wave I

	Law Enforcement	Fire Departments	Hospitals	Public Health Departments	OEMs
County-level variables:					
<i>region1</i>	--	--	-0.41	0.33	--
<i>region2</i>	--	--	0.72	-0.75	--
<i>region3</i>	--	--	--	--	--
<i>region4</i>	--	0.36	--	-0.42	0.60
<i>pop</i>	--	0.00	0.00	--	--
<i>pop_small</i> ^f	--	--	--	--	--
<i>pop_med</i>	-0.73	-0.24	--	--	-0.78
<i>pop_big</i>	--	--	--	-0.50	--
<i>dens_small</i>	--	--	--	--	--
<i>urban</i>	-0.35	-0.29	0.67	-0.03	-0.85
Organizational variables:					
<i>vol</i>	--	-0.68	--	--	--
<i>combo</i>	--	0.39	--	--	--
<i>hospital_beds</i>	--	--	-0.001	--	--
Wave I Questionnaire variables:					
Q10	--	--	--	--	--
Q12	0.77	0.27	--	0.07	-1.18
Q12a	--	--	4.50	-1.66	--
Q14	0.03	0.13	--	--	--
Q16ac	0.50	--	0.21	--	--
Q24	--	--	--	--	--
Q25	--	0.59	--	--	0.44
Q28	--	--	--	--	--
Q31	--	--	0.44	--	--
Q36	--	-0.17	--	--	0.34
Q40	--	--	0.68	0.73	--
β_{q0}	1.23	0.89	-0.34	0.59	2.15
N	147	300	105	150	142
Pseudo-R ²	0.05	0.07	0.15	0.06	0.09
Hosmer-Lemeshow p-value	0.93	0.74	0.32	0.57	0.09

TAB 7—SURVEY COMMENTS

This TAB presents the written comments received from respondents to the FWMDPPS II survey, organized by respondent group.

Law Enforcement

“Our small (13,366 population, 16½ sq. miles) bedroom community has no industry or commercial activities other than 10 resorts that cater to a national and international clientele. Therefore, we did not face a greatly increased risk after 9/11. Our major challenges were:

1. Jittery citizens, especially related to a local synagogue—the need to have information and a plan as well as tell them about what we have.
2. Increased call load: suspicious vehicles, persons and situations, possible “anthrax” items in the mail.
3. Increased flow of information and intelligence, and increased number of meetings related to terrorism, WMD, etc.

Fortunately, we had a totally new emergency management plan (less than a year old) prepared with the help of County Emergency Management, and had already scheduled an exercise for Dec. 2001/Jan. 2002.”

“We have a unit to plan everyday events. They are not picked for their subject matter expertise (SME) nor are trained to plan for large scale disasters or attacks.” [In reference to Survey Question 8: Does your organization have any individuals specifically assigned (full-time or part-time) to do emergency management or response planning?²⁵² “It is a No Priority or “Necessary Evil,” low priority.” [In reference to Survey Question 26a: How high a priority is it for your organization to spend resources preparing for the type of WMD incident you selected in Question 19?] “A scattered “Hey, you” mentality happened with no organization and either ignoring or ignorance of existing plans. Training concerns have been identified but not bought into.” [In reference to Survey Question 34a: Since September 11th, 2001, has your organization increased (or shifted over) the number of staff dedicated to addressing emergency preparedness for WMD incidents?] “Training concerns have been identified, however, no priority or a low priority has been given. No funding is available and a limited number of resources allowed.” [In reference to Survey Question 36: Since September 11th, 2001, has your organization developed, or are you in the process of developing, any unit(s) specially trained and equipped to respond to WMD incidents?] “Our department has just gone through a command change from chief down. This may change attitude.” “The city will not provide a budget for a response.” “Our Department has a “What’s the odds of it happening here” attitude and therefore, we will handle it when it happens.” [In reference to Survey Question 12: Does this interagency disaster preparedness committee, task force, or working group address planning for WMD incidents, specifically?]

“Unknown what substance was in container, suspects ran with container and remain unidentified.” [In reference to Survey Question 3: Since September 11th, 2001, did any of these terrorist incidents involve the use (or threat of use) of the following?] “Have numerous working groups for different issues. Military National Guard and FEMA involved in Chemical Depot Working Group.” [In reference to Survey Question 11c: Please indicate which organizations in your region regularly participate in this interagency disaster preparedness committee, task force, or working group.] “City Fire Department runs on off-site frequency than the other response agencies.” [In reference to Survey Question 30: Has your organization had communications interoperability problems in the past 5 years with any of the following agencies in your jurisdiction?]

1. “Bag containing explosives (unnamed) under interstate bridge.

²⁵² Question numbers listed refer to the specific version of the survey instrument for each type of organization.

2. Pipe bomb located in northern portion of county during time 21 year old placing explosives in mailboxes. Known that suspect came through county.
3. Suspicious male contacted by other agency below reservoir dam with laptop computer. Reported later that 2nd male had been discovered prior to Sept. 11, 2001, near reservoir area, also with laptop computer.”

[In reference to Survey Question 2: Since September 11th, 2001, have any incidents of terrorism (including hoaxes) occurred, been attempted, or threatened within your jurisdiction or region that required a response by your organization?]

“Following Sept. 11th our Department was inundated with suspicious powder calls that was extremely taxing on our resources. Local agencies need federal funding for equipment. More training and coordination with federal agencies. Lack of information sharing from federal agencies.”

“We rely heavily on the Fire Department personnel in controlling and securing Haz/Mat, bio, chem., etc., incidents. The Fire Department belongs to a task force for first responders.”

“We are a small town of 1,100 people.”

“The area we live in is “small town America,” 6,800 people within the city limits of City X. I feel funding from the federal level would increase our safety from future threats such as the railroad system moving through the center of 1st an Main St., City X. The chemicals trains carry would be an easy target that would cripple a small town with limited resources. Also, City X has just started a commercial section in town and an energy plant has just been built and with funding we possible could foresee and improve upon security issues.”

“Lack of personnel is a continual problem in our department.”

“Being a part of the chief law enforcement agency in the county, I have observed an increase of 100% Federal Officers/agencies. Our budget is being cut w/no increased funding for manpower or equipment. Doesn’t it make sense to give additional dollars to the agency that knows the needs, vulnerabilities, and people of the area?”

“This county has a major railroad line running through it. In the past 5 yrs., we have experienced 3 train derailments, with one causing a partial evacuation due to the possible release of chemical agents. The geographical location of this area greatly limits the ability to respond in a timely manner, should a terrorist act of sabotage occur. Small, poorly financed rural communities cannot prepare adequately, and money from grants is usually awarded to larger cities that agree to provide coverage. Nearest city to our location, 200 miles w/a 5 hr. response time. The rural area of eastern State X, in which our county lies, has been left out of most of our states emergency response plans due to our area being a low population, “low threat” area. I strongly disagree with the outlook from our state officials and offices. Our outer bank is a mecca for tourists, which inflates our area’s population to the size of some of our larger cities. We are 15 minutes to 45 minutes max away from several naval and coast guard bases, and a nuclear power plant. “Just because of a state-line as a boundary, this should not limit our area to training, equipment, or funds to combat terrorism or WMD incidents!”

“As a local police Department, our budget has been severely impacted by a \$2 million budget deficit in our state. No resource funding for equipment or training ref WMD is available locally.”

“Being that we are a village with a population of between 2000 and 3000 people, and the fact that we are not in what would be considered an ideal terrorist attack location, we haven’t changed anything in our

organization. Another strong reason for not changing anything within our organization is due to financial problems.”

“I believe we should get more information—before news media does. It seems police are the last to know and the first to get a call!! Fax us -- Phone us – before newspapers so we can at least know what is going on.”

“I define “most important” in Q19 as meaning the type of WMD attack we would most likely encounter. Our agency is part of the greater metropolitan area and is adjacent to the airport. At this point, I think we are more likely to see a WMD incident involving explosives, therefore, it is the most important. I think, however, that it is simply a matter of time before a WMD biological or chemical attack occurs. If it happened here, that would suddenly become the most important event because we would be almost completely unprepared for it!”

“We had the advantage of having a major international sporting event during the time period in question. This gave access to training and resources that would not usually have been available.”

“The federal funds are being distributed to the wrong organization and not where they can be best used.”

“Small departments (approx. 100) such as ours are without budgets to provide staff, training, and equipment to go beyond our day-to-day needs.”

“We are a city of about 3,500 people, with a police department of nine total. We have a volunteer fire department and volunteer ambulance corp. We are on in a very rural area. The state highway runs through town and we have numerous bridges in the area that connect both ends of town. 6,000 service population. Run our 911 and dispatch center. No funding for anything. Providing basis service.”

“Answers were based on regional considerations as well as local. Our agency is located close to several potential targets to include: military installations to include nuclear sub base; leading technological companies; seaports; international airport; several world headquarters. We are also in an area subject to frequent earthquakes and other seismic activity. Answers are also based on “since September 11th” wording.”

Paid Fire Departments

“Money is slow in coming out and access to it is very limited. We should focus on making operational areas prepared first! Local areas will each participate in the operational area program. We all have a role to play, but first response is very under-funded and trained. We need increased resources in personnel, equipment and enhanced federal response for extended incidents. We need emergency management on a full time basis. Increased funding to assist in developing plans that are coordinated and seamless.”

“I am willing to assist in any way to improve the response to terrorist events.”

“We need manpower, equipment and training. Small departments are struggling to keep pace with everything. Without the support staff, it is difficult to get organized.”

“Training is an integral part of WMD. Funds need to get down to the less populated areas as well for equipment and training. Most funding so far seems to be centered around our population centers, however, areas approximately 50 to 75 miles outside these population areas are not well trained and the potential for WMD is still high but with the possibility of more disastrous consequences.”

“Many of the federal funds address local municipalities, however, ignore contractors who protect federal sites. We are a federal contractor for the Department of Energy (DoE) and receive our budget as overhead funding from science funds. We are typically not eligible for any federal funding, including fire funds.”

“Our city’s division of fire had been aware of WMD and terrorism threats in this country prior to 9-11-01. We had a few personnel attend WMD or terrorism awareness training. Since 9/11, fire personnel have trained all of our police officers and public works maintenance personnel in H/M awareness and terrorism awareness. We have had personnel attend training in regional radiological events and in State X for WMD training, post 9/11 and paid by federal grants. I personally attended a public works terrorism preparedness seminar in July 2002, paid for by a Department of Justice (DoJ) grant.”

“Federal funding would be best used to allow for increased staffing for general disasters including WMD. The fire service is inherently fairly well prepared to cope with large-scale problems. We know how to take charge with IMS and when and where to get resources. The problem is during this period of bad economy. We need the bodies to enable us to mitigate problems. The training for WMD is getting blown way out of proportion. It is a modification to our current knowledge and training of HazMat and large scale incidents.”

“These surveys always make us chief officers feel like we are not doing enough toward the area of weapons of mass destruction. The truth of the matter is there is not enough money or time for a small fire Department to accomplish it all, but we will keep swinging and pray that it will never happen.”

“Further guidance and support is needed for private (industry) emergency response teams and departments. Funds are limited from within industry to improve security and emergency response. Industry emergency responders are being called upon more frequently to provide mutual aid. However, funding is always an issue.”

“Lack of funding for additional training and FTEs is major concern.”

“The fire service business is extremely diverse. Today, it is a misnomer to be called a “fire service department,” when in reality, we respond to a wide range of emergencies. These emergencies include fire, natural disasters, man-made disasters, medical responses, hazardous materials responses, elevated rescues, confined space rescues, high-angle rescues, water rescues, public education, code enforcement, and the list goes on and on. Because of this diverse mission statement, we also deal in probabilities as opposed to possibilities. I agree that there is a remote possibility that there may be a Weapons of Mass Destruction event in one or more of the small towns in America. There is also a possibility that I will win the lottery, but it is unlikely. If I am wrong, however, and there is a WMD event in a small town in America, I can assure you that it will immediately escalate into a Federal Response by our military community. I don’t know how prepared they are but if they are not, I can assure you that it is not for lack of funding when compared to the budgets of small fire department. The small town fire department will respond with their very limited resources and they will become cannon fodder and specimens for the next federal responding units to analyze before they make their entry. With that being said, let’s take a look at the probabilities in the fire service. It is not only probable, but rather it is an absolute fact that the burden on the fire service will increase due to the wide range of responses and services provided by these

departments. Another fact is that there will be fewer and fewer trained people to offer a response. Volunteer fire department rosters are dwindling. Paid professional fire department personnel are not being added proportionate to their service increases. In the final analysis, I believe that the Federal Government has failed to see the forest for the trees. They are providing millions of dollars for WMD responses that will probably never occur. This money will fund training that will be forgotten and equipment that will likely never be used. The opportunist who will capitalize on this panic frenzy will be eternally grateful as they sell snake oil computer programs and high tech trinkets to gullible fire departments and the federal government will pick up the tab. As a matter of fact, I'm thinking of my own gimmick to contribute to the pandemonium and enhance my retirement fund, but I digress. If the Federal Government wants to invest wisely in the fire service in this country, and get real value for their buck, then I offer the following suggestions:

1. WMD events are going to be far better managed and handled with a properly trained, adequately equipped military response. Invest their money in that area with only a minimal investment in the small fire departments proportionate to the results that they can expect to obtain in a WMD event.
2. Deal with the realities. The fire service is in desperate need of manpower. Let the Federal Government offer the same manpower grants for the fire service that they have offered for years to the police departments. All the plans, training, equipment, and gimmicks will be of no use if there is nobody there to use them.
3. Finally, give to those who you rely on the most. Anytime there is an emergency of any type, the first people to respond are firefighters. When a scene is brought under control and it is found to have been a criminal act, then the police assume responsibility, but only after the event has been brought under control by the firefighters. I have found that when someone needs rescue or property saved, they are not immediately concerned with who is responsible or if retribution is going to be assessed. They want the situation to be brought under control and that is what the fire service does. Therefore, if we are going to continue to first call on the fire service for help, then let's first offer to them any available financial aid.

In conclusion, I am very sorry if I have offended you with my personal comments and observations, but you did ask for them. I just feel that if we are not going to invest government dollars wisely with regard to the fire service, then let's just give the money to someone else. Just like we have been doing for the last 100 years. As always, we'll continue doing the best we can with what we've got. I hope our best is enough."

"It is true that we received a wake up call on 9-11-01. It is also true that a "knee jerk reaction" occurred and those who were not supporters or Nunn-Lugar, were now not only converts, but raving fanatical anti-terrorists. The brave soldiers, sailors, marines and fire fighters who lost their lives are truly heroes. Congressmen like X and Y are also heroes. They supported Nunn-Lugar, they warned us of the dangers ahead; they helped the first responders and had all Americans in their minds when they sought to protect us from the "Forces of Evil." These men are also true heroes. When states were required to make assessments, the effort made since 1997 to September 2001 were not examined by local officials and previous effort was disregarded. The work of those who participated in early preparation was ignored, like the voice of these patriots.

Volunteer Fire Departments

"Our Department is in a remote area. No cities or town are within 30 miles, very small population. Mostly forest, now 50% burned up. We are a very small Department without resources to go out of our area. No major concerns except one river and one power line."

"Our Fire Protection District is in rural part of the State and except for the interstate highway through the district, we do not anticipate ourselves becoming a specific target for terrorism or WMD incidents."

“We need additional funding and grants.”

“We are a small volunteer department. We don’t have funds to finance basic needs. We can’t afford to purchase items for WMD incidents.”

“We are in need of funds for equipment, trucks, as the area funds are very low. Also, we have one of the largest egg farms in the U.S. along with several dairy farms coming into the area. The two are very important to the population of the U.S.”

“We are a volunteer organization - TIME-FUNDING EQUIPMENT. Our people are dedicated and try to learn all they can to be prepared for all/any emergency. Being 20-30 minutes away from other responding agencies such as EMS-Hazmat police, our department must handle any response to WMD or any emergency. We have an interstate highway going through our response area. We know that all types of WMDs go through our area and any mishap can cause us multiple problems. Therefore, we try to concentrate on command and security of scene until greater help arrives. With funding and equipment we could be much better.”

“Our town is small (population 9,000) with limited resources. We do, however, have the possibility of an attack in our response area. For example, there are two large chemical plants 3 miles to our west, 2) a navy installation nearby, 3) a shipping goes right by our town, and 4) we have very large offshore drilling platform fabricators. I do not believe our town itself would be targeted, but the facilities listed above could very well be. When (or if) federal money for training, equipment, etc., is passed out, don’t forget the small towns.”

Combination Fire Departments

“Our department operates on a limited budget as I’m sure most of the country does. However, in our community, we have seen very little, if any, economic growth over the past five years. It is a very high priority for us to prepare for the current threat potential that exists. We are located adjoining a military base, so we feel that a definite threat possibility is there. However, due to our already depleted budget, we have been unable to shift any funds toward this goal.”

“Our department is contracted to provide services to an industrial park. Within this area are several defense contractors. It is my belief, as well as other Chiefs, that our end of the pecking order will never see any monies.”

“The most beneficial issue that could be addressed to help my organization would be funding to hire two to three emergency service technicians to address our current demand and emergency preparedness and terrorism needs. Additional money for training, equipment, communications, etc., is great, but it would be much more effective and beneficial to balance the additional training/workload with adequate personnel and staffing to manage and implement it.”

“Member of state committee on terrorism, of local terrorism working group, and of early warning group.”

“Our agency’s concern regarding WMD is an event happening south of us at a nuclear power plant or natural gas operated power generation plant and an event aimed at a state parks department-operated international tourist destination. An attempt on any of these would involve our agency.”

“Although there is a threat of WMD incident in our district, it is far more likely that we would respond mutual aid to another district. Currently we lack the basic training and equipment needed for such a response.”

“Since 9/11, Public Safety Agencies and representatives from city, county and state park have formed a planning group. This group coordinates and plans for integrated responses to major incidents. The group meets every two weeks and works to smooth out communications problems and standard operating procedures between the fire departments, police agencies, the emergency management agency, the hospital, and the departments of public works.”

“We are a small rural community with limited funds. I do believe these incidents can happen anywhere, but funds have to be allocated for the daily tasks. There are no funds left here after our everyday needs.”

“In late October, we will be involved with a multi-agency WMD drill that will involve approximately 50 area-wide agencies.”

“We have not had any type of training beyond the basic “Emergency Response to Terrorism.” Even with more defined training, the cost of equipment would be out of our reach financially.”

“We are mostly a residential and rural fire protection district. We operate at the operations level for HazMat and related incidents and summon regional specialty response teams. I believe all the uproar about communications inoperability is unjustified. I don’t want all the “non-fire/reserve” agencies at the scene operating on fire frequencies, nor do I belong in theirs. Each agency needs a high-ranking representative at the command post. We communicate face to face there and each direct our own resources on our own frequencies.”

“Sources of funding that may be available. Is there surplus military equipment?”

“The need for funding in small town America is just as great as the large metropolitan areas. Don’t leave us out when making your plans.”

“We need more equipment and radios that will work with the WMD teams in our area.”

“The Fire Protection District is chartered under a revised statute of our state laws, for the purpose of providing fire protection. Emergency medical service is provided by another countywide EMS political/taxing agency. Our fire protection district budget is derived from local properties taxes and hence is limited. This limited budget is barely able to provide equipment and training for our growing population in the 370 sq. mile district. There is insufficient resources, funds, equipment or manpower, to add WMD response capability. This task can only be accomplished by infusion of a large, continuous amount of outside funding and equipment.”

“WMD issues need to be intertwined with all of the other hazards. Funding is a major stumbling block for our area. Major transportation routes, major hospital, and other surrounding areas emergency management and fire service are low on local jurisdictions. Police seem to be getting money but do not or will not work with the Fire Service.”

“We have met with County and State representatives for law enforcement, health, Fire mutual aid, EMS mutual aid, State emergency management coordinator, but no Federal representatives. No training, or exercises, has resulted.”

“The questions make it look like we are making no efforts. All our extra WMD funds come through the County Emergency Management to us.”

“Spending resources preparing for a WMD incident is low priority due to very limited resources.”

“There is a need to fund additional personnel. Equipment is good but you have to have people to donate the equipment.”

“Most WMD incidents involve us doing things we already are trained to do. However, they now involve a new set of hazards. Recognition training, equipment to identify the hazards present and an [illegible] inoperable communications system are our greatest needs. We, of course, will need some additional PPE and decontamination equipment, as well. We believe our greatest threat is still conventional explosives/structural collapse type scenarios.

I had the opportunity to serve as on one of the national incident management teams sent by FEMA to the WTC site after the attack. It is my view that substantially more emphasis needs to be placed on unified command and the effective use of incident management. Teams to assist jurisdictions with coordinating such complex incidents.”

County Emergency Medical Services

“A lot of the questions dealt with after 9/11/2001. We had done a lot of the planning and training in August of 2001, so there was no need to readdress the issues and problems that were identified at that time.”

“There are no funding sources directly available to an organization as ours. We are a privately operated, for-profit company that has a long-term contract to provide emergency paramedic services and ambulance transport to County X. Other divisions of our company are similarly contracted with numerous other counties and each of us have been shut out of federal and state funding even though we serve an important role and are an integral component of any WMD response in our jurisdictions. Indeed, if a WMD event occurs in this region, but is outside of a contracted city, those WMDs would likely not respond (first responsibility is to protect their own cities), but our crews and ambulances would be sent as mutual aid EMS. We would benefit from funding to better prepare, since we cross city and jurisdictional boundaries.”

“Thanks for another survey. Some funding that escapes the state and federal bureaucracy would now be nice. Eventually, even some misdirected funds for actual preparedness and response is better than needs assessing into oblivion.”

“A good start has been made with WMD classes in the area, but I feel most of our areas are very under funded to carry sample protective equipment that should be available, i.e. personal alert monitors, better turn out gear, SCBAs, etc. Fire Departments are all given grants for this equipment. Private and EMS organizations perform many of the same tasks or will be asked to perform the same tasks, and we have to come up with our own funding. EMS organizations need federal assistance for preparedness also. I feel we are moving in the right direction, but are very far behind and have a long way to go before we are prepared for any WMD incident.”

“We have personnel who want to take the training, but we lack the funding to complete this training. We do not have any equipment to combat this threat or protect our personnel. I am sorry to report that we are no better prepared than before Sept. 11, 2001. Our funding from county government has been cut by \$30,000 since 1999. Our area has major interstates, highways, railways, and water treatment facilities. We also have two hydroelectric dams that I feel could be targets. We need to be better prepared, but to achieve this, funding is needed.”

“We are a small two ambulance rural EMS service. WMD is not a direct concern since we are a low-risk target. We may be called upon to send one of our two units to assist another area if an attack occurred in another part of the region. WMD is not a priority for us as with the cutbacks by insurance providers for EMS. We are happy to survive. If funding were available, we would not turn it away. However, it would probably be better spent in an urban setting. We are approximately 20 miles from a nuclear power plant so radiation is our biggest concern.”

“Department of Justice (DoJ) money has not been released to counties for purchases. Until this happens, we will not be able to purchase any WMD related equipment. This has also led to prices used for funding studies to be outdated when monies are released.”

“Funding for training and equipment is our biggest problem.”

“We are small. Federal money needs to be more accessible for rural groups.”

Regional Emergency Medical Services

“In our State, we use the standard emergency management system and the hospital incident command system. I feel we are much more organized than other parts of the county. The equipment/training is at local fire departments and hospitals – local Public Health departments. Need grants for private and public hospitals and health organization-skilled nursing homes. In my opinion, grants distributed by private health companies are more effective than government agencies. See tobacco dollars/leave out the essentials of health response.”

“The funding needs to trickle down to educate and train the services and personnel who will be on the front line of any WMD incident.”

“We need assistance/funding in the following areas: (1) Dedicated person for WMD; (2) Plan review/amend; and (3) Replace communications system.”

“Local [illegible] departments need access to timely laboratory analysis of suspected biological substances (environmental samples).

Local [illegible] departments need timely, accurate and consistent information from state Department of Health and the CDC regarding information to be disseminated to public at large and to community-based healthcare providers.

Hospitals must be included as “first responders” for funding/training/equipment, etc.”

“MMRS was executed quite well. However, there is no similar initiative in our State. Department of Justice (DoJ) money is primarily used for equipment. There is no statewide plan or capability.

Other issues include:

1. Hospitals are underfunded.
2.differences between emergency management and health,
3. lack of relationships with our state colleagues,
4. no single state agency has really “stepped forward”,
5. radiological management (health aspects is weak),
6. state OEM has not spoken to X MMRS.”

“County EMS – County Health – County OEM - have recently conducted a very successful distribution of KI (potassium iodide) tablets at the fire department for the nuclear plant in our county. We used a drive-through line distribution and distributed over 112,000 tabs in seven days. Actual time that each vehicle spent in line to receive tabs was 3 minutes.”

“I am with a state health department regional office that licenses and provides technical assistance to EMS and a liaison to our OEM (state).”

“My office serves a mainly volunteer population of EMS (95% vol.). We identified a great need to plan/train and dedicate programs toward preparedness for a WMD, but we are so poorly funded we cannot hire the staff needed or [illegible] beyond our basin. EMT – paramedic programs to address the need – My office works with 43 EMS agencies here in our State. In order to really get prepared, I need to have a full-time person working with this project – at least \$50,000 more for this position. Through grants, I may be able to get training programs but without the dedicated manpower, I am not able to move along. We have a nuclear full plant here as well as busy highways leading to a major metropolitan area and a port nearby at City X. I think money is sent to one fire department, a career agency, but most of my area is volunteer. What are we to do or are we on the expendable list? After your last survey, I hoped to see some local contact to help us get better prepared but not so. Are my answers to this just added to the number of responses—NOT a list you may be helping?”

“We are a regional council that represents EMS, fire Department, hospitals and other responders, so it was difficult to answer some questions such as, do we (our organization) stock equipment? No, our organization doesn’t but the agencies that belong to our organization do. For the most part, I tried to answer as our organization representative as a whole.”

City/county Offices of Emergency Management

“We had formed an anti-terrorism task force and had begun additional terrorism training six months prior to Sept. 11th, 2001.”

“Our department (emergency management) is not a response agency, per se, so questions about equipment were answered as though I was answering on a regional basis, unless the question specifically alluded to our Department”

“I really don’t believe that our highest priorities as a nation involve conflicts over resources, equipment, funding, training, etc. Our problems deal with the inability of organizations to work together under a standard system. We train in the incident command system (ICS) and so we use it, but when an emergency occurs we depart from ICS and use a modified version of it that fails us in the end. Furthermore, our federal partners don’t use the same systems or technology. FEMA, USFS, FBI all have different ways to manage an incident. They set poor examples for states and local governments to follow because we confuse each other of how to manage an emergency. The bottom line is that we could be a lot more efficient with the resources and training we already have if we used them properly.”

“Federal, state guidance and planning remain fragmented. Federal and state agencies are starting to do a better job of integrating their efforts but they are too slow to extend the integration down to the county level. Funds must reach the county level. However, there must be accountability on how those funds are used. The feds and the state should set consistent goals and scopes of work and the counties must show how their expenditure of funds will meet and support those goals and how they will accomplish the scope of work. However, locals must be included in the development of the goals and scope of work.”

“Our town is a community in the Deep South. Realistically, terrorism and WMD do not pose a direct threat. However, we have a large port nearby that is surrounded by chemical plants. Our threat is HazMat regardless of how initiated. A terrorist with any sense wouldn’t make much of an international impact in such a remote area, but regardless of the ignition source, 3.5 billion pounds of hazardous materials (HazMat) would make one hell of a statement. I believe WMD focus would be best directed towards our major metropolitan areas and then to our more rural, less concentrated areas. If you were a bad guy wanting to make an international statement, where would you target? The major 10 US Cities.”

“The events of 9/11 have emphasized funding for WMD events, i.e., chemical, biological and radiological, which deserves funding. My concern is that, if we look back at Oklahoma, WTC I and II, the problems and difficulties revealed in after-action reports have not been given due attention. Interoperability of communications, mandated use of ICS, emergency planning and emergency operations centers capable of coordinating multi-jurisdictional and multi-agency responses. We are not learning from our mistakes and correcting them before we attempt to run into other areas that have not yet occurred. Funding should be channeled into those areas that have already been identified and corrected before we train and prepare for hypothetical threats. Thank you for including our community into your survey. Money has been allocated to large metropolitan areas, but smaller communities need to be prepared as well.”

“Since the events of Sept. 11th, there has been a huge increase in funds allocated by the government at the Federal and State levels. A large amount of this was intended to go to Emergency Services personnel at the local level for purchase of equipment, improved training, etc. So far, we have seen almost no evidence of this at least in smaller counties such as mine. We have been asked to fill out stacks of paperwork by one group the State hired and were told that this group was going to decide what type of equipment we needed. How people sitting in an office a thousand miles away can tell what we need is almost laughable. At one point, they have told us they were going to be sending PPE Level A suits to the local fire, EMS department. Many of these small volunteer departments don’t even have decent turn-out gear and few if any SCBA, but they didn’t bother to ask questions about things like that. When you build something you start at the foundation, not from the top down. It appears that this money is going to be soaked up by agencies and bureaucrats at the Federal and State-levels and the actual responders are going to get little benefit from all the billions of dollars that the American people think is being spent to protect them.”

“Monies needed for emergency operations center upgrades and planning manpower – We also need increased funding for Incident Command training and infield incident command post equipment!!! Mandatory education for elected officials and administrators to understand WMD issues and planning requirements. Funding for regional response efforts is needed as well.”

“I would like to comment on the funding/positions that have been created since 9/11/02. Although no one is exempt from risk of terrorism, rural areas are less likely to be targeted. We struggle to maintain a decent local emergency management program, yet we now have a local “Bioterrorism Coordinator” – a full-time, heavily funded position!! Funding is available for HazMat teams, Health Department, etc., but severely lacking to assist with our local EM programs. We are at a much higher risk of a chemical spill or fire at a local firm or fruit processing plant than of a WMD or bioterrorism event, and yet there has been no increase in funding for the local programs. This is a problem that needs to be addressed.”

“Our emergency management organization at the county level is staffed entirely with personnel that have other full time jobs and do emergency management as a second job.

The DOJ grant monies received during 2002 had highly restrictive parameters. The monies could not be spent on what we thought was most important at our level.”

“Lack of funding, slow pace of available funds distribution, state involved in handling funds are all problematic. Total lack of recognition and funding support for agencies such as ours that developed WMD capability prior to Sept. 11th.”

“DOJ funding is providing equipment for two WMD teams in our area (\$500-600K). Nearly 70 WMD trainees developed (awareness, ops, tech, EMS Tech, ICS, Hospital Provider). Regional planning started for eighteen-county area. Two meetings held so far.”

“There are a couple of things that smaller jurisdiction in the wide-open spaces face. One, we cover large areas - our County is 43,040 sq. miles. Its topography is plains and mountain ranges (5 different ones). Within this area, there are many missile sites (maybe missile sites and military installation should be included on the survey as they could be a prime target for terrorism). Our County has a populace of between 12,500 and 13,000. Most fire departments (14 in all) are volunteers – little or no budgets. All ambulance services are volunteers (5). Law enforcement staff that covers this vast area is less than 20 to cover 24 –7. Disaster and Emergency Service is a staff of one full time and one volunteer with no other staff. We dispatch for three counties. The mountains in these counties often make radio communications difficult. Being small rural counties, there is no budget to cover the cost of additional repeaters (generally, grants don’t cover this kind of equipment). Warning systems throughout the county are also an identified need at the time of a disaster. We have little to no way of warning the people we should be protecting. We recently installed a NOAA station, but that does not cover the entire county (again because of the mountains). The county east of us has nothing for a warning system. I would also like to let you know that our radio station cannot reach everyone in the county and is the only station within 130 miles. It seems these two elements: Communications – repeaters and warning systems are two items that might be included in the survey. We have plans, do exercises, have mutual aids in place, some training and now, to be better prepared, we need help with some tools to help deliver what we have in place or all the plans, exercises, mutual aids and training will do little good. We need to let responders and the public know what actions to take.”

“Our County is in the process of getting a HazMat team equipped and ready to operate by the end of 2002. We have applied for equipment from my state. Some of the Federal money is starting to get down to the local levels. More money and/or equipment and training are needed. Money is needed to help promote full scale drills.”

“All activities undertaken by our County since 9/11/01, have been done so from the standpoint that any planning and training completed will improve our ability to manage all types of disasters, not just WMD events. It is therefore difficult to say that 9/11 served as a catalyst for anything other than increased interest and participation by partner agencies.”

“Local funding is inadequate. Funding is needed to back bill for training classes for all personnel: EMS, Fire, Dispatch, Police. We must find a way to fund overtime to send personnel to places for training, and to do a better job of training local personnel.”

“We need more staff and money!”

“We are a rural county with a small risk of WMD. We are poorly funded. We have ALL volunteer firefighters and EMS. We have an ancient communication system. We need funding to train personnel for basic response. We need funding to purchase basic equipment. An incident that would be considered “everyday” in a larger county could be devastating to our county. It does not serve any practical purpose to train for WMD until we have the basics. Please send \$\$\$\$\$. God help us if a terrorist does strike our county!”

“In our region and surrounding areas, we are handicapped due to a lack of funding. Another factor, the city CEOs (District Heads) and county personnel do not fully understand the serious situation that we could be in. I find it fighting an uphill battle, especially with the City personnel--the County personnel we can work with.”

“Lack of funding is the primary difficulty we face. Many times, the funding we do receive is so tied down that we cannot use it to address the most critical needs first. Most of our needs involve infrastructure and physical assets. We have good people that are able to perform well, if they have the necessary supplies to do so.”

“The DOJ monies have not yet been distributed. Our funding will be hampered due to costs rising after price changes went into effect.”

One, as an initial [illegible] City, many of the activities this survey covered were undertaken well prior to 9/11/01. Rather than initiate, we only continue to develop and improve. Two, based upon lessons learned from NYC as reported in the New York Times, government needs to focus not on what type of command system exists, but how well it is understood/practiced/exercised. That is where problems exist. Too many first responders do not operate in this environment on a regular basis to have achieved a comfort level—that and an attitude in these services—the “we know it all.” Regarding regional response, you need to examine local/state government structure as it aids or hinders regional cooperation/coordination.”

“In our rural community, we have much more threats from natural disasters and highway/rail hazardous materials incidents than we have from WMD incidents.”

“I would like to see funds made available to upgrade communication equipment to our local radio equipment.”

“Emergency management orgs need budget increases to pay for staff time expended on grant management. DOJ, FEMA, EPA, USPH grants need to be “holistic” in that they need to pay for grant administration, equipment, training on the equipment, maintenance and calibration of equipment. Equipment alone does not add capability. Matching grants do not work! Local governments do not have resources to match. Federal government needs one standard grant format, that is, holistic (see second paragraph above) and has same rules. Unified command needs to be mandated for local, state, federal organizations to use in response to WMD attack, e.g., especially FBI.”

“WMD has played a large role within the emergency management office. This office has had to shift many of its resources toward WMD and terrorism with no direct assistance in funding to do this. In fact, even regular funding for emergency management from the Federal Government (EMPG) will be reduced over the next few years in the amount of \$6,000. Our State does not directly enhance EMPG with any additional funds. I think that EMPG (Emergency Management Planning Grant) funds are severely low and do not offset the cost to perform emergency management or WMD.”

“We are trying to train and equip for larger incidents as a result of 9-11. However, for us (a small rural community) a large-scale incident such as a passenger plane crash will require significant outside assistance.”

Hospitals

“This tiny hospital is entirely dependent on local law enforcement and from plans (lip service only) for small events other than fire—the dominant threat. While I am personally aware of ongoing issues re terrorism/WMD casualty from state and other counties, there is no awareness, no planning in material preparedness locally. We are a rural county with a widely dispersed population of 16,000. Local health department is a joke at the state-level (“Oh, that one.”) No alternate site is designated for mass event triage. We are utterly dependent on other’s stockpile of any antidote other than our round of snake anti-venoms. We have no [illegible] pressure area and no clean air area in the hospital. In defense, most existing plans are rather unrealistic. Run-off water contamination; smallpox, etc.”

“The CEO and other community leaders provided the resources to do a bio-terrorism drill at a local industry. We have rivers and the ocean as a good path for a terrorist to enter here, so we simulated a bomb at a local seafood plant. We learned a lot and still have many needs for education and other resources in preparation for a WMD.”

“We do not have surveillance mechanisms of/for biologics.
We do not have enough equipment to do mass decontamination for chemical exposure.
We do not have equipment for detection of radiation.”

“Since 9/11, our disaster preparedness committee has worked aggressively at addressing all emergency management policies and procedures: Much of the education for the entire medical center is yet to come. This fall, the following has all been addressed since 9/11:

1. HazMat/Decon: increased supplies and training, Jan 2002 – March 2002.
 2. Bio-terrorism plan: completed July 2002 – training scheduled this fall.
 3. Adoption of HEICS: began in committee in June 2002 to be implemented this fall.
 4. Lockdown policy, credentialing policy, all emergency plans revised, etc.”
-

“If additional funding is not provided to hospitals, the cost of WMD preparedness will be difficult if not impossible to meet.”

“We are a rural medical facility. Financial survival is difficult in the current climate. Funding is not available for training (we can barely provide staff nurses and doctors for an ER shift) let alone pay overtime to train all the staff. We held a training day and broke staff away from their jobs for 15-20 minutes to give familiarization training with the decontamination shower, masks, and suits. Most staff are not interested and do not want to be involved. I fill the position as Safety and Security Manager. I have no budget, 3.8FTE to man security (152 hours for a 168 hour week) and little comprehension or buy in from Sr. management.”

“Our committee began preparation prior to 9/11/01. We have continued the efforts with regard to preparedness and have used the JCAHO format.”

City/County Public Health

“Aside from scheduled exercises, anthrax scares and have provided us with multiple opportunities to exercise some of our response capabilities, working with fire – HAZMAT, local law enforcement, FBI and involving private citizens, businesses, hospitals, regional airport and more. So much response planning is currently going on that there will certainly be changes in our preparedness within the next few weeks to months. This questionnaire does not capture the fluid nature of the current status very well.”

“Direct Federal-Local agency grants, e.g., original cities MMRS program with deliverables are the most successful in enhancing WMD response “where the rubber meets the road” i.e., providing services to patients or exposed individuals quickly. Grants that preclude hiring personnel, or are too small to provide a position are of little use to us. Due to Federal —> State —> Local cost shifting in health care, our office has lost 2 of 11 positions e.g. we are more than busy with our other mandated programs (EMS regulation, disaster prep, etc.) We can’t take on the administration of a grant as an additional duty. We need to increase capacity in our hospital and EMS systems – grants alone are too small. Reimbursement mechanisms, e.g., Medicare, need to be adjusted to provide more emphasis on emergency care and less on end-of-life care to prepare for a WMD incident! Let’s all pay for our own Viagra and let the government and insurance payors pay for more emergency department beds, and RN training programs!”

“Federal bioterrorism funders (CDC to State to Local health department) is just now (Sept. 2002) resulting in ability to recruit and hire dedicated staff for bioterrorism preparedness.”

“I work at the district level of public health, covering thirteen counties in the northeastern corner of the state. I answered most questions from both the district and largest county in the district perspectives. In our State, the Emergency Management Agency and county-level Emergency Management Agency Director have historically had the lead role in responding to emergencies of all types, and public health has always had a supporting role. We are slowly and steadily making progress toward the goal of integrating the responses of those two entities so that public health assumes a leading role in certain decision making in the case of WMD agents. Questions about preparedness to handle victims do not directly apply to public health our State even though we are a health organization, because most of our health care is preventive in nature. However, we do have responsibilities related to managing communicable diseases, food borne outbreaks and the like. Even here, we would not necessarily or even usually be the one to treat patients directly. At the district-level, we have been authorized to hire a Bioterrorism Coordinator, a Staff Development Specialist/Assistant BT Coordinator, and a Risk Communication Specialist. We are currently recruiting for those positions.”

“Staff time remains an issue in planning preparedness. Most positions funded by categorical grants. So far, state and federal dollars prohibit expenditures for staff overtime for training. Communication systems remain an issue if conventional methods (phone, fax, computer) systems are compromised. Requests for radio equipment denied by State. Difficult to find balance between efforts for preparedness vs. other public health priorities in shrinking resource environment.”

“I appreciate the interest of the committee and hope this information will have value. One area the survey did not cover which I think has value is the funding sources of local health departments and its effect on emergency planning. Our department receives most of its funding in federal, categorical grants. None of these grants have any appreciation of WMDs and how it affects a given population. This hinders our department’s abilities to plan and train its staff. Almost all of our staff is tied to categorical funding sources which limits the time our department has at its disposal.”

“Small local health departments are concerned about lack of emergency power sources. So far, no funding has been allocated for this need. In our area, power outages are frequent and most certainly would happen in any major emergency. We would need backup power for lighting, heating/AC, refrigeration and computer links to state (IDPH).”

“I am the Health Officer for a small county health department. I am involved with our LEPC. Our department has only one sanitarian and one full time nurse. Our county has an active HAZMAT team but they are not prepared for biological incidents.”

“I have completed numerous surveys for assessing preparedness. Someone should compile these or collaborate with each other!”

“We still do not have enough time or staff to do everything we are expected to do. Funds for additional staff have become available, but we have not yet been able to hire anyone. We are working on our plan, but do not yet have a plan to answer “yes” to your questions. Similarly, training is in the planning stages but has not yet been completed. A radiological tabletop exercise is due in November. It would be really helpful if someone would prepare a cookie-cutter, fill in the blanks manual for small agencies that do not have access to experts on a usual basis. Flip charts with step-by-step response instructions would be wonderful. In this subject area, CDC needs to behave more like FEMA, and develop and issue uniform standardized procedures for local agencies to adapt and follow, rather than just giving general advice and leaving each agency to develop whatever it comes up with.”

“We do not have local or state budget to do any of this work. FY 02-03 state funds are supposed to be available for personal computers and other office equipment to start planning for this area.”

“Prior training of health Department staff with medical and hospital personnel, prior to Sept. 11, 2001, was a great help. Prior tabletop exercises with EOL was a great help. E-mail from CDC and state agencies was very good sources of information. Meeting with clergy in area helped some to calm public.”

“Contrary to some popular beliefs, these survey requests (multiple) can be a real pain to respond to at times. However, if organizations like yours also took the time and trouble to provide copies of any summarized reports to participating agencies, it would not only improve the overall participation rate, but hopefully also provide these agencies with important feedback information. Thanks for your consideration in this matter!”

“I personally feel that a lot of the funding for Emergency Preparedness will not be spent in the most effective manner.”

“Have not heard from the planners they hired to help our county. We have just been doing all of this on our own with help from all the other organizations.”

“While our County did not have anthrax “hoaxes” there were “scares” around the County related to white powder. September 11, 2001, incidents have motivated us to refocus on our Emergency planning and preparedness. We have renewed partnerships on the local state and national level (e.g. State Department of Health and Centers for Disease Control).”

“The CDC grant funds directly given to Health helped us to finally play a viable role and to fund health response needs. Everybody else wants us to find things but we were never before recognized as a partner.”

“From a Health Department’s local perspective, the critical issues are 1) private cooperation and 2) “dual use” of new resources. At the Federal level, guidance regarding public/private health response tends to be inadequate, overly prescriptive, or otherwise unhelpful. Similarly, there is an emphasis on creating special resources and responses that fail to a) take advantage of existing health resources, and b) ignore community members’ usual information-seeking and care-seeking behavior. As a result, there is a tendency to produce systems that create lower than necessary quality/intensity of care, and will exacerbate community members’ reasonable fears and anxieties.”

“Major issue for our organization – a local health department – is limited resources. We have almost no surge capacity for CPI investigations, limited communications infrastructure and support. City and state have planned no added funds for WMD preparedness, and very little of federal, city and CDC funding will reach the local level in our State. Our sole source of WMD preparedness funding was the MMRS program, which was received 1998-2000 – funds no longer available. Access to lab support is not ideal— State public health lab is 30-40 miles away and that lab has very limited infrastructure and capacity.”

“Please note you refer to events of 9/11 but many health care system changes were related to experience with anthrax. In general, our systems had GOOD plans for dealing with explosions and airplane crashes, but POOR plans for identifying and responding to biological incidents. Also, some of your questions are hard to answer if not a “hospital” or conventional medical care facility. We are a local health department with very different responsibilities and staffing than a hospital.”

“Some of the questions were difficult to answer accurately due to the local and regional perspective and were not clear.”

“Community members struggle with difficulty in realizing bioterrorism is a criminal activity. They repeatedly forget the role of law enforcement, medical examiner in handling crime scene, victims, lab samples, dead bodies. We need help with this. Waiting for national smallpox policy is worrisome as know we will have to implement it and possibly within short timeline. Anthrax victim –Victim support services not tuned in to these people as crime victims. Helpful when aggressively lobbied, but need education in serving this group. Appreciate Department of Defense (DoD) grant/state \$ supporting new staff.”

“Surge capacity of local public health agencies is crucial. Budgetary cutbacks in state programs cause loss of personnel (public health nurses/environmental health specialists) that would be critically needed in a health emergency.”

“In our rolling hills, communication is an overwhelming problem. Will communication ever be provided via satellite (e.g.) by Federal Govt. for use by local govt. to alleviate the communication problems we have from each organization having different equipment, most of which is too weak (but affordable) to communicate with?”

State Office of Emergency Management

“There is not a federal recommendation for a single system of communications. There are many approved but this will only enhance the problem because local agencies will order what they want off-the-shelf but not all will order the same.”

“Federal funding to upgrade state/local emergency operation centers through FEMA. FEMA placed a 50/50 match requirement on EOC funding although congressional language in the FY-2002 supplemental did not allow for such a requirement. States are not economically able to meet any match and will be forced to not participate in EOC grants.”

“Lack of personnel and resources hinder organizations’ ability to properly address this issue in a timely manner.”

“This survey does address local jurisdictions in our State well. However, states positions are not considered. Results could be skewed by that oversight.”

“Updated/created checklists for 911 call-takers to answer questions for “white powder” incidents, etc.” [In reference to Survey Question 18: Since September 11th, 2001, has your organization updated or newly developed a written response plan to specifically address...[CBRN]?” All the ‘billions’ supposedly coming? Of course we “anticipate.” But state budgets are going down. FEMA anticipating FY02 supplemental and FY03, didn’t ask for TCMPA for the states – that is a cut in 100% money.” [In reference to Survey Question 43: With the start of the new fiscal year, does your organization anticipate any additional increases in its today budget to address WMD preparedness?] You have to apply – how can you not. The challenge will be the staff needed to work these programs.” [In reference to Survey Question 44: Compared with other needs that may be facing your organization, would you consider applying for Federal funding to prepare for WMD as a low, medium, or high priority – assuming such funding were to become available specifically for organizations like yours?]

State Emergency Medical Services

“In our State, Emergency Medical Services is a division of the state emergency management agency. We coordinate statewide resources for emergency medical response. We do not own EMS resources; we will rely on EMS services for transportation resources. We have begun planning regional EMS and mass casualty cache capabilities. We are coordinating with Department of Health on surge capacity for out-of-hospital as well as in-hospital patient influx. I would like to see EMS be an active part of the syndrome surveillance system for early recognition and detection.”

“My job is primarily regulatory and coordinating in nature. I have taken the lead role in our state in developing a communication and training network for EMS providers, which allows them to be recognized as a key player in Response Planning. I am responsible for the state EMS and trauma plan, therefore, my office is developing a set of protocols for bioterrorism response. These will be disseminated as operational guides statewide. I sit on the HRSA state hospital preparedness program and the DCD Public Health Infrastructure Advisory committee and the states Homeland Security Committee. Our challenges are making sure that the EMS presence is felt and their voice heard on such matters as surveillance, notification, medical treatment protocols, decontamination and emergency transport. As I answer this, I am sitting in on the first of a series of EMS sponsored DOJ training courses—this one is “Emergency Response to Domestic Biological Incidents” which is being taught by an EXCELLENT national faculty who are here representing X University’s Counter-Terrorism Academy which is part of a multi state consortium. We are fortunate to have these resources at our disposal as well as a National Guard Weapons of Mass Destruction Unit. Both agencies have offered FREE training and guidance to EMS and Public Health. Thank you for the opportunity to participate.”

“The EMS office is a bureau within the State Department of Health. It is not a field response unit. Some of the PPE questions were therefore not applicable. In terms of LEPC, some of the district and regional offices are closely working with these elements. The State EMS office works with the State emergency management agency.”

State Public Health

“With the introduction of increased federal funding, we saw a REDUCTION of State funding.” [In reference to Survey Question 40: With the start of the new fiscal year, does your state health department anticipate any additional increases in funding from your State government to address bioterrorism and/or WMD preparedness?]

“Most activities are in the planning or early implementation stage. Activities were dependent on receipt of federal funds.”

“Many questions say since 9/11. We were part of the Oct/NN anthrax events so some activities for preparedness were put on hold (exercises) – others accelerated. Questions regarding written plan. We do not yet have an official, comprehensive written plan. This does not mean we do not have a plan or could not mount a response.”

“State fiscal issues and Lame Duck session make it difficult to hire staff. Lack of staff makes it difficult to support local public health departments and health care providers. We have a great plan to move forward and prepare the entire state health care system—we just need the staff to carry out. Local health departments are frustrated and feel money would best be directed at them. At this time, fragmented local planning will not build a State System of preparedness.”

Our State, like many others, is just establishing an infrastructure to administer the federal resources available for bioterrorism preparedness and response. Many of the issues will be quickly addressed once staff is hired. Goals and objectives have been identified. Now it is time to begin activities to accomplish them.”

“Resources and legislative authority to respond to radiological events no longer within State Health Department role. Statewide critical need for resources to enhance wireless communications – do not necessarily need frequency [illegible] – need upgraded equipment. Hardware is mostly 20 years old.

APPENDIX E– THE TERRORIST THREAT TO U.S. AGRICULTURE

Introduction

Over the past decade, the United States has moved to substantially increase their ability to detect, prevent and respond to terrorist threats and incidents. This focus, which has involved substantial financial outlays, has fed into an increasingly well-protected public infrastructure throughout much of the developed world where, at a minimum, effectively developed vulnerability-threat analyses have been used to maximize both anti-terrorist contingencies and consequence management modalities. More specifically, investments in preparedness, training and response have helped with the development of viable incident command structures that now span the ambit of potential terrorist attacks, from conventional bombings to more “exotic” biological, chemical, radiological and nuclear incidents.

Agriculture is one area that has received very little attention in this regard, however. In terms of accurate threat assessments and consequence management procedures, the industry continues to exist as a notable exception to the wide-ranging emphasis that has been given to critical infrastructure protection (CIP) in this country; indeed the sector has yet to be included under the provisions of Presidential Decision Directive 63 (PDD-63), which specifies critical nodes deemed to be vulnerable to terrorist attack or disruption.²⁵³

This paper aims to expand the current debate on domestic homeland security by assessing the vulnerabilities of agriculture and the food chain to a deliberate act of biological terrorism. It first briefly discusses the methods used to complete the analysis and the current state of research on the topic. The study then outlines the general economic importance of agriculture to the U.S. economy before going on to assess the vulnerabilities in the sector, the capabilities that are needed to exploit these vulnerabilities and the likely ramifications that would result from a successful attack.²⁵⁴ The paper considers the question why terrorists have yet to embrace agricultural assaults as a specific modus operandi and concludes with some tentative recommendations for the U.S. policymaking community.

²⁵³In May 1998, the Clinton administration passed into law PDD-63 on Critical Infrastructure Protection. The initiative designates eight physical and cyber-based systems essential to the minimum operations of the economy and government that are deemed vulnerable to possible terrorist attack. Such sectors are taken to include: banking and finance; transportation; electricity, gas and oil; telecommunications; emergency law enforcement; government services; emergency fire; public health service; and the water supply. It should be noted that Agriculture and Food Safety is included as one of eight sub-groups of the National Security Council’s (NSC) Weapons of Mass Destruction Preparedness Group, which was established in 1998 under the auspices of Presidential Decision Directive 62 (PDD-62), “Combating Terrorism.” The USDA serves as chair of this sub-group. However, as Parker notes, the Department is a relative latecomer to the national security and defense structure and presently lacks sufficient visibility and influence to champion greater federal attention to countering biological attacks against agriculture (which is, itself, invariably overshadowed by other terrorism-related issues). See Henry Parker *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat*. McNair Paper 65 (Washington DC: Institute for National Strategic Studies, National Defense University, March 2002), 30. For details on PDD-63 see White Paper, *The Clinton Administration’s Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, May 22, 1998.

²⁵⁴For the purposes of this paper, agroterrorism will be defined as the deliberate introduction of a disease agent, either against livestock or into the food chain, for purposes of undermining stability and/or generating fear. Depending on the disease agent and vector chosen, it is a tactic that can be used either to generate cause mass socio-economic disruption or as a form of direct human aggression.

RESEARCH METHODS AND THE CURRENT ACADEMIC LITERATURE ON THREATS TO AGRICULTURE AND THE FOOD CHAIN

The research for this study proceeded in four main stages. First, a qualitative and conceptual framework for analysing threats to agriculture and the general food chain was established, based primarily on the author's own background in the subject matter and previous writings. Second, interviews were conducted with members of the agricultural policy community to determine the specific make-up of the US farm-to-table food continuum, its interface with developments that are currently taking place in national critical infrastructure protection (CIP) and the factors that are serving to exacerbate its vulnerability to deliberate disruption and sabotage. Third, the costs and wider consequences of agricultural disasters were delineated by examining real-life instances that have occurred in other parts of the world, utilizing a taxonomy that measured "seriousness" in terms of wider public health, economic security and political stability impacts. Finally, the principal findings from the primary field work and secondary research were integrated and incorporated into the initial conceptual framework to generate a final document.

The issue of agricultural insecurity is one that difficult to address in a systematic manner, both on account of the highly dispersed nature of the sector and the fact that many of the process evaluations used to assess vulnerability cannot be validated empirically. Nonetheless, the analysis contained in this analysis is useful to the extent that it highlights critical nodes and key outcomes that can be used to delineate priority areas for future research. In addition, it helps to enrich a body of work that, in comparison to other areas of CIP, remains relatively thin and limited in scope.²⁵⁵

THE IMPORTANCE OF THE AGRICULTURAL SECTOR TO THE US ECONOMY

Agriculture and the general food industry remain critical to the social, economic and, arguably, political stability of the United States. One in eight people work in an occupation that is directly supported by the industry, which makes it the country's largest single employer. Cattle and dairy farmers alone earn between \$50 billion and \$54 billion a year through meat and milk sales,²⁵⁶ while roughly \$50 billion is raised every year through farm-related exports. In 2001, food production constituted 9.7 percent of the U.S. GDP, generating cash receipts in excess of \$991 billion.²⁵⁷ Agriculture's share of commodities sold overseas is also more than double that of other industries, which gives the sector major importance in terms of positively impacting on Washington's balance of trade.²⁵⁸ Added to this is a solid research foundation and well-developed infrastructure, which has made the U.S. farming system the most efficient

²⁵⁵ Comprehensive analyses in the field are currently limited to the following published and unpublished works: Parker, *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat*; Peter Chalk, *The Political Terrorist Threat to Agriculture and Livestock* (Santa Monica: RAND, DRR-2187-OSD, September 1999); Paul Rogers, Simon Whitby and Malcolm Dando, "Biological Warfare against Crops," *Scientific American* 280/6 (1999); Norm Steele, "US Agricultural Productivity, Concentration and Vulnerability to Biological Weapons," unclassified Defense Intelligence Assessment for the Department of Defense Futures Intelligence Program, January 14, 2000; Agricultural Research Service, "Econoterrorism, a.k.a. Agricultural Bioterrorism or Asymmetric Use of Biological Weapons," unclassified briefing, US Department of Agriculture (USDA), February 28, 2000; Simon Whitby and Paul Rogers, "Anti-Crop Biological Warfare – Implications of the Iraqi and US Programs," *Defense Analysis* 13/3 (1999); Terrance Wilson, "A Review of Agroterrorism, Biological Crimes and Biological Warfare Targeting Animal Agriculture," draft manuscript, 2001; John Gordon and Steen Bech-Nielsen, "Biological Terrorism: A Direct Threat to Our Livestock Industry," *Military Medicine* 151/7 (1986); and Agricultural Research Service, *Agriculture's Defense Against Biological Warfare and Other Outbreaks* (Washington DC: USDA, December 1961).

²⁵⁶ Overall livestock sales in 2001 were in excess of \$108 billion. See "Agro-Terrorism Still a Credible Threat," *The Wall Street Journal*, December 26 2001.

²⁵⁷ Bureau of Economic Analysis, "Gross Domestic Product: First Quarter 2002 (Advance)," available at on-line at <http://www.bea.doc.gov/bea/newsrel/gdp102a.htm>.

²⁵⁸ Ellen Shell, "Could Mad Cow Disease Happen Here?" *The Atlantic Monthly* 282/3 (1998): 92; "Stockgrowers Warned of Terrorism Threat," *The Chieftain*, August 19, 1999.

and productive in the world. Indeed, Americans spend less than eleven percent of their disposable income on food, compared with a global average of around 20 to 30 percent.²⁵⁹

Although significant, these figures represent only a fraction of the total value of agriculture to the U.S. economy, as they do not take into account allied industries and services such as suppliers, transporters, distributors and restaurant chains. According to the Department of Commerce (DoC), the economic multiplier effect of exported farm commodities alone is in the region of 20:1.²⁶⁰ The down stream effect of a major act of sabotage against this highly valuable industry would be enormous, creating a fiscal “tidal wave” that would be felt by all these sectors, impacting, ultimately, on the American consumer him/herself.²⁶¹

THE VULNERABILITY OF U.S AGRICULTURE TO ATTACK

For a variety of reasons, the U.S. agricultural sector remains acutely vulnerable to attack. Critical susceptibilities stem from six main factors:

- The concentrated and intensive nature of contemporary U.S. farming practices;
- The increased disease susceptibility of livestock;
- A general lack of farm/food-related security and surveillance;
- An inefficient passive disease reporting system that is further hampered by a lack of trust between regulators and producers;
- Veterinarian training that tends not to emphasize foreign animal diseases (FADs) or large-scale husbandry; and
- A prevailing focus on aggregate, rather than individual animal statistics.

The Concentrated and Intensive Nature of Contemporary U.S. Farming Practices

Agriculture is both a large-scale and extremely intensive business in the United States. Most dairies in the country can be expected to contain at least 1,500 lactating cows at any one time, with some of the largest facilities housing upwards of 10,000 animals.²⁶² In California, one of the U.S’ most important agricultural states, there are 31 feedlots with a capacity of at least 15,000 head of cattle (1996 figure), the bulk of which are concentrated in just two regions: the Imperial Valley (average size between 30,000 and 50,000 head) and the San Joaquin Valley (average size between 15,000 and 20,000 head).²⁶³ Unlike humans, these animals exist as highly concentrated populations and tend to be bred and reared in extreme proximity to one another. The outbreak of a contagious disease at one of these facilities would be very difficult to contain, especially if it was airborne in nature, and could well necessitate the wholesale destruction of all exposed livestock – a formidable and highly expensive task.²⁶⁴

²⁵⁹ Wilson et al., “A Review of Agroterrorism, Biological Crimes and Biological Warfare Targeting Animal Agriculture,” 22.

²⁶⁰ Parker, *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat*, 11

²⁶¹ Wilson et al., “A Review of Agroterrorism, Biological Crimes and Biological Warfare Targeting Animal Agriculture,” 22.

²⁶² See, for instance, Siobhan Gorman, “Bioterror Down on the Farm,” *National Journal* 27 (July 1999): 812; and Agricultural Research Service (ARS), *Agriculture’s Defenses Against Biological Warfare and Other Outbreaks*, 2. Currently, roughly three quarters of all dairy commodities are concentrated in the hands of less than ten percent of the country’s cow and calf production facilities.

²⁶³ Javier Ekboir, *The Potential Impact of Foot and Mouth Disease in California. The Role and Contribution of Animal Health Surveillance and Monitoring Services* (Davis, CA: Agricultural Issues Center, 1999), 26, 29.

²⁶⁴ The level at which eradication becomes unfeasible depends on available technical, economic and political limits, but is generally considered to be around one percent. In other words, once one percent of a susceptible population has been infected with an animal disease, eradication is no longer deemed to be advantageous.

Problems are further exacerbated by the widespread and rapid dissemination of animals from farm to market (a pound of meat generally travels about 1000 miles on the hoof before it reaches the dinner table). One representative survey of U.S. barn auctions showed that between 20 and 30 percent of cattle were regularly consigned to non-slaughter destinations at least 40 kilometres from their original point of purchase and in many cases had crossed several states within 36 to 48 hours of leaving the sales yard. Economic forces and the out-sourcing of traditional agricultural activities have added considerably to this movement. In the Californian dairy industry, for instance, there has been a trend toward the contract rearing of replacement heifers by large-scale calf-raising operations, many of which typically manage between 10,000 and 40,000 animals from as many as 80 separate farms. In most cases, calves are transported daily to rearing sites and each week weaned calves are returned back to their original dairies.²⁶⁵ The rapid transfer of animals in the U.S. livestock industry necessarily increases the risk that pathogenic agents will spread well beyond the locus of specific outbreaks before health officials become aware that a problem is at hand.

The Increased Disease Susceptibility of Livestock

U.S. livestock has become progressively more disease prone in recent years as a result of husbandry changes and biotechnic innovations that have been introduced to increase the quality and quantity of meat production as well as to meet the specific requirements of individual vendors. These modifications, which have included everything from sterilization programs to dehorning, branding, crowding and hormone injections, have combined to dramatically elevate the stress levels of exposed animals. This has both lowered their natural tolerance to contagious pathogenic agents as well as increased the “volume” of bacteria that would normally be shed in the event of an infection.²⁶⁶

Over-use and misuse of antibiotics to treat common ailments has further exacerbated these effects, resulting in a process of “pathogenic natural selection” that has led to the emergence of ever more powerful, resilient and resistant disease strains.²⁶⁷ This process of microbial evolution has left livestock acutely vulnerable to a whole new generation of genetically modified “super bugs” that either offer resistance to several families of antibiotics (or dozens of individual drugs) at any one time or confer greater powers of infectivity and virulence.²⁶⁸

Insufficient Farm/Food-Related Security and Surveillance

A deliberate act of sabotage is simply not something that the majority of the agricultural community have actively thought about, much less physically prepared to guard against. Indeed, it was not until October 1998 that the words “terrorism,” “agriculture,” and “biological weapons” were officially strung together by the USDA and used in the same conceptual sense when assessing potential vulnerabilities and threats to the industry.²⁶⁹ Farms in the U.S. have therefore tended to evolve, not surprisingly, as extremely open affairs, seldom incorporating concerted means to prevent unauthorized access or intrusion. This is

²⁶⁵ Wilson et al., “A Review Agroterrorism, Biological Crimes and Biological Warfare Targeting Animal Agriculture,” 25-26.

²⁶⁶ Comments made by Paul Effler during the “Transnational Security Threats in Asia” Conference, Honolulu, Hawaii, August 8-10, 2000.

²⁶⁷ Overuse of antibiotics constitutes a critical trigger for microbial adaptation by forcing replication of plasmid in DNA and RNA codes – the dynamic of which commands mutation under stress.

²⁶⁸ See Parker, *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat*, 13; Laurie Garrett, “The Return of Infectious Disease,” *Foreign Affairs* 75/1 (1996): 67; National Intelligence Council (NIC), *The Global Infectious Disease Threat and Its Implications for the United States*, National Intelligence Estimate 99-17D (January 2000), 23; “Wonder Drugs at Risk,” *The Washington Post*, April 19, 2001.

²⁶⁹ Comments made by U.S. Department of Agriculture (USDA) officials during the National Research Council (NRC), “National Security Implications of Advances in Biotechnology: Threats to Plants and Animals” Planning Meeting, National Academy of Sciences, Washington DC, August 1999.

especially true of outlying fields and feedlots but is also often the case with respect to centralized facilities such as milking stands.

Security at animal fairs and barn sales tends to be in equally short supply, with most bereft of any on-site surveillance or monitoring. During the 1950s and 1960s, U.S. officials staged a number of test exercises at these sites to simulate the intentional dissemination of FMD, successfully introducing mock versions of the virus at several locations without interception. According to Terence Wilson, a senior USDA liaison officer stationed at Fort Detrick's Armed Forces Medical Intelligence Center in Maryland, little has changed over the course of the intervening forty years and similar interventions would be just as possible today.²⁷⁰

Food processing and packing plants also tend to lack sufficient security and safety preparedness measures, particularly those that have proliferated at the lower and medium end of the production spectrum. Thousands of these facilities exist across the country, the vast bulk of which are characterized by lax internal quality control (typically only a fraction of the commodities originating from these plants is actually subjected to end of line testing), minimal bio-surveillance and highly transient, unscreened workforces. Entry-exit controls are inadequate (and occasionally do not exist at all) and even basic measures such as padlocking storage rooms may not be practiced. Moreover, many small-scale operations do not keep accurate records of their distribution network, meaning that it may not be possible to trace a tainted food item back to its original source of production.²⁷¹

An Inefficient Passive Disease Reporting System

Responsibility for reporting unusual disease occurrences in the U.S. lies with agricultural producers. However in many cases, communication channels between and state emergency management personnel remain underdeveloped, particularly with regards to information frameworks that clearly designate relevant regulatory agencies and primary or secondary personnel that need to be contacted in the event of a serious viral or bacterial outbreak.

Equally as important, farmers are often reluctant to quickly report outbreaks of notifiable diseases, fearing that if they do so, they will be forced to carry mass, unrecompensed depopulation measures. This reticence reflects the fact that there is, at present, no standardized and consistent system of agricultural reimbursement to compensate producers affected by pathogenic outbreaks, with all designations currently determined on a case-by-case basis. Moreover even in the event that large-scale culling is unlikely to eventuate, farmers generally do not want to invite regulators on to their premises, lest this transmits a message to the wider community of a potential problem that leads to a loss of sales and curtailment of domestic markets.²⁷²

The current operation of the U.S. animal disease reporting system does little to avail the early identification and containment of viral and bacterial infections, which is vital to any effective emergency management system. More seriously, it may actually be helping to *institutionalize* delayed and localized response modalities, which in the case of highly transmissible diseases such as FMD, could prove to be catastrophic.

Inappropriate Veterinarian and Diagnostic Training

The number of appropriately trained veterinarians capable of recognizing and treating exotic livestock diseases is rapidly declining in the U.S. In part, this reflects the smaller numbers of people actually entering veterinarian science – itself a product of the lack of educational support and financial incentive given to the discipline in the country – and the preference choices of those that do – most of who tend to

²⁷⁰ Wilson et al., “A Review Agroterrorism, Biological Crimes and Biological Warfare Targeting Animal Agriculture,” 26.

²⁷¹ Author interview, California Department of Health and Human Services (CDHHS), Sacramento, August 2000.

²⁷² Author interview, agricultural specialists, University of California at Davis, Sacramento, August 2000.

focus on domesticated pets such as dogs and cats rather than large-scale husbandry (as this is where the most money is to be made).²⁷³ Just as importantly, it is indicative of college curriculae that, in most cases, reportedly do not emphasize FADs sufficiently, with most focus directed toward diseases that are endemic to the United States itself.²⁷⁴ The overall result has been a dearth of accredited state and local veterinarians that have either a background in farm animal diagnostics or the necessary expertise to deal with “Class A” agents²⁷⁵ of the sort likely to be used in a deliberate terrorist introduction.

Focus on Aggregate as Opposed to Individual Animal Statistics

The scale of modern agriculture in the U.S. and trend towards larger herds and breeding operations has largely precluded the option of attending to animals on an individual basis. In most cases farmers are forced to regulate and monitor livestock populations by reference to aggregate statistics such as overall milk production levels. This, combined with the declining pool of accredited state and local livestock veterinarians (see above), has effectively meant that more and more animals throughout the country are currently receiving no form of comprehensive medical examination or observation. The possibility of emerging diseases being missed has, thus, emerged as an increasingly real threat.

CAPABILITY REQUIREMENTS FOR CARRYING OUT AN AGRO-TERRORIST ATTACK

What makes the vulnerabilities inherent in agriculture so worrying is that the capability requirements for exploiting these weaknesses are not significant and certainly far less than those that would be needed for a human-directed bio-attack. Several factors account for this. First, there is a large “menu” of agents to choose from, with no less than twenty Class A pathogens identified as having the potential to severely effect agricultural populations (see Table One). Most of these diseases are environmentally hardy – being able to exist for extended periods of time on organic or inorganic matter – and many are not routinely vaccinated against in the United States. Moreover, some of the most dangerous agents are readily accessible in regions close to American shores and could be smuggled into the country with little risk of detection. A case in point is FMD - the agricultural equivalent to smallpox given its highly contagious nature - which is prevalent in South America and which could be transported into the United States on the bottom of a shoe (as a manure scraping) or on a handkerchief (as absorbed vesicular fluid droplets).²⁷⁶

²⁷³ Comments made to author during the ADD DETAILS OF THE DC CONFERENCE IN MARCH 2002.

²⁷⁴ Comments made by USDA officials attending the NRC “National Security Implications of Advances in Biotechnology: Threats to Plants and Animals” Planning Meeting, Washington DC, August 1999.

²⁷⁵ Class A agents refer to those pathogens that have been identified as most threatening to livestock populations by virtue of their ability contagiousness, ability to survive in the environment, overall lethality and general availability.

²⁷⁶ Comments made during the “Agro-Terrorism: What is the Threat?” Workshop, Cornell University, Ithaca, New York, November 2000.

Table 1. Class A Animal Pathogens

PATHOGEN	MORTALITY	ZOONOTIC
Foot and mouth disease (FMD) virus	Less than 1%	No
Hog cholera	High	No
African swine fever (ASF) Virus	60-100%, depending on isolate virulence	No
Rinderpest (RP) virus	High	No
Rift Valley fever (RVF) virus	10-20% among adult populations; higher among young lambs, kids and calves	Yes
Avian influenza (AI) virus	Near 100%	Yes
Newcastle disease (ND) virus	90-100%	Yes*
Venezuelan equine encephalomyelitis (VEE) virus	50-90%	Yes
Bluetongue (BT) virus	0-50%	No
Sheep and goat pox (SGP) viruses	Near 50%, though can be as high as 95% in animals less than 1 month old	No
Aujeszky's virus	Near 100% in young animals; between 5 and 10% among older populations (except for sheep and goats where mortality remains near 100%)	No
Vesicular stomatitis (VS) virus	NEED	Yes
Lumpy skin disease (LSD) virus	Variable, depending on prevalence of insect vector	No
Heartwater (HW)	60% (cattle); 3-80% (sheep, according to species type)	No
African horse sickness (AHS) virus	70-95% (horses); 10-50% (mules, according to species type)	No
Screwworm Myiasis	Variable, depending on prevalence of insect vector	Yes
Lyssa and rabies viruses	100%	Yes
Anthrax	Near 100% for respiratory anthrax; variable for skin and intestinal versions.	Yes
Porcine reproductive and respiratory syndrome (PRRS)	Variable	No
Ornithosis	20%	Yes

Sources: Wilson et al., "A Review of Agroterrorism, Biological Crimes and Biological Warfare Targeting Animal Agriculture," 15-16; United States Animal Health Association, Foreign Animal Diseases.

*Human manifestation limited to conjunctivitis

Second, many FADs are non-zoonotic in nature meaning that they can be handled with no risk of latent or accidental (human) infection. There is, thus, no requirement on the part of the perpetrator to have an advanced understanding of animal disease epidemiology and transmission modes nor is there any need for elaborate containment procedures and equipment in the preparation of the agent. Primary diseases that could be used in this regard include FMD, rinderpest, ASF, Hog Cholera, Exotic Newcastle Disease (END, Vesicular Stomatitis (VS) and Lumpy Skin Disease Virus.²⁷⁷

Third, animal diseases can be quickly spread to affect large numbers of herds over wide geographic areas. This reflects the intensive and concentrated nature of modern farming practices in the US and the increased susceptibility of livestock to viral and bacterial infections (see above). There is, in other words,

²⁷⁷ All of these animal pathogens are currently being considered by the Ad Hoc Group of State Parties to the Biological and Toxin Weapons Convention (BTWC).

no issue of weaponization - which is frequently cited as one of the most important barriers preventing non-state offensive use of biological agents²⁷⁸ - that needs to be overcome in agricultural terrorism as the animals, themselves, become the primary vector for pathogenic transmission. Models developed by the USDA, for example, have shown that a disease such as FMD could be expected to spread to as many as 25 states in as little as five days simply through the regulated movement of animals from farm to market.²⁷⁹ If one takes into account that certain livestock consignments are unregulated, taking the form of either illegal shipments or the re-selling and switching of animals at market, then true rates of transmission could be even greater than this.

Fourth, if the objective is human deaths, the food chain offers a low-tech, yet highly conducive mechanism for disseminating toxins and bacteria such as salmonella, *e-coli* and botulism (none of which require any substantial scientific knowledge to isolate or develop). Developments in the farm-to-table food continuum have greatly increased the number of entry points for these agents, which combined with the lack of security and surveillance at many processing and packing plants, has helped to substantially augment the technical ease of orchestrating a food-borne attack. It is also worth bearing in mind that, at least at present, there are no definitive technologies which could be used at these sites to detect bio-chem contaminants in a real-time sense, meaning that authorities would only know about an attack *after* it has taken place.²⁸⁰ Possibilities for pre-emptive action are therefore highly limited.

THE IMPACT OF A MAJOR ACT OF AGRO-TERRORISM

Notwithstanding its operational ease, there would be little point in investing the time and effort to carry out attacks against livestock and the food chain if the impact of such action was not likely to be that great. However, this is where the real potential threat of agroterror comes in. The ramifications of a concerted bio-assault on the U.S. meat and food base would be far-reaching and could easily extend beyond the immediate agricultural community to affect other segments of society. It is possible to envision at least three major effects that might result.

Economic Destabilization

Perhaps one of the most immediate effects of a major act of biological agroterrorism would be to create mass economic destabilization, generating costs that could be expected to cross at least three levels. First, there would be direct economic losses resulting from containment measures and the eradication of disease-ridden livestock. The outbreak of a particularly severe case of FMD in Taiwan in 1997, for instance, immediately cost the Republic \$10 million in vaccine purchases²⁸¹ and has since necessitated government spending in excess of \$4 billion for surveillance, cleaning, disinfection and related eradication programs.²⁸² A 1994 USDA study has similarly concluded that were a disease such as ASF ever to become entrenched in the U.S., the direct financial impact over a ten-year period would be at least

²⁷⁸ A good summary of the technical constraints inherent in weaponizing biological agents can be found in Seth Carus, *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents in the 20th Century* (National Defense University, Washington DC: Center for Counterproliferation Research, 1999) 26-29.

²⁷⁹ Author interview, USDA officials, Washington DC, and Maryland, 1999-2000.

²⁸⁰ Comments made by Janet Kause during the "Bioterrorism in the United States: Calibrating the Threat" Seminar, Carnegie Endowment for International Peace, Washington DC, January 2000.

²⁸¹ Comments made during the Asia Pacific Center for Security Studies Senior Executive Course, Honolulu, Hawaii, April 22, 2002.

²⁸² Wilson et al., "A Review of Agroterrorism, Biological Crimes and Biological Warfare Targeting Animal Agriculture, 24; Parker, *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat*, 15.

\$5.4 billion.²⁸³ One commentator has estimated that the true cost of such an outbreak in today's figures could as much as three to five times higher.²⁸⁴

Second, indirect multiplier effects would accrue both from compensation paid to farmers for the destruction of agricultural commodities²⁸⁵ and revenue deficits suffered by both directly and indirectly related industries. As the 2001 outbreak of FMD illustrates, the extent of these costs can be staggering. By the year's end, well over GBP1 billion had been paid in compensation to farmers affected by mass culling operations, with losses to tourism as a result of cancellations brought about by the quarantine of farms located in or near popular holiday destinations such as the Lake District estimated to have been in the range of GBP2.5 billion.²⁸⁶

Third, international costs in the form of protective embargoes imposed by major external trading partners would manifest. One study from California, which presented eight different scenarios associated with a theoretical FMD outbreak, concluded each day of delay in instituting effective eradication and control measures would cost the state \$1 billion in trade sanctions. These projections become even more telling when one considers the legal nature of California's present export treaties, which allow overseas trading partners to automatically institute wholesale export bans in the event of *both* minor and major FAD occurrences.²⁸⁷ In effect, this means that even small-scale or, indeed, isolated disease outbreaks (both of which are easier, still, to perpetrate than more wide-spread pandemics) have the capacity to cause exorbitant, latent run-on trade effects. In this sense agroterrorism retains an enormous potential in terms of coercive economic cost: benefit ratios.

These latter considerations are equally as pertinent to deliberate product contamination. Perhaps the clearest indication of this is the Chilean grape scare of 1989. This particular incident involved a plot by anti-Pinochet extremists to lace fruit bound for the US with sodium cyanide. Although in the event only a handful of grapes were actually contaminated, import suspensions subsequently imposed by the U.S., Canada, Denmark, Germany and Hong Kong cost Chile in excess of US\$200 million in lost revenue earnings.²⁸⁸

²⁸³ See C. Renlemann and C. Spinelli, "An Economic Assessment of the Costs and Benefits of African Swine Fever Prevention," *Animal Health Insight* (Spring/Summer 1994).

²⁸⁴ Parker, *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat*, 15.

²⁸⁵ Although the U.S. has no standardized system of compensation in place, federal funds would be forthcoming in the event of a large-scale agricultural disaster such as a multi-focal outbreak of FMD.

²⁸⁶ "Farmers Paid GBP1 Bn For Culled Animals," *The Daily Telegraph* (UK), June 30, 2001; "After Foot and Mouth," *The Economist*, May 5, 2001; "Spring Returns to Rural Britain, But Not Tourists," *The Washington Post*, March 16, 2001.

²⁸⁷ Author interview, California Department of Food and Agriculture (CDFA) officials, Sacramento, September 2000. See also "Eastern Oregon Farmers Ready to Eradicate Cattle Disease Threat," *The Oregonian*, August 17, 1999.

²⁸⁸ See Ron Purver, *Chemical and Biological Terrorism: A New Threat to Public Safety*, Conflict Studies No. 295 (London: Research Institute for the Study of Conflict and Terrorism, 1996/1997), 13-14; David Rapoport, "Terrorists and Weapons of the Apocalypse," paper presented before the "Future Developments in Terrorism" Conference, Cork, Ireland, March 1999, 13-14; and "Plant Scientists Sound the Alarm on Agroterrorism," *The Philadelphia Inquirer*, September 13, 1999.

LOSS OF POLITICAL SUPPORT AND CONFIDENCE

A successful bio-attack against the U.S. agricultural sector would also serve to undermine confidence and support in State governance. Successfully releasing contagious agents against livestock would undoubtedly cause people to lose confidence in the safety of the food supply and could lead them to question the effectiveness of existing contingency planning against weapons of mass destruction in general. Although agricultural attacks are far easier to execute than civilian-directed assaults (as is pointed out above), such nuances are almost certainly going to be lost on publics who tend to cast simple assertions on complex events. People may begin to equate the ability to infect animals with an enhanced capacity to target humans, calling for greater emergency planning in cities such as Los Angeles, New York and Atlanta, more stockpiling of vaccines and increased surveillance of “high-risk” groups (which carries risks in terms of civil liberties). Critics, unfairly and with the benefit of hindsight, would almost certainly demand why the intelligence services failed to detect that an attack was imminent and why the agricultural sector was left exposed. Graphic images of diseased cows and sheep would likely be propagated by the media and highlighted as evidence of the extreme susceptibility and vulnerability of all animal life, including human beings, to deadly pathogens. The combined effect would be to initiate a chain of socio-political reactions/events, which, if not carefully managed, could fundamentally alter the relationship between citizen and government at both the state and federal levels.

The actual mechanics of dealing with an act of agricultural bioterrorism could also generate widespread public criticism. Containing a major disease outbreak would almost certainly necessitate the slaughter of hundreds of thousands of animals. The 1999 *hendra encephalitis* (HE) variant epidemic in Malaysia, for instance, led to over 800,000 pigs being shot, while the 2001 FMD outbreak in the UK had, by the end of June (the height of the epidemic), resulted in nearly 3.5 million animals being destroyed (see Table One).²⁸⁹ Euthanizing such volumes will be sure to generate widespread opposition from the general population, not to mention farmers and animal rights, particularly if culling involved the slaughter of susceptible, but non-disease showing livestock (so-called fire breaker operations – a scientifically justifiable method of virulent viral containment) and/or wildlife. The fact that the U.S. has not experienced a major cattle or sheep outbreak in the era of public television is especially important in this regard as it effectively means no visual point of reference has been available to prepare the public at large for the consequences of containing such a catastrophe. The use of government marksmen armed with high velocity bolt guns to massacre half a million head, including those that exhibited no outward sign of clinical infection, would simply not be endorsed as a legitimate form of disease containment.²⁹⁰

Table 2. Culling Operations Instituted during the UK 2001 FMD Outbreak, February to June 28

Total FMD Cases, to June 29	1,799
Animals slaughtered to June 28	3,347,000
Animals awaiting slaughter	11,000
Carcasses awaiting disposal	9,000
Total number of affected premises	8,450

Source: Department for Environment, Food and Rural Affairs

The potential political fall-out of mass eradication measures is well exemplified by the British FMD example. The measures instituted by the Blair government to try and stem the epidemic engendered significant opposition from farmers, scientists, politicians (both of who cited over-reaction) and the public, significantly undermining the domestic support base of a Labour administration that, hitherto, had

²⁸⁹ “Pig-Borne Epidemic Kills 117,” *The Sydney Morning Herald*, April 10, 1999; “Farmers Paid GBP1 bn for Culled Animals,” *The Daily Telegraph*, June 30, 2001.

²⁹⁰ Author interview, USDA officials, Washington DC, July 1999.

been relatively popular.²⁹¹ The following commentary by Simon Jenkins in the London *Times* newspaper is representative of the extreme criticism that was directed at the Blair government during the crisis:

Policy on foot and mouth disease (FMD) is now running on autopilot... Nothing in the entire history of the common agriculture policy has been so crazy. The slaughter is not declining but running at 80,000 a day... At the last estimate, 95 percent of the three to four million animals dead or awaiting death are healthy... The obscenity of the policy is said to be irrelevant “because of its success.” Yet what other industry would be allowed to protect its profits by paying soldiers with spades to kill piglets and drown lambs in streams? What other industry could get civil servants to bury cattle alive or take potshots at cows from a 60ft range? What other industry can summon teams from Whitehall to roam the lanes of the Forest Dean, as one frantic farmer telephoned me, “like Nazi stormtroopers seeking healthy sheep to kill on the authority of a map reference”? [The government] is killing healthy animals not from any concern of welfare but to help livestock exports. I cannot imagine another industry that would be protected in this appalling fashion.²⁹²

Even in the unlikely event that large-scale culling operations were accepted, the actual removal of carcasses would be just as challenging. The quickest and easiest way to dispose of contaminated animal waste is either by burying corpses in landfills covered with quicklime or by incinerating them in pits lined with burning tires. However, utilizing such methods in an ecologically “friendly” manner is only feasible if a small number of bodies need to be dealt with. Burning thousands of carcasses with rubber tires, for instance, would create a huge, smoldering open fire as well as a highly visible atmospheric pollution problem, both of which would attract widespread popular criticism. Mass burial is likely to be just as contentious, not least because of the risk it would be seen as posing to ground water supplies and the fact that it would render large areas of land essentially unusable for many years (of particular concern to heavily urbanized states). On the other hand, the longer officials prevaricate and leave diseased carcasses out in the open, the higher is the probability that they will act as a source for future infection epidemic spread – an equally unacceptable outcome.²⁹³

The USDA has attempted to come to grips with the problem of mass carcass disposal by looking at the rendering system as a possible way to deal with livestock slaughtered from quarantined farms. To test the viability of this alternative, the Service simulated an outbreak of FMD in 1998 in which destroyed animals were exposed to extreme heat,²⁹⁴ reduced and re-processed into feed meal as part of the emergency containment process. However, within one week the test system had been completely

²⁹¹ Author interview, British Broadcasting Corporation (BBC), Washington DC, March 2001.

²⁹² Simon Jenkins, “This Wretched Cult of Blood and Money,” *The Times*, May 23, 2001.

²⁹³ Corrie Brown, “Impact and Risk of Foreign and Animal Diseases,” *Vet Med Today* 208/7 1039. See also Gordon and Beech-Nielsen, “Biological Terrorism: A Direct Threat to Our Livestock Industry,” 360.

²⁹⁴ So long as high temperatures are used (above 140 degrees Celsius), there is no danger that the rendering process will result in the recycling of animal diseases as infectious agents are susceptible to heat. It is only when lower temperatures are incorporated that this risk becomes apparent. There are indications that the bovine spongiform encephalopathy (BSE) outbreak in the UK, for instance, was effectively amplified by the repeated use of recycled ruminant protein that had been subjected to temperatures considerably less than the 140-degree threshold. It has been estimated that by the early 1980s, 60 to 70 percent of British rendering plants had switched to low-temperature systems in order to reduce energy costs. For further details See Nicols Fox, *Spoiled. The Dangerous Truth about a Food Chain Gone Haywire* (New York: Basic Books, 1997), 291-31; and Shell, “Could Mad-Cow Disease Happen Here?” 97.

overwhelmed and could no longer deal with the volume of animal protein that was coming in.²⁹⁵ Following the exercise, APHIS officials concluded that the rendering system was ineffectual in terms of mass carcass disposal and that, in the event of a major disease outbreak, the only realistic way of quickly dealing with animal corpses would be through burning or burial. USDA officials have since conceded that gaining public and political acceptance of these methods, or conceptualizing viable alternatives to them, remains one of the most challenging issues currently facing the Department in terms of future emergency contingency planning.²⁹⁶

Social Instability

Beyond immediate economic and political impacts, bio-terrorist assaults against agriculture have the potential to create mass panic and could, possibly, stimulate socially disruptive rural-urban migrations. Several animal diseases are zoonotic in nature, meaning they have the ability to “jump” species and affect humans, including AI, RVF, VS and Screwworm. Should an epidemic of any one of these diseases occur in the U.S., it could have severe repercussions in terms of galvanizing a mass public scare throughout the country, particularly if human deaths actually occurred. Terrorists could use this to their advantage, allowing them to create a general atmosphere of fear and anxiety without actually having to carry out indiscriminate civilian-oriented attacks (and “accepting” all this entails in terms of attracting mass reprisals and alienating actual or potential support).

Two pathogenic outbreaks that occurred in 1999 illustrate the rapidity by which such effects can occur and extent to which zoonotic diseases can impact on the psyche of the ordinary citizen. In the first case, a new strain of the HE virus (since termed “*nipah*”) spread throughout Malaysia’s Negri Sembilan province, devastating the region’s swine population in addition to claiming the lives of 117 villagers. The outbreak, the main part of which lasted just over a month, caused thousands of people to desert their homes and abandon their livelihoods, with many fleeing as internal “environmental refugees” to shanty towns on the outskirts of Kuala Lumpur.²⁹⁷ The second instance occurred in New York City and involved an outbreak of West Nile Virus (WNV), which was apparently brought to the country by migrating birds from Africa and the Middle East. The disease, which was previously unknown to the US, quickly spread to humans, several of whom subsequently died as a result of massive heart and liver failure. A major and largely unprecedented public health scare ensued, the dimensions of which were further exacerbated by the epidemiological difficulty (at least initially) of definitively determining the pathogen’s type, source and transmission mode.²⁹⁸

A food-borne attack would do equally as well in terms of galvanizing public panic and general social instability. Because most processed food is disseminated to a “catchment” area within a matter of hours, a single case of contamination could have highly significant ramifications in terms of latent run-on effects, especially if the source of the problem was not immediately apparent and chronic or acute ailments actually ensued. The heightened state of American public anxiety post-September 11 have only

²⁹⁵ In large part, this was due to the fact that, since 1997, animal protein coming from sheep, cattle, goats, deer, elk and mink (the prime candidates for FMD) has been banned for use as feed to other ruminants and can only be given to swine and poultry. The logic behind the move is the assumption that cannibalism among species works to amplify the transmission of progressive neurological disorders such as BSE. Chicken and poultry have been exempted from the stipulations largely because the US Food and Drug Administration (FDA) contends they are not susceptible to these sorts of infectious disorders (a claim rejected by most Governments in Europe, which have banned animal rendered products to all agricultural livestock since 1996). See Fox, *Spoiled. The Dangerous Truth about a Food Chain Gone Haywire*, 329-30 and Shell, “Could Mad-Cow Disease Happen Here?” 94-96.

²⁹⁶ Author interview, USDA officials, Washington DC, July 1999.

²⁹⁷ See, for instance, “Malay Troops Slaughter Pigs in War on Virus,” *CNN Interactive World News*, March 20, 1999; “Pig Borne Epidemic Kills 117,” *The Sydney Morning Herald*, March 10, 1999.

²⁹⁸ Comments made during a special panel on West Nile Virus during the International Conference on Emerging Infectious Diseases, Atlanta, Georgia, July 2000.

exacerbated the potential for such psychological dynamics to the extent that even a handful of fatal cases could now be expected to spark severe reactions among the population at large.

The Use of Agro-Terrorism as a Form of Finance Generation/Coercive Blackmail

It should, finally, be noted that the low probability of detecting intentional biological assaults against agriculture also makes this *modus operandi* an ideal and largely risk-free way for terrorists (and criminals in general) to generate, or otherwise raise financial capital. One particularly effective way of achieving this would be to create and then exploit fluctuations on the commodity futures market. An attack that severely crippled the U.S. cattle industry, for instance, would be sure to result in a major increase in demand, and corresponding price rise for the products of the State's major beef and milk competitors. An astute perpetrator could take advantage of this by simply investing in appropriate stock shares before carrying out his/her assault. All they would then have to do is wait for the "natural" economic laws of demand and supply to take effect before cashing in on their elevated dividend premiums.²⁹⁹

The potential impact and mechanics of agroterrorism additionally gives this form of aggression a high pay-off in terms of more basic extortion and coercive blackmail. Unlike human-directed biological threats, terrorists would have the advantage of definitively establishing the credibility of their resolve by actually carrying out a large-scale livestock or food-borne attack without, thereby, attracting massive retaliation from governing entities that no longer feel they have anything left to lose. Moreover, given the enormous direct and latent damage that could be inflicted by repeat attacks, both State and Federal governments would have a strong incentive to negotiate, a key consideration in any blackmail attempt.

Biological Assaults Against Agriculture And Terrorism Modus Operandi

Despite the ease by which an act of agroterrorism could be carried out and the severe ramifications that a successful assault could elicit (especially in terms of economic and political fallout), it is unlikely to constitute a primary form of terrorist aggression. This is because such acts would probably be viewed as "too dry" in comparison with traditional tactics in the sense that they do not produce immediate, visible effects. The impact, while certainly significant, is delayed – lacking a single point of reference for the media to focus on (and highlight). More specifically, there is no drama of the sort that would flow from a suicide bombing or September 11-style attack, which is absolutely integral to the hostility and publicity that terrorists both exude and crave.³⁰⁰ In this light, it is perhaps understandable that biological attacks against agriculture have not emerged as more of a problem. Indeed since 1912, there have been a mere twelve documented cases involving the sub-state use of pathogenic agents to infect livestock or contaminate related produce. Of these, only two incidents could in any way be termed terroristic in nature: the 1984 Rajneeshee salmonella food poisoning in Oregon and the 1952 Mau Mau plant toxin incident in Kenya (see Table 3).

²⁹⁹ Personal correspondence between author and USDA officials, Washington DC, July 1999. See also

"Administration Plans to Use Plum Island to Combat Terrorism," *The New York Times*, September 21, 1999.

³⁰⁰ See, for instance, Brian Jenkins, "Future Trends in International Terrorism," in Robert Slater and Michael Stohl eds., *Current Perspectives on International Terrorism* (London: Macmillan Press, 1988).

Table 3. Selected Agricultural or Food Bioterrorism Incidents in the 20th Century

YEAR	NATURE OF INCIDENT	ALLEGED PERPETRATORS
Confirmed Use		
1997	Spreading hemorrhagic virus among wild rabbit population in New Zealand	New Zealand farmers
1996	Food poisoning in Texas hospital using shigella	Hospital lab worker
1995	Food poisoning of estranged husband using ricin	Kansas physician
1984	Food poisonings of salad bars in Oregon restaurants using salmonella	Ranjneeshee Cult
1970	Food poisoning of Canadian college students	Estranged roommate
1964	Food poisoning in Japan using salmonella and dysentery agents	Japanese physician
1952	Use of African bush milk to kill livestock	Mau Mau
1939	Food poisoning in Japan using salmonella	Japanese physician
1936	Food poisoning in Japan using salmonella	Japanese physician
1916	Food poisoning in New York using various biological agents	New dentist
1913	Food poisoning in Germany using cholera and typhus	Former chemist employee
1912	Food poisoning in France using salmonella and toxic mushrooms	French druggist
Threatened Use*		
1984	Attempt to kill a race horse with pathogens (insurance scam); confirmed possession	Two Canadians
1984	Threat to introduce FMD into wild pigs, which would then infect livestock; no confirmed possession	Australian prison inmate

Source: Carus, "Bioterrorism and Biocrimes: The Illicit Use of Biological Agents in the 20th Century"; Parker, "Agricultural Bioterrorism: A Federal Strategy to Meet the Threat," 20-21.

* Not related to food poisoning

This being said, agroterrorism could well emerge as favored form of secondary aggression that is designed to exacerbate and entrench the general societal disorientation caused by a more conventional campaign of bombings. The mere ability to employ cheap and unsophisticated means to undermine a state's economic base and possibly overwhelm its public management resources give livestock and food-related attacks a highly beneficial cost/benefit payoff that would be of considerable interest to any group faced with significant power asymmetries. These considerations have particular pertinence to an organization such as *al Qaeda*, which has repeatedly stated its intention to conduct economic warfare against the United States (Bin Laden regarding Washington's wealth as the main anchor of the "morally bankrupt and dysfunctional" Western system that he seeks to overthrow) and explicitly endorsed the acquisition and use of biological agents to undermine American interests (in whatever manner possible) as a religious duty beholdent on all "true" Muslims.³⁰¹

It is also perhaps worth noting that, at least at the nation state level, the potential viability of employing livestock diseases as a form of indirect warfare has long been recognized. As far back as World War Two, the British were experimenting with "cattle cakes" – cow "snacks" laced with anthrax – as a way of

³⁰¹ "The World's Newest Fear: Germ Warfare," *The Vancouver Sun*, September 24, 2001; "Fear and Breathing," *The Economist*, September 29, 2001, p. 37.

crippling the German beef industry.³⁰² Before terminating its biological weapons (BW) program in 1969, the United States had field-tested both hog cholera and NVD for offensive purposes.³⁰³ A key component of Soviet BW efforts was similarly directed toward the development of agricultural pathogens, including FMD, rinderpest, CSF and sheep/goat pox viruses.³⁰⁴ During the Apartheid years, the Republic of South Africa (RSA) weaponized both FMD and ASF for use in Angola, Namibia (then Southwest Africa) and Zimbabwe, while in Iraq it is now known that at least anti-animal agents had been developed prior to the Gulf War: FMD and camelpox.³⁰⁵

There are several ways by which a deliberate act of agriculture sabotage or terrorism could occur on U.S. soil, using a variety of different causative agents and dissemination methods. Attacks directed against either the cattle industry or instituted via the food chain, however, pose the most serious threat in terms of latent run-on effects and general socio-economic and political disruption. Possible threat scenarios could embrace:

1. The introduction of a zoonotic pathogen designed to kill both humans and animals. One possible agent would be screwworm myiasis. The disease is endemic throughout the world, remaining prevalent in Panama and of at least residual concern in Mexico. It is caused by the *Cochliomyia hominivorax* maggot, which feeds on the living tissue of any warm-blooded mammal. Infecting cattle would not be problematic as females are able to oviposit eggs (which number in excess of 400 in a single laying) in a wide range of wounds common to these animals, including tick bites and cuts/lesions resulting from dehorning and castration. An initial infestation could easily spread to urban areas (adult flies have the ability to travel up to 300 km on wind currents), where it would pose an immediate health risk to both domesticated pets and humans.³⁰⁶
2. The introduction of a non-zoonotic pathogen designed to undermine support and confidence in government and trigger mass economic destabilization. The most viable agent in this instance would be FMD, which is easy to acquire, environmentally hardy and highly transmissible – remaining one of the most contagious viruses currently known to medical science. Disseminating FMD would be as simple as scraping a viral sample directly on a cow in a remote field or merely introducing the agent into a silage bin or feedlot an auction barn. Because of the disease's highly

³⁰² Gorman, "Bioterror Down on the Farm," 813. According to Carus, the German Secret Service was experimenting with anti-livestock biological agents even earlier. He attests that various programs involving glanders and anthrax cultures were developed during World War One as part of a concerted effort to destroy animals that were deemed to be contributing to the Allied war effort in Europe. Targets included sheep, cattle, horses, mules, donkeys and ruminants in Russia, Romania, Argentina and the United States. See Carus, *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents in the 20th Century*, 87-8.

³⁰³ Wilson et al., "A Review of Agroterrorism, Biological Crimes and Biological Warfare Targeting Animal Agriculture," 10. See also E. Regis, *The Biology of Doom. The History of America's Secret Germ Warfare Project* (New York: Henry Holt and Company, 1999); and L. Cole, *The Eleventh Plague. The Politics of Biological and Chemical Warfare* (New York: W.H Freeman and Company, 1997). On 12 occasions between 1964 and 1967, Fidel Castro accused the United States of using animal, plant and human viruses and insects to harm and disrupt the Cuban economy. He has also claimed that livestock pathogens were intentionally introduced into the country at least six times following the formal termination of Washington's BW program, once in 1971 and 1979 and twice in 1981 and 1985.

³⁰⁴ Wilson et al., "A Review of Agroterrorism, Biological Crimes and Biological Warfare Targeting Animal Agriculture," 13-14.

³⁰⁵ Comments made during the "National Security Implications of Advances in Biotechnology: Threats to Plants and Animals" Steering Group Meeting, National Academy of Sciences Meeting, Washington DC, August 1999. See also Wilson et al., "A Review of Agroterrorism, Biological Crimes and Biological Warfare Targeting Animal Agriculture," 11-12, 14.

³⁰⁶ Author interview, CDFA officials, Sacramento, California, August 14, 2000.

contagious nature and the concentrated and intensive nature of contemporary U.S. farming practices, a multi-focal outbreak across several states would be virtually assured.³⁰⁷

3. An attack carried out further down the food chain, either for blackmail purposes or as a form of direct aggression against humans. Packing plants dealing with fresh fruits and vegetables and small-scale food manufacturers, particularly those specializing in ready-to-eat meats or aggregated foodstuffs represent the greatest threat. These sites are vulnerable as they lack adequate bio-security provisions, do not use heat in the processing stage (a good “front-end” barriers against pathogenic contamination) or deal in pre-prepared produce that does not require cooking (a good “back-end” defense against microbial introduction). Likely agents would include bacteria and toxins such as salmonella (which can be grown in a domestic kitchen), E. coli 0157 (which is commonly shed by cattle) and botulism (which has no odour, does not visibly spoil food and does not require sophisticated equipment to manufacture).³⁰⁸

POLICY SOLUTIONS

The US - more by luck than design - has not experienced a major agricultural or food-related disaster in recent memory. There has, as a result, been no real appreciation of either the consequences or threat potential of such an event taking place in this country – a cognitive perception that has been further exacerbated by the general “invisibility” of the sector in American society.³⁰⁹ This has been reflected in the make up of the U.S. agricultural emergency preparedness and response, which have yet to be given the resources necessary to develop into a truly integrated and comprehensive system capable of addressing mass, multi-focal contingencies. Federal appropriations specifically designated to the Agricultural Research Service (ARS) for counter-terrorism purposes in FY01, for instance, amounted to only \$500,000 (a request for \$391 million was originally made), representing a mere 0.003 percent of the total homeland security budget allocated for that year (\$16 billion).³¹⁰

Just as importantly, general bio-security and surveillance at many of the country's food processing and rendering plants remains inadequate. Formal state and federal inspections of these sites are rudimentary, with most produce tested on a simple and generally highly unrepresentative sample-basis only.³¹¹ Moreover, the current oversight of food production is quite inconsistent. Remarking on this, Robert Robinson, Managing Director of Natural Resources and the Environment at the General Accounting Office (GAO) has observed: “If you are producing a packaged open-faced meat or poultry sandwich, you get inspected daily... If, on the other hand, you are producing a close-faced sandwich with identical

³⁰⁷ Comments made during the “Agro-Terrorism: What is the Threat?” Workshop, Cornell University, Ithaca, New York, November 12-13, 2000.

³⁰⁸ Comments made during the “Bioterrorism in the United States: Calibrating the Threat,” Seminar, Carnegie Endowment for International Peace, Washington DC, January 2000.

³⁰⁹ Three main factors account for the invisibility of the agricultural sector in the U.S. First, most Americans take safe and available at food for granted, generally finding it difficult to conceive of circumstances where it would be scarce, expensive or risky to consumers. Second, the increasingly concentrated nature of modern agricultural practices in the United States has led to a dramatic reduction in the number of individual farms in the country stems (2.2 million in 1998 compared to 6.3 million in 1929). Third, technological innovation has resulted in fewer Americans being directly employed in agricultural production: farming accounted for 2.6 percent of the U.S. workforce in 1998, down from 23 percent in 1929. Parker, *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat*, 29. See also USDA, *Agriculture – Farms, Acreage and Foreign Trade: 1990-1998*, National Agricultural Statistics Service No. 1441 (1999).

³¹⁰ Parker, *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat*, 30; USDA, *Advisory Committee on Agricultural Biotechnology*, Federal Register Notice 64.

³¹¹ Generally only canned foods that have a low acidic count are monitored on a comprehensive basis. This is because these products have a high potential to harbor botulism.

ingredients, you get inspected...on average once every five years.”³¹² This lack of officially administered surveillance becomes especially problematic when one considers that the bulk of the country’s food manufacturing and packing industry exists in the complete absence of effective bio-security and/or internal quality control.

In specific terms, it is possible to identify the following key deficiencies in the current U.S. agricultural emergency management system:

- A lack of resources, particularly in relation to quickly identifying, containing and eradicating large-scale disease outbreaks;
- Insufficient personnel with appropriate training in foreign animal disease (FAD) recognition and treatment;
- A declining diagnostician pool in general as a result of insufficient educational support for veterinary science;
- Inadequate forensic coordination between the agricultural, intelligence and domestic criminal justice communities;
- An emergency response program that relies on unreliable passive disease reporting systems, and which is hampered by a lack of communication and trust between regulators and producers;
- Insufficient food surveillance and inspections at processing and packing plants;
- Inadequate response modalities to deal with food-borne diseases.

The catastrophic events of September 11 have, to a certain extent, galvanized more concerted national attention on (some) of these weaknesses and the general vulnerability of the U.S. agricultural sector to deliberate sabotage and disruption. The ARS’ counter-terrorism budget for FY03, for instance, has been increased to \$5.5 million (from a FY02 base that remained unchanged at \$500,000) while the USDA has received \$328 million in Emergency Supplementary Appropriations (ESA) to augment overall preparedness and consequence management efforts in relation to intentional attacks against the country’s food supply.³¹³ In addition, the department’s FY03 budget includes extra allocations amounting to \$146 million to strengthen food safety programs as well as to support general efforts aimed at responding, managing and containing livestock (and crop) disease outbreaks.³¹⁴

However, Federal fiscal resources available to the department remain at marginal levels – in excess of \$4 billion has been earmarked for general bioterrorist purposes alone over the next two years³¹⁵ – and no provision has been made in the ESA to support in-depth state and local first response (a main area of weakness in terms of national contingency efforts).³¹⁶ Moreover, agriculture is still to be officially

³¹² Testimony of Robert Robinson before the Subcommittee on Oversight of Government Management, Restructuring and the District of Columbia of the Committee on Governmental Affairs, “Food Safety and Security: Can Our Fractured Food Safety System Rise to the Challenge?” United States Senate, October 10, 2001.

³¹³ Author interview, USDA officials, Washington DC, May 23 2002. See also USDA, *FY03 Budget Summary*, available at on-line at <http://www.usda.gov/agency/obpa/Budget-Summary/2003>.

³¹⁴ “Agriculture Budget Proposes Increases in Key Areas,” USDA News Release, No. 0031.02, February 4, 2002; USDA, “FY03 Budget Summary.” Key areas for this funding include:

- Plant and animal health monitoring (\$48 million);
- Overseas disease monitoring (\$5 million);
- Border inspections (\$19 million);
- Food safety inspections (\$28 million);
- Research (\$34 million);
- Diagnostic, management, response and other scientific and technical services (\$12 million).

³¹⁵ Figure cited in “House Passes \$4.6 Billion Bioterror Bill,” *The Associated Press*, May 22, 2002.

³¹⁶ ESA funding is earmarked for the following areas only:

recognized as a critical infrastructural node for the purposes of PDD-63 and was conspicuously absent in a GAO report on combating terrorism released nine days after the attacks on the World Trade Center and Pentagon.³¹⁷

The U.S. ignores the continuing vulnerability of the agricultural sector at its own peril. Measures can and, indeed, should be instituted to pursue a more aggressive and coordinated strategy to securing the industry from deliberate attack, an approach that would have the added ancillary benefit of augmenting general food and livestock response and consequence management efforts. These initiatives should build on programs already underway, leverage existing Federal, state and local capabilities and involve key customers, stakeholders and partners.³¹⁸ At least six policy recommendations can be made for the short and medium term.

First, a comprehensive needs analysis should be undertaken to ascertain appropriate investment requirements for the Federal emergency management infrastructure, particularly in relation to:

- Continuing FAD intramural research in ARS laboratories;
- Regular preparedness and response exercises and programs, embracing both in-house tabletop/day after games as well as full-scale field simulations;
- The upgrading of existing diagnostic laboratories to bio-safety level 4 (BSL4) (necessary for high level research in the most contagious and dangerous animal pathogens;³¹⁹ and
- Integrated electronic field diagnostic and communication systems and emergency control centers that are able to take advantage of the very latest information and data management technology.

Second, moves need to be made to increase the number of state/local personnel who have the requisite skills to identify and treat exotic animal diseases. Useful in this regard would be some initial reform of the overall veterinary science curriculum, with a greater emphasis on developing and supporting on-going FAD and large-scale husbandry education components. A review of the training and certification requirements of non-veterinarian practitioners who view the conditions of individual animals on a regular basis (such as ranch handlers) would also be helpful. Together with appropriately accredited local/state

-
- Improving agricultural quarantine inspection and emergency management systems within the USDA's Animal and Plant Health Inspection Service (APHIS);
 - Accelerating construction of facilities to support ARS animal health research and APHIS diagnostic and vaccine programs;
 - Upgrading laboratory security and improving operational security equipment.

³¹⁷ Parker, *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat*, 1, 30. ADD REFERENCE FOR GAO REPORT (FROM PARKER). The GAO specifically excluded consideration of the agricultural sector in its analysis because it was not included as one of the critical systems specified under PDD-63.

³¹⁸ Parker, *Agricultural Bioterrorism.: A Federal Strategy to Meet the Threat*, 31.

³¹⁹ The USDA currently relies on two main reference centers for virulent and contagious animal viruses: the Foreign Animal Disease Diagnostic Laboratory (FADDL) on Plum Island, New York; and the National Veterinary Services laboratories (NVSLs) in Ames, Iowa. However, neither facility has been certified above BSL 3, meaning that they cannot conduct concerted research into the most dangerous livestock pathogenic agents; currently, the USDA relies on the Centers for Disease Control (CDC) in Atlanta and the U.S. Army Medical Research Institute for Infectious Diseases (USAMRIID) at Fort Detrick for these assessments. Comments made during the "Agro-Terrorism: What is the Threat? Workshop, Cornell University, Ithaca, New York, November 2000. See also "Administration Plans to Use Plum Island to Combat Terrorism, The New York Times, September 21, 1999.

vets, these individuals would help to fulfill an important USDA “force multiplier” function by providing an effective “first line of defense” against threatening livestock pathogenic outbreaks.³²⁰

Third, assessments of how to better foster more coordinated and standardized links between the U.S. agricultural and intelligence communities should be undertaken. Although partnership agreements have been established between the USDA, Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI), they have yet to be embraced on a department-wide level - largely because only a small percentage of USDA personnel have adequate clearances to access relevant security data in the first place.³²¹ Gauging the extent to which this intelligence gap needs to be bridged would provide a valuable (and necessary) base metric for the subsequent institution of an appropriate and secure terrorist-agriculture information-exchange environment.³²²

Fourth, attention needs to be devoted to issues of law enforcement and criminal justice, particularly in the context of forensic investigations to determine whether disease outbreaks have been deliberately orchestrated or are the result of naturally occurring phenomena. A useful USDA-FBI liaison program already exists, which allows for regular personnel exchanges and cross-agency meetings and discussions in an ad hoc working group setting.³²³ This framework of budding federal cooperation should be fully institutionalized and used to guide the development of similar arrangements at the state and local levels.

Fifth, the overall effectiveness of the passive disease reporting system needs to be re-visited. The role of insurance and indemnity in offsetting potential delays in disease reporting and augmenting general bio-preparedness should be analyzed, particularly in terms of mitigating producer concerns relating to compensation for destroyed livestock and costs incurred as a result of cleaning and disinfection.³²⁴ Moves should also be made to improve the transparency of farm-emergency management communication channels, logically through dedicated Federal and state outreach and information programs. This type of systematic interaction could also be used to help elevate the level of trust between regulators and producers, particularly with regards to highlighting the positive benefits of early disease reporting. The USDA is well placed to develop initiatives of this sort given the close links it has established with the American agribusiness spectrum through its extensive network of field offices, agricultural extension specialists, research facilities and land-grant universities.³²⁵

Finally, bio-security, surveillance and emergency response at food processors and packing plants needs to be upgraded, especially at those facilities that exist at the smaller end of the scale. Although EAS funding has been made available to support the oversight activities of the Food Safety and Inspection Services (FSIS – see f/n 64) and full implementation of the Hazard Analysis and Critical Control Points

³²⁰ This “force multiplier” function becomes especially important when one considers that APHIS – the USDA’s main emergency management body – has a full-time staff of just 400, of which only 250 and 300 can be realistically expected to be made available at any one time. Author interview, APHIS officials, Washington DC, July 1999. See also Gordon and Beech-Nielson, “Biological Terrorism: A Direct Threat to Our Livestock Industry,” 357.

³²¹ Author interview, USDA official, Washington DC, July 1999.

³²² Parker, *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat*, 42.

³²³ Comments made during the NRC “National Security Implications of Advances in Biotechnology: Threats to Plants and Animals” Planning Meeting, National Academy of Sciences, Washington DC, August 1999.

³²⁴ It should be noted that the USDA is considering a review of indemnity provisions specifically related to foot and mouth disease, which would authorize payments to cover both disinfection costs as well as the full market value of destroyed animals and related products and materials. For a detailed description of the proposed changes see USDA, *Foot and Mouth Disease Payment of Indemnity; Update of Provisions* [Docket Number 01-069-1], RIN 0597-AB34, November 2002, available at on-line at: <http://frwebgate.access.gpo.gov>

³²⁵ Parker, *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat*, 32. According to Parker, the USDA is unique among Federal agencies in its closeness to public and private constituencies.

(HACCP)³²⁶ rule is now theoretically meant to be in place, the number of sites that exist in the country relative to available Federal and state inspectors largely precludes significant scope for change in this area. A far better alternative would be for companies, themselves, to institute more effective internal quality and regulatory control. Some basic improvements that could be immediately implemented include:

- The institution of more effective site security, such as restricting rights of entry and exit, locking up storage/bulk ingredient containers, and mounting video surveillance at key internal processing hubs;
- Increased background checks of seasonal employees, at least to the extent that character references are both supplied and verified. Medium-sized firms might also consider conducting basic security and criminal (and health) checks of workers involved in the manufacture of widely distributed and highly aggregated foodstuffs, such as sausage meat;
- The development of clearly documented, well-rehearsed product recall plans overseen by dedicated crisis management teams that are quickly able to assess the scope of potential problems and the modalities required for containing and correcting them. At a minimum, all food processing companies should be able to produce the regulatory documents as designated and prioritized by the Food and Drug Broad, in four hours or less on any day of the year for a given three month time-frame.³²⁷

Over the longer-term, thought could also be given to the practicalities of standardizing and rationalizing food and agricultural safety within the confines of a single Federal agency that has both budgetary and programmatic powers over a wide spectrum of functional domains and jurisdictions. Such a body would certainly help to streamline the patchwork of largely uncoordinated food safety initiatives that currently exists in the U.S., many of which have sought to only individually enact specific preparedness and response objectives. In addition, it would contribute substantially to the development of an integrated national emergency animal and food disease prevention and response plan that cuts across

³²⁶ Under the HACCP rule, all plants slaughtering and processing meat and poultry are required to identify critical control points where microbial contamination is likely to occur and institute FSIS designated systems to prevent or reduce those hazards from eventuating. HACCP controls were instituted at the country's largest meat and poultry plants in January 1998 and have since been extended to all smaller facilities, including those with 10 employees or less. Comments made by Dr Kaye Wachsmuth before the Annual Meeting of the American Public Health Association, Washington DC, November 18 1998, available at on-line at http://www.fsis.usda.gov/oa/speeches/1998/kw_percent5Faph.htm.

³²⁷ These include:

- Complete label sets and ingredient lists for all products;
- Process flow chart for each product;
- Distribution lists (by products) for each day of the time period;
- Written explanations for all commodity codes and expiration dates;
- Monitoring and production logs and test results as required by the HACCP regulation system;
- Complete current customer lists by state (including names, street addresses and phone, fax, and pager numbers);
- Invoices and bills of lading for all ingredients;
- Draft recall memos/letters to customers;
- Draft recall press releases;
- Draft recall verification/contact logs;
- Lists containing the names and numbers of primary and secondary contacts at all relevant regulatory agencies;
- Logs and summaries of all consumer complaints for the time period in question;
- Written plans for deciding upon and evaluating the scope of the recall;
- Written plans for ensuring and maintaining a proper chain of custody for all recalled products; and
- Written plans for the secure storage and/or destruction of all recalled products.

Data derived from Jeff Farrar, "Foodborne Outbreak Investigations: What Agencies Do and What Regulators Expect of You," unclassified briefing provided to author, August 2000.

mission/capability areas of multiple Federal, state and local agencies and, thereby, helps both to reduce conflicts and eliminate unnecessary duplication of effort. Possible components of such a strategy could include the following elements:

Table 3. Components of a National Strategy to Counter Biological Attacks against Agriculture

PREVENTIVE MEASURES	RESPONSE MEASURES
Intelligence measures (identify potential threats and perpetrators; understand motivations; predict behaviour)	Consequence management
Monitoring programs (detect and track specific pathogens and diseases)	Early detection of exotic/foreign pathogenic agents
Targeted BSL 4 research	Early prediction of disease dispersion patterns
International counter-proliferation treaties, protocols and agreements	Early containment procedures
Creation of agent-specific resistance in livestock	Epidemiology and treatment
Vaccination against specific Class A agents	Depopulation and carcass disposal
Modification (where possible) of vulnerable U.S. food and agriculture practices	Diplomatic, legal, economic and political responses
Bio-security and surveillance	Compensation and indemnity
Education and training (Federal, state and local)	Education and training
	Public awareness and outreach programs
	Vaccine and pharmaceutical stockpiling

Source: Much of this list was taken from Parker, “Agricultural Bioterrorism: A Federal Strategy to Meet the Threat,” 40-41.

Implementing these various recommendations will require active political input and commitment. Reform along the lines recommended above - which would serve the dual (and equally important) purpose of also augmenting the USDA’s ability to deal with natural disease outbreaks - will not be cheap and will definitely need Federal support. Considerable money has already been devoted to defending against the relatively low risk scenario of viral attacks aimed at human populations. By comparison, contingency measures for livestock and crop protection have attracted only limited support, despite the comparative ease of carrying out such attacks and the enormous implications they pose for the economic, social and political stability of the U.S. Serious assessments of the threat posed by biological terrorism suggest that this imbalance needs to be modified, or, at least recognized, both as a matter of fiscal responsibility and judicious public policy.

APPENDIX F– THE PSYCHOLOGICAL IMPACT OF AGRICULTURAL TERRORISM

The following is a mini-review of the Foot and Mouth Disease outbreak in the United Kingdom and its potential impact on human psychology.

Methodology

To prepare this report, Internet searches for information on the Foot and Mouth Disease in the UK in medical journals and news media were conducted. The resulting information (mostly commentaries and news articles) was reviewed and interpreted within the context of knowledge and previous research on the psychological consequences of disasters, mass violence, and terrorism.

Research Questions and Analysis

What was the impact of the FMD outbreak in the UK on human psychology and behavior?

The outbreak of Foot and Mouth Disease in the United Kingdom during the spring of 2001 resulted in the culling of more than 4.3 million livestock (sheep, cattle, and pigs). The outbreak and the following clean up efforts had many economic (e.g., higher beef and pork prices, loss of income for affected individuals, etc) and social (e.g., restricted travel) consequences through the English countryside and farming communities.

While there were not any empirical reports in the scientific literature indicating the actual psychological impact of this crises in either the farming communities or general public, several anecdotal news reports have indicated emotional and behavioral responses in some of the populations. Several news articles and even reports following the crises have reported anger, frustration, and mistrust among community members with respect to the government's response to the outbreak. Many articles noted problems in communication with the public and the need to place blame on someone for this crisis. Reports cited disagreement with the government enforced travel restrictions. The farmers as well as the tourism industry within these regions all experienced great financial loss. While some of the loss was compensated by the government's Rural Recovery Fund, many individuals were forced to question the future of their career and livelihood, and some had their applications turned town because all the money ran out (a potential source of additional frustration).

In a report to the National Assembly for Wales, the Welsh Institute of Rural Health reported that individuals affected by the FMD experienced a range of psychological symptoms. Using a survey of organizations that provided voluntary and statutory support to the affected individuals, they noted that those seeking assistance commonly experienced tearfulness, lack of sleep, loss of appetite, increased consumption of alcohol and tobacco, increased anger, irritability, increased marital and domestic discord, and general feelings of depression. One help line also noted that up to 50% of callers related to FMD exhibited symptoms of a mental health impact. Health practitioners also reported seeing farmers and business owners with a range of mental health problems from stress, anxiety and depression. It should be noted that these data were not scientifically assessed or quantified, they are based on the recall of support workers, and they only include the experiences of those who sought help.

Such psychological reactions are most likely the result of the great economic impact this outbreak had on these communities. While such economic impact is probably the most traumatic to the direct victims (farmers and community members), it is hard to separate out what psychological impact, if any, the FMD had on the UK population. Representatives from the US Department of Health and Human Services heard anecdotally on several occasions that the FMD outbreak added an additional level of cumulative stress on

a community that was already undergoing stressful economic and social change. There were also anecdotal reports of depression and suicides among the farmers; of isolation and decreased levels of social interaction; and of social tension and community conflict. These impacts however represent only one component of the potential traumatic impact of an agricultural terrorism event.

Trauma is not necessarily defined by the event itself, rather it is defined by the meaning of the event for people and by its practical implications to the community. Since this outbreak was natural and farmers in the UK have dealt with such disease before, the previous familiarity with the disease likely reduced the fear and anxiety (related to the outbreak itself) in the community. This prior familiarity in dealing with FMD and the natural source of the infection are important factors that distinguish the FMD outbreak from agricultural terrorism. However, if this outbreak had been viewed as agricultural terrorism the psychological consequences would likely have been greater. For example, if this had been (or even rumored to be) man-made or if the virus had been modified in any way, the psychological impact on the farmers and community members would likely have been much greater. The mere rumor and uncertainty that disease or disaster had been intentionally caused has been shown to create fear, anxiety, and anger (Halloway, 1997), as have intentional actions (Norris, 2002). Additionally, had there been any perceived health risks to humans (or even rumors of such a risk), such as might occur if there was evidence that a biological agent had been modified in any way, it is likely that the psychological effect from the attack itself would have been greater.

For example, both the direct and responder populations were exposed to some health risks, which in turn may have created additional psychological response. While FMDV is widely advertised as not transmittable to human beings, approximately 40 cases have been documented around the world. While the last case was documented in 1967, approximately 21 individuals, most with oral lesions and who had been exposed to FMDV were tested during the UK outbreak. All tested negative, however, the potential for difference in information about potential transmittal to humans may have created additional anger and confusion among the populations. In addition, the fires that were lit to destroy infected herds released harmful carcinogenic dioxins into the atmosphere. News of this increased individual levels of fear and anger among all of those exposed (farmers, slaughter men, nearby residents). Individuals who perceived themselves to have been exposed have been shown to have had increased short and long term psychological responses after other events. Representatives from the USDHHS that visited the affected area several months after the outbreak observed reports of high levels of stress and about potentially traumatic experiences for some staff involved in the response. They noted that veterinarians had a particularly difficult time coping.

In sum, the recent FMD outbreak in the UK is probably a poor example of the potential range of psychological reactions associated with agricultural terrorism because it was not considered an act of terrorism nor were there great health risks to humans. However, it does provide some anecdotal evidence that the economic impact of such an outbreak has an effect on the emotions of those it affected and how response strategies can both create or mitigate psychological consequences. For example, the public confidence in the government communication was affected by prior poor communication and lack of trust. As such good risk communication strategies will be important. In addition, although the FMD was not traumatic as commonly defined, it was quite stressful.

How might we better understand the anticipated psychological impact of agricultural terrorism?

Whether or not widespread and significant psychological responses will be observed in the event of agricultural terrorism will be largely dependent upon the characteristics of the event (e.g., intentional infection), of the agent (e.g., contagiousness to humans) and the impact the event and the response (e.g., travel restrictions, food recall, clean up and recovery efforts) has on the individual and affected community. Also, to the extent that agricultural terrorism occurs in isolation or in conjunction with other types of terrorism will also be important. Further, the psychological impact of the event will depend

upon the extent to which these factors contribute to whether or not the event is considered traumatic (to people and society).

Human psychology broadly defined includes the emotional, behavioral, cognitive, and biological responses of individuals and communities. The psychological impact of natural as well as man-made disasters (including technological disasters including potential chemical or radiological contamination) has been documented. Previous research studies have also demonstrated the psychological impact of conventional terrorism and mass violence on people. While less is known about the psychological consequences of bioterrorism, it is reasonable to anticipate that the psychological impact of bioterrorism will be similar to the consequences observed from other traumatic experiences. It has also been postulated that the unknown, invisible characteristics of bioterrorism may contribute to greater fear and anxiety. The same may be true of agricultural terrorism, animal diseases may be unfamiliar and if the spread is due to an invisible, potentially contagious agent. Thus, an agricultural terrorism event could be considered to be potentially traumatic (e.g., if there are human morbidity and mortality concerns) to people, but again it will depend on the meaning the event has on the people impacted. However, given previous studies it is reasonable to anticipate that if there were an intentional effort to infect a large number of livestock or other agricultural food products with the intent to kill or harm humans, there would indeed be substantial psychological consequences.

While the human psychological consequences of agricultural terrorism cannot necessarily be predicted with certainty, it is possible to establish means and opportunities to understand, monitor, and prevent or mitigate responses, particularly those with negative consequences. In a recent Animal Health Emergencies Exercise for the state of Indiana, human health issues were not considered in the After Action Report. However, it is reasonable to anticipate that there may in fact be health issues (including mental health) that will need to be considered especially among the farmers and the responders and particularly given the relationship between health and behavior. As noted above, if human health risks or rumor of intentional infection were greater components of the FMD outbreak, the psychological and behavioral impact would have likely been much greater.

In the absence of these factors, the psychological effects of agricultural terrorism are likely to be a consequence of the greater level of stress that will result, and the impact on the existing social structure and the way it may affect coping strategies. As such, much can be learned from the UK experience with regard to the anticipated needs for healthcare among the affected communities

To gain a better understanding of the psychological consequences associated with an agricultural event, we propose activities in each of three stages (pre-event, acute, and longer term). At each of these phases, we propose two goals: (1) understanding and monitoring psychological response among the populations of interest; and (2) implementing strategies that would serve to mitigate or prevent negative psychological and behavioral consequences.

Pre-Event Phase:

- (1) Gain a baseline understanding of the perceived risks and level of knowledge about potential risks of agricultural terrorism within the agricultural environment/community and the general public. We might also want to assess risk factors for negative psychological consequences to understand where screening/assessment and treatment interventions might best be aimed in the acute phase. We might also suggest assessing how rural communities have dealt with other community wide stressors (economic or traumatic), in order to understand how strategies may need to differ from urban areas. For many types of agricultural terrorism that are not a threat to humans, this would inform the development of response strategies that are sensitive to the impact on human psychology.
- (2) This could be followed with educational information aimed at the particular populations that is aimed to not only provide accurate and useful information about the risks and types of agricultural terrorism, but about how a likely response scenario would impact their personal lives.

Acute Phase (detection and management):

- (1) All victim populations (direct victims, responders, community members, etc) should be screened and monitored for psychological consequences (emotional, cognitive, biological, and behavioral responses) at repeated intervals. This will enable the targeting of interventions and educational information that might serve to mitigate any potentially severe and negative consequences. At the same time, it would be critically important to measure and monitor: utilization of health care services, consumer behavior for various agricultural products, and other markers of social or economic impact (e.g., local real estate market, measures of community involvement, police activity, etc).
- (2) Monitor coping strategies used in affected community
- (3) Educational information should be made available to those within the affected communities as well as the general public about the event, the response, and its impact on their life. Responders should be targeted for additional information, resources, and counseling as necessary. Risk communication strategies will need to be employed and will play a critical role in mitigating potential negative psychological consequences.

Recovery Phase (longer term management):

- (1) It will be important to continue monitoring the areas outlined above in the acute phase to track trends and target appropriate interventions (including both the implementation or withdrawal of programs) for all victim populations.
- (2) Educational information should continue to be made available but it should focus on recovery issues that promote positive behaviors and consumer responses and serve to regain and reinforce trust in the community, agricultural industry, and government. Those requiring specialty services (e.g., mental health counseling or other health care services) should be directed to and supported through appropriate care. Risk communication strategies will continue to be important.

In the interim, it may be best to build a better understanding of the potential impact agricultural terrorism scenarios will have on human psychology using examples of animal and food-borne diseases that may be more unfamiliar and have human health risks. In this manner, we can begin to understand the ways people are likely to react, develop educational materials, devise risk communication techniques, and implement programs to increase understanding and decrease the potential trauma of an agricultural terrorism event.

Citations:

Deaville J, Jones L. The Health Impact of the Foot and Mouth Situation on People in Wales—The Service Providers Perspective. A summary report to the National Assembly for Wales by the Institute for Rural Health. May 2001.

United States Government Accounting Office. Foot and Mouth Disease: To Protect US Livestock, USDA Must Remain Vigilant and Resolve Outstanding Issues. GAO Report to the Honorable Tom Daschle, US Senate. July, 2002. GAO-02-808

APPENDIX G



United States Animal Health Association

USAHA 2001 Resolution No. 10

UNITED STATES ANIMAL HEALTH ASSOCIATION - 2001

RESOLUTION NUMBER: 10

SOURCE:

Committee on Transmissible Diseases of Swine
Committee on Transmissible Diseases of Poultry
Committee on Foreign and Emerging Diseases

SUBJECT MATTER: FOREIGN ANIMAL DISEASE (FAD) DIAGNOSTIC CAPABILITY AT THE STATE AND LOCAL LEVEL

DATES: Hershey, Pennsylvania, November 1-8, 2001

BACKGROUND INFORMATION:

Under current protocols, testing for a foreign animal disease (FAD) such as foot-and-mouth disease or classical swine fever in the United States can only be accomplished by shipping samples to National Veterinary Services Laboratories. The process of shipping samples to these laboratories takes time and a great deal of effort and is not one that is normally used unless signs are likely that a FAD may exist. Also, the current protocol is not one that is conducive to screening routine laboratory submission for foreign animal diseases.

If an outbreak of a foreign animal disease occurs in the United States, early detection will be critical in the containment and elimination of the disease. Probabilities suggest that by the time an outbreak is detected, it will already have spread to more than one location, probably in more than one state. Our ability to respond could be greatly increased by the ability to conduct tests for FADs at the local level.

With the development of new diagnostic tests such as PCR, it seems that early detection and rapid response to a foreign animal disease outbreak could best be accomplished if state veterinary diagnostic laboratories are trained and equipped to run FAD diagnostic tests. Sample submission would be more rapid than current protocols allow and it is likely that routine screening for FADs would increase. FAD diagnostic capabilities at the local level would increase the likelihood of early detection of a FAD outbreak in the United States.

RESOLUTION:

The United State Animal Health Association urges United States Department of Agriculture-Animal and Plant Health Inspection Services-Veterinary Services to implement a program to train, equip and encourage state veterinary diagnostic laboratories to perform tests and enhance surveillance for diseases that are foreign to the United States.

[USDA] RESPONSE:

By law, tests for Foot-and-Mouth Disease can only be conducted at Plum Island. Currently, all testing for foreign animal diseases is done at either the National Veterinary Services Laboratories or the Foreign Animal Disease Diagnostic Laboratory. Samples are submitted overnight in most cases; in "highly likely" cases, submission is even faster. Laboratory test results can be ready within between eight hours to several days after receipt of samples. The speed of results depends on the suspected disease and type of test.

In an outbreak situation, where laboratory diagnosis would overwhelm Federal capacity, consideration to allow State diagnostic laboratories to test would be given. The classical swine fever testing at the State level is being conducted as a pilot program and will provide valuable information on how to proceed with this endeavor.

Accessed December 3, 2002, at <http://www.usaha.org/resolutions/reso01/res-1001.html>

APPENDIX H– DEFINING A PUBLIC COMMUNICATIONS STRATEGY FOR COUNTER TERRORISM

Introduction

Since September 11, 2001, there has been growing appreciation for the importance of a public communications strategy to support counter terrorism in the United States. Such a strategy would help to limit the physical impacts of an actual attack, while reducing the ongoing psychological impacts on the general public. Encompassing all efforts to shape and transmit communications from the government to the general public on terrorism, a public communications strategy would range from dissemination activities following an attack, to comprehensive guidelines for information flows during a public health emergency, to ongoing public education efforts promoting preparedness. Spurred by a growing base of research, there is an evolving view of how to integrate these types of activities into an overall strategy. However, the elements of a comprehensive plan are still lacking in the public debate as the government reorganizes to address the threat of terrorism. With this background, this research note, for the Gilmore Commission, summarizes the research results and their implications for a top-level counter terrorism communications strategy. In conclusion, recommendations are presented to implement the strategy. Notably, this discussion does not address the issue of threat and warning communication, which is a separate topic, deserving of its own analysis.

Literature Survey

The following provides a brief description of recent research and writing that addresses the role of public communications in the government's counter terrorism efforts.

- 1) *Terrorism: Informing the Public* (Nancy Ethiel, Ed., Cantigny Conference Report, 2002, 196 pages). Narrative report of a workshop on how the government should engage the news media to report on terrorism. The workshop involved members of the news media and terrorism experts. The workshop was held before Sept 11, 2001, though the report was published afterwards.
- 2) *Volume Two: Homeland Security, A Governor's Guide to Emergency Management* (National Governor's Association Center for Best Practices, 2002, 133 pages). A practical guide for state governor's, describing planning and preparation for state-level emergency management operations. Specific advice is provided for public communications efforts.
- 3) *Critical Information Flows in the Alfred P. Murrah Building Bombing: A Case Study* (C. Manzi, M. J. Powers, and K. Zetterlund, Chemical and Biological Arms Control Institute, 2002, 150 pages). Analysis of the importance of information flows in the time periods surrounding the Oklahoma City bombing. The analysis addresses internal information flows, associated with emergency management operations, and external information flows, associated public communications and the media.
- 4) *Lessons Learned from a Full Scale Bioterrorism Exercise* (R. F. Hoffman, and J. E. Norton, Emerging Infectious Disease, 5, 652-653, 2000). Commentary from participants in the bioterrorism exercise, Operation Topoff, noting the need to improve public communication capabilities for these types of events.
- 5) LI NYC Emergency Management Lessons Learned from the World Trade Center Attack, (http://www.pswn.gov/library/pdf/lessons_WTC.pdf , 2002, 35 pages). Summary of a high level conference, with discussions of strategies for public communications during times of crisis.

- 6) *Homeland Security: Physical Protection of Critical Infrastructure* (RAND, 2002). Presentation of a federal strategy to protect critical infrastructure from terrorist attacks. The role of the media and public communications in these efforts are highlighted throughout.
- 7) *Public Responsibility and Mass Destruction: The Bioterrorism Threat* (Critical Incident Analysis Group, 2002). Draft working paper on the bioterrorist threat, with recommendations on the importance of public communications.
- 8) *Consequence Management in the 1995 Sarin Attacks on the Japanese Subway System* (R. Pangi, BCSIA Discussion Paper 2002-4, ESDP Discussion Paper ESDP-2002-01, John F. Kennedy School of Government, Harvard University, February 2002, 41 pages). Description and analysis of the public health and government response to a chemical attack. It concludes that the public communications efforts were poorly handled.
- 9) *Preparing for Terrorism: What Governors and Mayors Should Do*, (R. Pangi, Perspectives on Preparedness, No. 5, John F. Kennedy School of Government, Harvard University, November 2001). A brief summary of the planning efforts that mayors and governors should initiate as part of terrorism preparedness efforts. Developing public communication plans is an important part of these efforts.
- 10) *Bioterrorism in the United States: Threat, Preparedness, and Response* (J. Ban, C. Manzi, and M. J. Powers, Chemical and Biological Arms Control Institute, 2000, 339 pages). Comprehensive analysis of the issues surrounding bioterrorism in the United States. There are specific recommendations on the role for public communications.
- 11) *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, (National Academy of Sciences, 2002, 440 pages). Analysis of technical approaches to reducing infrastructure vulnerabilities to terrorist attacks. The report emphasizes the importance of engaging technical experts in public communications.
- 12) *Lessons learned from the Anthrax Attacks* (various media reports, 2001-2002). At the one year anniversary of the anthrax attacks, a number of media reports highlighted the public communications failures during this incident. It was widely viewed that the public communications were confusing, incorrect, contradictory, and evasive, and that they negatively impacted the public response to these events.

Key Research Results

The following section synthesizes the key results from the above research.

Public communications contribute to a range of counter terrorism efforts.

Preparedness: In the period before a terrorist incident, public communications contribute to preparedness by educating the public and the media about the types of events that might occur, how the government would respond to them, and most importantly, steps the public can take to reduce their personal risk to terrorist impacts. Members of the media develop an understanding of the types of information that will be important during a terrorist event. And members of the public are educated about the types of actions that will be required, and the resources that will be available for recovery.

Deterrence: Public communications may play a role to deter terrorist plans if they convey the scale of preparedness, capabilities to limit impacts, and reduced levels of vulnerability. Ideally, this element of public communication would coordinate with other deterrent strategies, most importantly

implementing appropriate security measures. The deterrent role of public information can occur at all times: as part of preparedness efforts before a terrorist incident, in the communications immediately following an incident, and as part of long term recovery efforts.

Reassurance: In the time immediately following an event, it is most critical that communications contribute to public reassurance and calming. This can be accomplished through a number of ways: by establishing a sense of control and authority over the current situation, by conveying the scale of emergency management operations, and demonstrating that the government is working to prevent further terrorist attacks.

Conveying key information: Following certain types of events, there will be a need to communicate with the public to limit the scale of the impacts and to speed recovery. This will be especially critical following a chemical or biological events where there will be a need to limit exposures to hazard materials, direct populations toward medical treatment, and limit the spread of disease. To carry out these tasks, it will be critical to have strong coordination between public communication efforts and internal incident management and public health communication systems (e.g., the Health Alert Network).

It is important to distinguish the different time scales for counter terrorism communications strategies: pre-event communications, immediate event communications, and post-event communications.

While there is considerable interest in public communication activities following a terrorist incident, public communication efforts for counter terrorism should be ongoing, in a continuum fashion. Before a terrorist event, public information flows contribute to preparedness while they may also play a role to deter terrorist plans. Immediately following a terrorist incident, public information flows are vital for conveying key information to reduce the impacts, reducing panic, and speeding recovery. With increasing time after an event, public information flows play an important role to restore calm and public order. In this way, post-event communications eventually take on the roles and characteristics of pre-event activities.

The roles and relationships between the government and media are extremely fluid in the time immediately following a terrorist event.

Most communication strategies are structured on the premise that the government (or in some cases private industry) provides information about terrorism to the public via the media. While this is assumption is largely correct, the roles can be inverted in the hectic period immediately following a terrorist incident. During this time, the government often relies on the media to obtain critical information about a terrorist incident (what has happened, are there casualties, what is the public reaction, etc). In fact some members of the media view themselves as part of the “first responders” to a terrorist incident. Because the media is the primary source of information at this point, it can contribute to the sense of chaos and that idea the government is not “in charge.” Thus, an important component of a public communications strategy is the capability to start operations quickly and to accomplish integration with the emergency management efforts.

During an incident, any spokesperson(s) should have strong operational and technical credibility, with good communications skills.

In the period following a terrorist event, there is a need for correct information, delivered in a reassuring and authoritative way. This goal is best accomplished by someone (or persons) with strong communications skills and who are fully integrated with the emergency management operations. That is, public information strategies do not need to rely on top level officials as the primary

communicator, unless these individuals have a natural capability or desire to play this role. In many cases, the most appropriate person will already play the role of a public spokesperson, with established relations and credibility in the media. To insure that public messages are credible and reassuring, there will be a critical need for coordination between the large number of entities with communication responsibilities following an event (e.g., between different of government, between different agencies, and between elected and appointed officials). On an operational level, the goal will be to coordinate the range of voices into chorus, rather than a confusing mix of contrasting sounds. During some incidents, it will also be important to engage technical experts so that correct and authoritative information can be delivered to the public to minimize collateral impacts. In this way, the role of technical experts will be essential during a chemical or biological event.

There are a number of qualities that should be avoided in public communications, at all costs.

In choosing appropriate people to speak with the media and the public, a communications strategy tries to avoid communication styles that are known to be counterproductive. If public communications are speculative, confusing, or incorrect, they will significantly increase public anxiety, and they will cause people to mistrust future statements. Similar reactions will be generated by communications that seem to be disconnected from the information flows within emergency management operations, or contradictory to other messages from public officials. A challenging but equally disruptive issue involves withholding information about a terrorist incident. In some cases, authorities may decide that information must be withheld because it would compromise efforts to respond to the terrorist incident or it may reveal critical vulnerabilities that could be the target for subsequent attacks. While such actions may be justified, there is a risk that they will generate mistrust and anxiety if the public perceives that critical information is being withheld.

It would be valuable to carry out a range of communication preparedness activities, including

Educational Efforts: It would be valuable to carry out a continuous schedule of briefings with government officials and technical experts to educate the media on what to expect during different types of terrorist incidents. These could include technical information about the impacts of an attack, associated public health concerns, the nature and organization of the government response, the scales of possible damage, and what types of public actions will be required to speed recovery and limit damage. These briefings would also contribute to public preparedness, because the media would report the information.

At the same time, developing internet web pages with continuously updated information, could make a large contribution to public education. In some cases, the web pages would have threat-specific information, conveying risk-reduction strategies to the general public. Such information could be utilized before or after a terrorist incident, and it could be integrated into the curricula for various civic organization (e.g., the Boy Scouts). Notably, the Red Cross has already developed analogous information on its web page related to natural disasters. Besides the educational value of the information, web pages can inform the public on the basic organization of the government in its response to terrorism.

Decision Making Exercises: As the government responds to a terrorist attack, and initiates a public communication campaign, there will be a need for rapid and difficult decision making by public officials and members of the media. For example, what is the most important information to convey? What information, if any, should be withheld? What will be the criteria for withholding information? What is the balance between accurate and detailed reporting and limiting public hysteria? Because answers to these types of question hinge of the details of a terrorist incident, the success of a public communication strategy will depend, in part, on “sensitizing” the participants to the types of decisions that will be required by the government and the media. This can be accomplished through decision

making exercises where government officials and the media carry out their responsibilities in hypothetical situations that simulate the response to a terrorist attack. Ideally, these exercises would be carried by people who will play key roles in responding to a terrorist incident.

Outreach Efforts: Effective publication strategies will depend on strong working relationships between government officials and members of the media. To facilitate these relationships, and to educate the media on key government personnel, it would be valuable for the government to carry out a range of outreach efforts to all sectors of the media.

Defining a Comprehensive Communications Strategy

Taken together, the analyses from these studies indicate that a public communications strategy should be an important component of the government's counter terrorism strategy. Simply put, the task of public dissemination cannot be delegated to the media, because the communication requirements are far more complex than describing facts and relaying information. Rather, public information, proactively shaped by the government, can play a critical role to counter the impacts of a terrorist incident. At this point, the missing element is a comprehensive strategy that defines the government's approach to public communications, and links these efforts to other elements of a counter terrorism plan (e.g., incident management, preparedness efforts, etc.).

Studies performed to date have examined parts of this problem; for example, focusing on communications in response to specific types of threats, or responding to specific needs within the news media. In this setting, we synthesize the conclusions from previous analyses to assemble a "first draft" of the goals for a comprehensive counter terrorism public communications strategy.

- 1) **Preparedness and a public communications strategy for counter terrorism are inextricably linked.** A continuing effort to communicate the risks of terrorism and the types of responses that will be required plays a strong role to promote public preparedness. It also helps prepare the news media for their roles and responsibilities following a terrorist incident.
- 2) **Following a terrorist incident, one of the principal roles of a public communications strategy is to reassure the public that the government is working to restore order and minimize damage.** That is, a public communications strategy is much more than simply reporting the facts, and it will require considerable planning an analysis before an event so that the government and the media can work together effectively.
- 3) **When necessary, convey critical information that the public can use to minimize the impact of an event and speed recovery.** The details of this type of information will depend on the nature of the terrorist incident. It is anticipated that this role for public communications will be especially important during a chemical or biological attack. In these circumstances, it will be important to communicate such information with authority to insure that the public will take necessary actions.
- 4) **There are no "one size fits all" strategies to communicate effectively with the American population.** Because of the diversity in America, public communications efforts should engage a range of strategies to insure that important information is delivered to the largest fraction of the population. A public communications plan should not assume that the media will play the primary role to "translate" a government message into a widely understandable format. This approach will be especially critical when the public needs to quickly assimilate information and take action to reduce impacts of a terrorist attack (e.g., during a biological event).

- 5) **Minimize the disclosure of sensitive information that could reveal vulnerabilities or impede efforts to catch a perpetrator.** In some cases, a public communications strategy will need to focus on information that should not be disseminated because it would have negative ramifications. Identifying and safeguarding such information will be key operational challenges for a public communications strategy during times of crisis.
- 6) **During an incident response, convey that communications efforts are well coordinated and integrated with emergency management activities.** These types of communications, which are qualitative rather than specific, play an important role to reassure the public that the government is responding to a crisis situation.
- 7) **“Feed the beast.” That is, respond to the media’s need for 24/7 information on an important story.** This point, which is emphasized by the media, is important to reduce the appearance of withholding information. It also improves the quality of government relations with the media.
- 8) **Minimize sensational or incorrect reporting.** To effectively shape the tone and accuracy of news reporting following an event, there needs to be continuous monitoring of the media coverage, and direct efforts to counter stories which are viewed as incorrect or unnecessarily inflammatory.

Basic Principles

Carrying out a strategy, such as the one described above, will require large-scale planning and coordination efforts. The following principles should guide such efforts.

- 1) **A lead federal agency should be identified to manage public communications as part of the federal government’s counter terrorism efforts. These responsibilities would continue on an ongoing basis, encompassing both long term preparedness and emergency response communications. The agency would identify strategies to coordinate public information flows, coming from different government sources, in the hectic period following a terrorist attack. In its longer term management role, the agency would have responsibility to define and carry out the government’s public communications plans and programs. These efforts, carried out in coordination with other federal agencies and state and local governments, would play a central role in the federal government’s public preparedness efforts for counter terrorism. In the shorter term, the lead federal agency might delegate its communication responsibilities to another following a terrorist incident (e.g., to transfer communications to an agency with particular technical expertise).**
- 2) **At a higher level, clear authorities and plans should be developed to define the relationship between public communication efforts and emergency response operations following a terrorist incident. Particular attention should be focused on identifying the individual(s) with decisionmaking authority to release or withhold information from the public.**
- 3) **Within the lead agency, the primary individual who will speak for the government should be identified. This person would be the federal government’s spokesperson on terrorism issues on a continuing basis, though this role could be delegated for specific purposes during emergencies (e.g., to particular experts or agencies to speak on well defined technical issues). It is not essential that this person hold a leadership position within the government (e.g., cabinet rank), though it is important that he or she have direct access to key decision makers, analogous to the President’s press secretary. It is critical that communications from this individual be coordinated with other government information flows to enhance operational credibility and minimize public confusion.**

- 4) **Public communications during an emergency situation should be carried out in close coordination with relevant technical experts. Planning should begin immediately to identify specific expert groups to be utilized for different terrorist situations. There should be well defined procedures to transmit the expert advice to high level officials who authorize the release of information to the public.**
- 5) **Different communication plans should be developed for different types of terrorist incidents including biological, chemical, radiological, nuclear, agricultural, cyber, and conventional explosive attacks.**
- 6) **There should be an immediate effort to educate the media and government officials about the types of activities and decision making that required for public communications during the above events. The activities would “sensitize” public officials and the media to difficult issues within a public communications strategy, such as withholding vs. releasing information, compelling the public to take difficult actions under stressful circumstances, countering disinformation activities by terrorists, and using public communications to restore order.**

APPENDIX I– PROGRAMS OF THE FEDERAL EMERGENCY MANAGEMENT AGENCY AND THE DEPARTMENT OF JUSTICE

Introduction

The September 2001 terrorist attacks provided an important impetus to reassess the United States' terrorism preparedness responsibilities. In particular, the establishment of a Department of Homeland Security (DHS) has created a window of opportunity to examine the missions, programs, and effectiveness of government agencies that play an important role in domestic preparedness.

Since September 2001 much has changed in the way the government is structured to handle terrorist incidents and disasters, and more change will come. Three changes are particularly significant for this study. The first was the creation of the Office of Homeland Security (OHS) in the Executive Office of the President to coordinate homeland security policy and programs. This was an important first step to centralize national homeland security efforts. OHS published *The National Homeland Security Strategy* in July 2002, which laid out for the first time a vision for homeland security.³²⁸ Second was the proposal to form a Department of Homeland Security (DHS) to serve as the focal point for homeland security programs and operational issues. And third, the creation of the DHS triggered a move to replace the concepts of consequence management and crisis management with that of “incident management.” Just as the DHS is envisioned to consolidate disparate federal agencies and functions that deal with homeland security, so too does the concept of incident management seek to integrate all aspects of federal response to the threats and consequences of terrorist incidents.³²⁹

This section focuses on the Federal Emergency Management Agency (FEMA) and the Department of Justice (DoJ). As a result of federal restructuring, FEMA and several offices in the DoJ—such as the Office for Domestic Preparedness (ODP), the Immigration and Naturalization Service enforcement functions, and the National Infrastructure Protection Center—will be folded into the DHS. However, these structural changes are not a guarantee that egregious domestic preparedness problems will be fixed. Consequently, this section has three major objectives. First, its primary aim is to offer policy recommendations for the federal government to improve state and local terrorism preparedness. Second, it outlines the domestic preparedness missions and programs of FEMA and DoJ. Third, it examines the effectiveness of their domestic preparedness programs by asking several questions: Are sufficient federal resources for combating terrorism being allocated at appropriate levels and in ways most likely to be effective? Are federal programs and activities adequately addressing the needs of state and local efforts to achieve better preparedness? Is there significant duplication of missions and responsibilities?

Recommendations

We begin by outlining several policy recommendations, which have been compiled after conducting interviews with FEMA and DoJ personnel and examining strategic documents and staffing plans from both agencies.

³²⁸ *National Strategy for Homeland Security* (Washington: Office of Homeland Security, July 2002).

³²⁹ The concept of incident management is envisioned to combine that of crisis management (minus law enforcement functions) and consequence management. See *National Strategy for Homeland Security*, pp. 42. All future references in this document to the consolidation of these two functions into that of incident management will be understood to indicate that law enforcement functions will remain within the DoJ, regardless of the LFA for incident management.

Substantial duplication of grants and training programs continues to exist across the federal government. This includes FEMA and DoJ, as well as such agencies as the Environmental Protection Agency and the Departments of Defense, Energy, Health and Human Services, and Transportation. This duplication decreases efficiency, unnecessarily complicates accountability, and weakens domestic preparedness. *We recommend that the DHS make a long-term, concerted effort to ameliorate redundancies through consolidation. Federal training and grant programs that relate to terrorism response should be integrated within the DHS. Programs tightly tied to the core mission of their parent agency (e.g., HAZMAT programs offered by EPA) that are not moved to the DHS should still be coordinated by the DHS.*

Information sharing between federal agencies and state and local first responders is inadequate. Indeed, interviews with FBI and law enforcement officials suggest that this problem has worsened, rather than improved, since September 11, 2001. *We recommend that a National Counter Terrorism Center (NCTC) improve the collection, synthesis, analysis, and distribution of terrorism-related intelligence information to appropriate state and local officials.*

There is an egregious absence of common standards for domestic preparedness training courses, equipment, and trainers across the United States. This has compromised interoperability and preparedness by causing such problems as inadequate training and incompatible equipment. *We recommend that the DHS establish an inter-agency working group that includes representatives from the private sector and state and local governments to set minimal performance standards for training courses, equipment, and trainers.*

The large number of training and grant programs located in different agencies of the federal government make it difficult for first responders to determine what opportunities exist for training and resources. *We recommend that the DHS establish one office that is the single federal POC for local and state agencies seeking information on training and grant opportunities for homeland security and related subjects. This office should provide its clients with real-time information about training and grant programs offered by all agencies of the federal government.*

There are no sufficient, agreed-upon measurements for evaluating the readiness of state and local first responders. Field exercises, after action reviews (AARs), and other types of evaluations are invaluable ways to train first responders in realistic scenarios and to assess the effectiveness of current courses and grants. *We recommend that the DHS increase the number and quality of comprehensive terrorism field exercises for states and major metropolitan areas. It should also work with state and local governments to create a process that develops standardized templates and evaluation material that can be used by jurisdictions throughout the United States.*

Federal Emergency Management Agency

The Federal Emergency Management Agency (FEMA) has encompassed two primary missions regarding terrorist incidents, which will change with its integration into DHS and the creation of incident management. First, it has been the lead federal agency (LFA) for consequence management following a domestic terrorist incident. This included the responsibility for taking over as on-scene manager for the federal government in situations when the FBI transferred the lead role to FEMA. Both Presidential Decision Directive 39 (PDD-39) in 1995 and Presidential Decision Directive 62 (PDD-62) in 1998 formalized FEMA's role as the LFA in managing and coordinating the consequence management response to terrorist attacks in support of state and local authorities.³³⁰

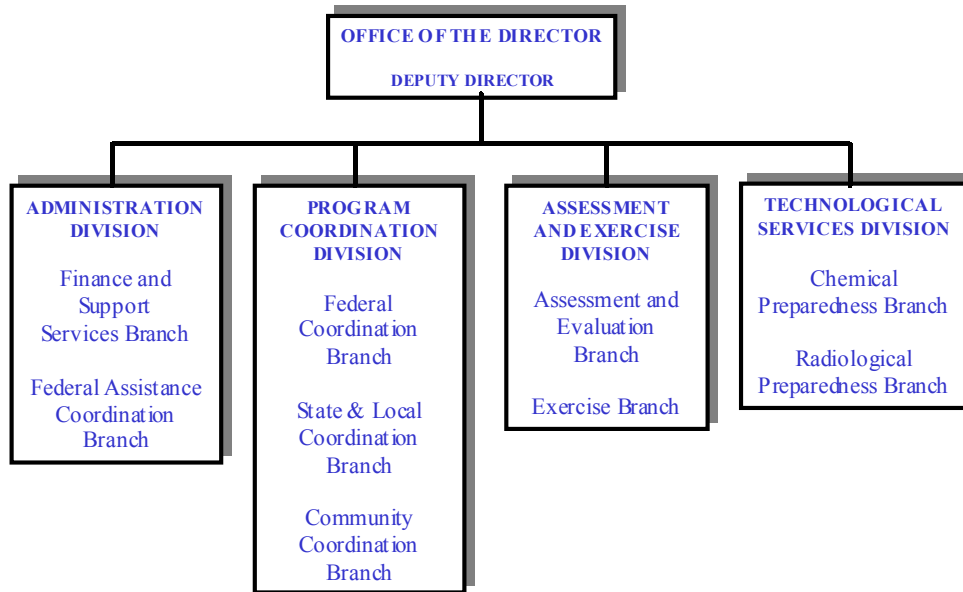
³³⁰ *Presidential Decision Directive 39* (Washington: The White House, 1995); *Presidential Decision Directive 62* (Washington: The White House, 1998). Also see *United States Government Interagency Domestic Terrorism Concept of Operations Plan (CONPLAN)*, January 2001.

Second, FEMA has played a critical role in domestic preparedness for terrorist incidents. As PDD-39 notes:

The Director of the Federal Emergency Management Agency shall ensure that the Federal Response Plan is adequate to respond to the consequences of terrorism directed against large populations in the United States, including terrorism involving weapons of mass destruction. FEMA shall ensure that States' response plans are adequate and their capabilities are tested.³³¹

Indeed, PDD-39 and PDD-62 gave FEMA the responsibility to ensure that states are adequately prepared to respond to domestic terrorist incidents. This mission was reinforced in 2001 when President George W. Bush asked FEMA to establish the Office of National Preparedness (ONP) to “coordinate all Federal programs dealing with weapons of mass destruction consequence management” and to “work closely with state and local governments to ensure their planning, training, and equipment needs are addressed.”³³² The ONP was tasked to help coordinate domestic preparedness programs within the Departments of Defense, Health and Human Services, Justice, and Energy, the Environmental Protection Agency, as well as other federal agencies.

Figure 1: The ONP's Organizational Structure



Programs: As Table 1 illustrates, FEMA’s total budget for terrorism-related activities in FY2002 was \$38.6 million. Its programs for domestic preparedness can be broken down into two types. The first include training courses such as those offered by the Emergency Management Institute (EMI) and the National Fire Academy (NFA) in Emmitsburg, Maryland. EMI’s audience includes a broad range of full-time FEMA employees; on-call personnel; state, local, and tribal officials; personnel from other federal departments and agencies; and others who play a role in emergency response. Its courses are designed to enhance the preparedness of first responders for a variety of scenarios — including terrorism incidents. Courses geared specifically to terrorism include “Senior Officials Workshop on Terrorism,” a series titled “Weapons of Mass Destruction,” and “Emergency Response to Criminal and Terrorist Incidents.”

³³¹ Presidential Decision Directive 39, p. 8.

³³² See President Bush’s comments on May 8, 2001 in *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822 (Washington: General Accounting Office, September 2001), p. 166.

The National Fire Academy focuses predominantly on improving the preparedness of fire officials and the emergency response community. It offers courses at its resident facility in Emmitsburg, Maryland, and at various locations throughout the United States in cooperation with state and local fire training organizations and colleges and universities. Specific terrorism courses include “Emergency Response to Terrorism” for command officers and emergency medical services.

Table 1: FEMA Terrorism Preparedness Budget

	FY2001 Actual (millions US\$)	FY2002 Enacted (millions US\$)	Emergency Response Fund (millions US\$)
Combating Terrorism	\$28.7	\$36.0	\$35.0
Critical Infrastructure Protection	1.6	1.5	0.0
Continuity of Operations	1.2	1.2	0.0
Unconventional Threats Total	31.5	38.6	35.0

Source: *Annual Report to Congress on Combating Terrorism* (Washington: Office of Management and Budget, June 2002).

The second type of program includes grants to state and local governments to support a range of domestic preparedness activities. Furthermore, the Assistance to Firefighters Grant program supports basic firefighting and equipment needs of local fire departments and fire service organizations. Furthermore, the Citizens Corps Initiative programs offer grants to assist individuals and communities in implementing a number of homeland security programs in their areas.³³³ Prominent examples include:

- Volunteers in Policy Service Program
- Neighborhood Watch Program
- Medical Reserve Corps
- Community Emergency Response Teams (CERT)

Department of Justice

The Department of Justice has at least three primary missions for terrorist incidents, some of which will change with restructuring. First, it plays an important role in preventing terrorist acts. As noted in its *Strategic Plan 2001-2006*, the DoJ’s primary anti-terrorist mission is to “prevent, disrupt, and defeat terrorist operations before they occur.”³³⁴

Second, as laid out in PDD-39 and PDD-62, it has been the lead federal agency for crisis management.³³⁵ This responsibility, which was handed over to the FBI, authorized it to designate a federal on-scene commander once a domestic terrorist incident has occurred to coordinate the US government response with federal, state, and local authorities. While PDD-39 and PDD-62 made some progress toward clarifying the role of government agencies with respect to terrorist incidents, the distinction between “crisis management” (DoJ’s responsibility) and “consequence management” (FEMA’s responsibility) was too vague. Indeed, the President’s *National Strategy for Homeland Security* explicitly aims to “consolidate existing federal government emergency response plans into one genuinely all-discipline, all hazard plan -- the Federal Incident Management Plan -- and thereby eliminate the ‘crisis management’

³³³ Other FEMA grants related to domestic preparedness include the Chemical Stockpile Emergency Preparedness Program (CSEPP) and the Radiological Emergency Preparedness (REP) Program.

³³⁴ *Strategic Plan 2001-2006* (Washington: Department of Justice, 2002), p. 17.

³³⁵ *Presidential Decision Directive 39; Presidential Decision Directive 62.*

and ‘consequence management’ distinction.”³³⁶ As the LFA for incident management, the DHS should become the lead agency for domestic preparedness training.

Third, the Department of Justice has also played a role in domestic preparedness. The 1998 Appropriations Act (Public Law 105-119) authorized the Attorney General to provide “training and related equipment for chemical, biological, nuclear, and cyber attack prevention and response capabilities to State and local law enforcement agencies” and to provide “bomb training and response capabilities to State and local law enforcement agencies.”³³⁷ In April 1998 the Attorney General delegated this authority to the Office of Justice Programs (OJP). Within the OJP, the Office for Domestic Preparedness (ODP) is primarily responsible for enhancing the capacity of state and local jurisdictions to respond to — and mitigate the consequences of — incidents of domestic terrorism.³³⁸ The Bureau of Justice Assistance, National Institute of Justice, and Office for Victims of Crime also have domestic preparedness responsibilities within OJP. Other components of the Justice Department that play a role in domestic preparedness include the Criminal Division and the United States Attorneys office.

Programs: As Table 2 highlights, the DoJ’s terrorism budget for FY2002 was \$1.7 billion -- more than double the figure for FY2001. The FBI’s portion was the largest, reflecting its primary role in identifying and countering threats to the US and serving as the LFA for terrorism investigations and crisis management. Since September 11, 2001, it has substantially increased its terrorism resources by devoting more money and agents to counterterrorism and counterintelligence, though it has been criticized for failing to perform a comprehensive threat assessment facing the US.³³⁹

Table 2: DoJ Terrorism Preparedness Budget

	FY2001 Actual (millions US\$)	FY2002 Enacted (millions US\$)
Criminal Division	\$4	\$4
FBI Construction	0	5
FBI	595	1,063
General Administration	0	6
Counterterrorism	47	5
OJP (ODP)	91	646
US Attorneys	0	3
Total	737	1,732

Source: *FY 2001 Performance Report & FY 2002 Revised Final, FY03 Performance Plan* (Washington, US Department of Justice, 2002), p. 4.

³³⁶ *National Strategy for Homeland Security* (Washington: Office of Homeland Security, July 2002), p. 42.

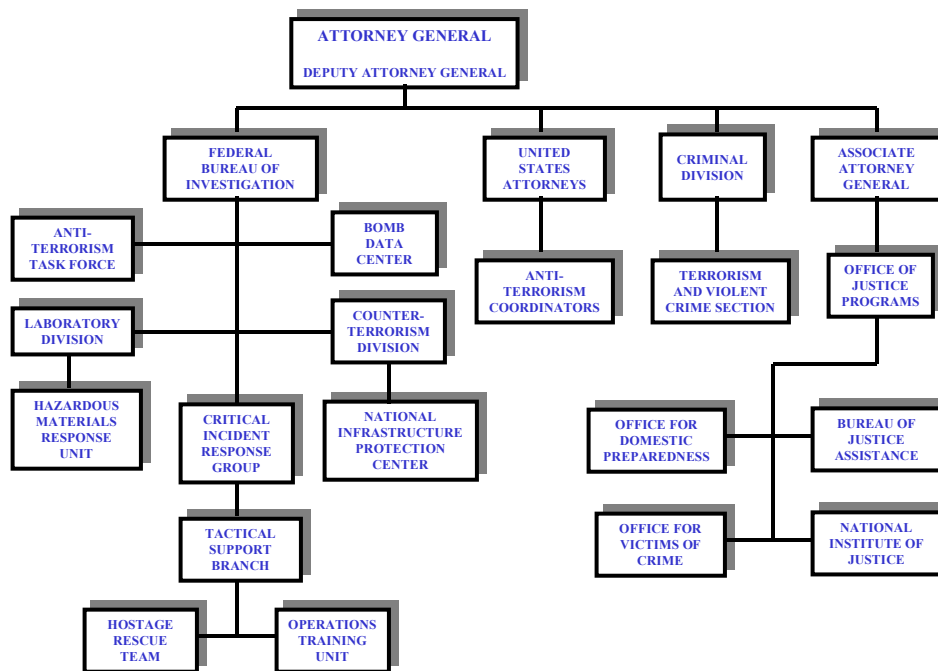
³³⁷ *Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 1998* (Public Law 105-119, November 26, 1997), p. 2441. The 2001 CONPLAN likewise noted that the Department of Justice is responsible “for ensuring the development and implementation of policies directed at preventing terrorist attacks domestically.” CONPLAN, p. 2.

³³⁸ The USA Patriot Act of 2001 noted that the ODP “shall make a grant to each State, which shall be used by the State, in conjunction with local government, to enhance the capability of State and local jurisdictions to prepare for and respond to terrorist acts.” *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, p. 335.

³³⁹ See, for example, *A Review of the Federal Bureau of Investigation’s Counterterrorism Program: Threat Assessment, Strategic Planning, and Resource Management*, Report No. 02-38 (Washington: Office of the Inspector General, September 2002).

The FBI has several components that are directly involved in domestic preparedness. First, Anti-Terrorism Task Forces (ATTFs) were created within each FBI jurisdiction to coordinate the counterterrorism activities of law enforcement agencies throughout the country.³⁴⁰ Second, the National Infrastructure Protection Center (NIPC), which is located within the Counter-Terrorism Division, serves as the focal point for threats or attacks against America’s critical infrastructures. It also coordinates training for cyber investigators and infrastructure protectors in government and the private sector. Third, the Tactical Support Branch, which is composed of the Hostage Rescue Team and the Operations Training Unit, ensures that the FBI has a trained, national-level tactical team capable of being deployed to conduct rescue operations. Fourth, the Bomb Data Center collects and reports bombing information to public safety agencies, elected officials, and the public. Moreover, it trains public safety bomb personnel at the Hazardous Devices School in Huntsville, Alabama. Fifth, the Hazardous Materials Response Unit of the FBI responds to criminal incidents involving the use of HAZMATs, and trains, equips, and certifies field office personnel for HAZMAT operations.

Figure 2: The DoJ and Domestic Preparedness



There are several other components of DoJ that have domestic preparedness responsibilities. The US Attorneys offices, through their Anti-Terrorism Coordinators, help coordinate the dissemination of information and the development of a prosecutorial strategy involving federal law enforcement agencies, state and local police forces, and other state agencies and officials throughout the country. Furthermore, the Terrorism and Violent Crime Section of the Criminal Division coordinates interagency efforts to designate terrorist organizations and investigate and prosecute them.

Finally, ODP has established a series of training programs and grants to fulfill its mission to train, equip, and provide technical assistance to state and local first responders. The ODP provides direct training and technical assistance to state and local jurisdictions to enhance their capacity and preparedness to respond

³⁴⁰ The Anti-Terrorism Task Force includes representatives from the FBI, INS, DEA, Marshals Center, Customs Service, Secret Service, and Bureau of Alcohol, Tobacco and Firearms. See *Strategic Plan 2001-2006* (Washington: Department of Justice, 2001), p. 17.

to domestic incidents. One of the primary ways has been through the National Domestic Preparedness Consortium (NDPC), which consists of several training centers.

- **Center for Domestic Preparedness (CDP):** CDP offers specialized advanced training to state and local first responders in the management and remediation of incidents of domestic terrorism, particularly those involving chemical agents and other toxic substances. It is the only location in the US where first responders can be trained in a contaminated environment using “live agents” (actual toxic substances). Located at Fort McClellan in Anniston, Alabama, the CDP offers such courses as “Weapons of Mass Destruction Technical Emergency Response,” “Weapons of Mass Destruction Hazardous Materials Technician,” and “Weapons of Mass Destruction Incident Command.”
- **Energetic Materials Research and Testing Center at the New Mexico Institute of Mining and Technology (EMRTC):** EMRTC is the lead NDPC partner for explosives and firearms, and it offers field exercises and classroom instruction. The course “Incident Response to Terrorist Bombing,” for example, is designed to give technical-level firefighters, law enforcement personnel, and other emergency first responders the skills and knowledge necessary to evaluate and respond to incidents of terrorism involving WMD — especially those involving explosives or incendiaries.
- **Academy of Counter-Terrorist Education at Louisiana State University (ACE):** ACE focuses on specialized training programs in the areas of WMD law enforcement response, public health emergencies, and biological related incidents. It offers a number of courses such as “Law Enforcement Response to WMD Incidents” and “Emergency Response to Domestic Biological Incidents.”
- **Texas Engineering Extension Service at Texas A&M University (TEEX):** TEEX provides a number of courses to prepare public officials, emergency medical services, law enforcement, fire protection, and public works for the threat posed by WMD. Examples include: “WMD: Incident Management,” “Preparing for and Responding to Terrorism/Weapons of Mass Destruction,” and “Internet-Terrorism Awareness.”
- **US Department of Energy’s Nevada Test Site (NTS):** In conjunction with the Department of Energy, NTS conducts large-scale field exercises using a wide variety of live agent stimulants and explosives. Courses cover advanced HAZMAT training and radiological/nuclear agents.

Table 3: ODP Equipment and Exercise Grants

Equipment and Exercise Grants	FY2002 Amount (millions US\$)
Nunn-Lugar-Domenici	\$2.6
TOPOFF II	7.0
State & Other Equipment Grant Program	112.7
State & Local Bomb Technician Equipment Program	10.0
Exercises	295.2
Total	427.5

Source: FY2002 CJS Appropriations Act, Conference Report 107-278; FY2002 Department of Defense/Supplemental Appropriations Act, Conference Report 107-350.

The ODP also provides assistance to state and local jurisdictions by offering equipment and exercise grants. FY2002 figures are included in Table 3. Funds are designed to improve the capabilities of state and local responders by covering the cost of WMD exercises and purchasing a range of domestic preparedness equipment such as WMD technical assistance equipment, communications equipment, and personal protective wear.

In 2000 President Clinton designated the Attorney General as the lead federal official responsible for administering the Nunn-Lugar-Domenici Domestic Preparedness Program.³⁴¹ This responsibility was handed to ODP, which oversees grants to the nation's 120 largest cities for receipt of training, exercise, and equipment monies to enhance their response to WMD incidents. Furthermore, the Domestic Preparedness Equipment Grant Program provides funding for a variety of equipment: PPE, chemical, biological, and radiological detection, decontamination, and communications equipment. Jurisdictions that currently receive funding include all 50 states, the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of Northern Mariana Islands, Guam, and the US Virgin Islands. Other types of domestic preparedness grants include the BJA's Byrne Formula Grant Program, which can be used by state and local governments to support counter-terrorism initiatives; and the BJA's Local Law Enforcement Block Grants Program, which can be used to procure law enforcement equipment and to support multi-jurisdictional task forces.

Figure 3: Cities Targeted by Nunn-Lugar-Domenici Funding³⁴²



Preparedness Goals

This section offers seven major recommendations for improving domestic preparedness efforts across the United States. They include: 1) integrating federal preparedness efforts; 2) improving intelligence sharing; 3) establishing training standards; 4) creating equipment standards; 5) initiating teaching

³⁴¹ Title XIV of the *National Defense Authorization Act of 1996* (P.L. No. 104-201) initially authorized the Department of Defense to act as the interagency lead to develop the Nunn-Lugar-Domenici program. However, in April 2000 the President shifted this responsibility to the Department of Justice, effective in October 2000.

³⁴² Source: Monterey Institute of International Studies.

standards; 6) establishing a single point of contact for information; and 7) increasing interagency field exercises and evaluations.

1. INTEGRATE FEDERAL PREPAREDNESS EFFORTS: One of the DHS's most important priorities should be to integrate and centralize federal terrorism preparedness efforts across the country. In the past, preparedness efforts have been hampered by the absence of a single federal oversight office. The move to coordinate terrorism preparedness efforts within the Office for Domestic Preparedness is an important step. But it does not *ipso facto* solve the duplication problem.

Indeed, there is currently far too much duplication, confusion, and inefficiency because of the plethora of government agencies involved in preparedness and the lack of coordination among them. As highlighted in the *Assessment of Federal Terrorism Preparedness Training* report in 2002, at least 7 different government agencies administer over 150 federal training courses on weapons of mass destruction.³⁴³ These include the Department of Defense (22 courses), the Department of Energy (37 courses), the Department of Health and Human Services (13 courses), FEMA (52 courses), the Department of Justice (27 courses), the Environmental Protection Agency (10 courses), and the Department of Transportation (6 courses).

As highlighted in this report, FEMA has administered funding through the Assistance to Firefighters Grant program and the Citizens Corps Initiative programs. Likewise, ODP has offered funding to state and local officials through several grants: the Nunn-Lugar-Domenici Domestic Preparedness Program, the State and Local Domestic Preparedness Equipment Support Program, the County and Municipal Agency Domestic Preparedness Equipment Support Program, and the Domestic Preparedness Equipment Program. There is also considerable overlap among clients. The availability of training and grants should be viewed from the perspective of the clients — state and local governments. Unfortunately, most of the training courses and grants target the *same* clients: emergency management (such as mayors, city council, and county commissioners), firefighters, HAZMAT teams, law enforcement, EMS, health and medical personnel, and public works.

A good case of duplication is the Nunn-Lugar-Domenici program. The Department of Defense was initially charged with overseeing the program, even though it expressed serious reservations because domestic WMD preparedness and response operations were a distraction from its core war-fighting mission. While people involved in the program in 1996 and 1997 assumed that it would be transferred to FEMA because of its consequence management role, the Clinton Administration transferred the program to the DoJ in October 2000. However, several months later the Bush Administration asked FEMA to create the Office of National Preparedness to coordinate federal programs dealing with WMD consequence management. In sum, both the executive and legislative branches have contributed to the duplication and decentralization of domestic preparedness activities. As Amy Smithson and Leslie-Anne Levy conclude in their report *Ataxia: The Chemical and Biological Terrorism Threat and the US Response*: “The terrorism issue and the US bureaucracy tasked with addressing it is notorious for being a convoluted maze of agencies, bureaus, task forces, and working groups.”³⁴⁴

We recognize, of course, that there are millions of first responders — such as law enforcement, firefighters, HAZMAT technicians, and Emergency Medical Service personnel — who must be prepared to respond to terrorist incidents. The problem is neither that there are so many programs nor that they cover the same areas such as WMD. Rather, the problem is that there is no centralization and little inter-agency coordination. This results in inadequate baseline training and equipment standards, decreased

³⁴³ *Assessment of Federal Terrorism Preparedness Training* (Washington, DC: Federal Emergency Management Agency, April 2002).

³⁴⁴ Amy E. Smithson and Leslie-Anne Levy, *Ataxia: The Chemical and Biological Terrorism Threat and the US Response*, Report No. 35 (Washington, DC: The Henry L. Stimson Center, October 2000), p.154.

efficiency, and weakened domestic preparedness. This predicament is primarily a function of the ad hoc manner in which Congress has doled out domestic preparedness grants.³⁴⁵ Indeed, Congressional funding has been given to a number of federal agencies with insufficient attention to centralization and coordination.³⁴⁶ The result is an amalgam of redundant programs controlled by legislation that federal agencies are obliged to implement as ordered and using the funds provided in each year's appropriation. Furthermore, the executive branch has until recently been unwilling to develop a national strategy for domestic preparedness.

Consequently, it is critical that the DHS develop a national strategy and doctrine for domestic preparedness.³⁴⁷ This should include answers to the following questions: What are the most significant terrorism threats to the US homeland? What are the appropriate domestic responses to those threats? What are the primary objectives for ensuring domestic preparedness if a terrorist attack occurs? Such steps as the replacement of consequence management and crisis management with that of "incident management" are important. But much more needs to be done, as the next six recommendations indicate.

2. IMPROVE INTELLIGENCE SHARING: There must be substantial improvement in the sharing of terrorism-related intelligence information between federal agencies and state and local levels. Current information and intelligence practices neither transfer to local authorities the information they need, nor adequately take into account information collected by local authorities. Moreover, regional threat information should be specific enough for local jurisdictions to act upon.

In particular, interviews with FBI and law enforcement officials for this report suggest that there has not been a significant increase in intelligence-sharing between the two since September 11, 2001 -- and there may actually be a decrease in cooperation. At least two factors have contributed to this problem. First, considerable animosity lingers between the FBI and law enforcement. Much of this is rather banal and sophomoric. As one FBI agent put it: "Many state and local police officers continue to view the FBI as an organization staffed with incompetent, white-collar agents that possess little real-world experience. And a number of FBI officials consider police officers uneducated, inept, and inadequately prepared to deal with weighty issues such as terrorism."

Second, there continues to exist a security clearance problem: most police departments don't have enough officers with the necessary security clearances to view and process classified information on terrorist activity. This problem also inhibits the sharing of sensitive information between federal agencies and emergency responders that are not in law enforcement. Both of these factors -- lingering animosity and security clearance problems -- have stalled significant intelligence-sharing.

An important step would be the creation of a National Counter Terrorism Center (NCTC), which would be tasked with the collection, analysis, and distribution of intelligence information on terrorist threats. As the June 2002 *Department of Homeland Security* strategy paper acknowledged:

Multiple intelligence agencies analyze their individual data, but no single government entity exists to conduct a comprehensive analysis of all incoming intelligence information and other key

³⁴⁵ See, for example, Richard A. Falkenrath, "Problems of Preparedness: U.S. Readiness for a Domestic Terrorist Attack," *International Security*, Vol. 25, No. 4, Spring 2001, pp. 147-186; *Report of the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction* (Washington, DC: Government Printing Office, July 1999).

³⁴⁶ *Bioterrorism: Federal Research and Preparedness Activities*, GAO-01-915 (Washington: General Accounting Office, September 2001).

³⁴⁷ On general United States grand strategy see Michael E. Brown, Owen R. Coté, Sean M. Lynn-Jones, and Steven E. Miller, eds., *America's Strategic Choices* (Cambridge, MA: MIT Press, 2001).

data regarding terrorism in the United States. There is no central clearinghouse to collect and analyze the data and look for potential trends.³⁴⁸

The NCTC would be an important step toward establishing efficient and comprehensive intelligence collection; increasing transparency between federal, state, and local officials; and improving overall information-sharing. However, it will still be a difficult task to break down cultural and territorial barriers between federal, state, and local levels where there remains mutual mistrust and animosity.

3. ESTABLISH TRAINING STANDARDS: The DHS should adopt baseline proficiency standards for terrorism training throughout the country. Numerous first responders, who were trained at FEMA and DoJ facilities and interviewed for this report, acknowledged that there continues to be a notable absence of common standards for domestic preparedness training programs across the United States. The major reason for this deficiency is the duplication of programs among federal agencies and the lack of inter-agency coordination.

As used here, “training standards” refer to minimal proficiency levels that first responders should be expected to achieve. Of course, standards should vary depending on the type of first responders (such as police officers or firefighters) as well as the nature of the incident (such as chemical or biological attacks). First responders constitute the front line when a terrorist attack occurs, and it is critical that they achieve at least minimal standards of competency in training classes. Federal agencies lack the resources to train all of the millions of first responders throughout the country, and much of the training that occurs is beyond their purview. For example, the Center for Domestic Preparedness has directly trained 18,000 first responders since 1998.³⁴⁹ In FY2001 FEMA trained 8,000 personnel at its Emmitsburg, Maryland campus.³⁵⁰ While important, these figures are a tiny percentage of the total set of first responders.

The vast majority of first responders are trained at the state and local level. Since most of the training is “indirect,” it is critical that the DHS develop common performance standards to ensure that first responders are meeting at least minimal levels of proficiency. The DoJ’s Office for Domestic Preparedness has taken steps in this direction by compiling baseline performance standards for first responders dealing with WMD incidents.³⁵¹ Unfortunately, this is insufficient since first responders are trained in diverse courses at the federal, state, and local level.

4. CREATE EQUIPMENT STANDARDS: The DHS should adopt and enforce common equipment standards. The absence of baseline equipment standards continues to be problematic. For instance, first responders often receive training on one type of PPE at institutes like EMI and CDP, but have PPE that is substantially different and not interoperable in their jurisdictions — or perhaps no viable PPE at all. A number of reports that examined the response to the September 11 terrorist attacks in New York City and Washington, DC, argued that the absence of common standards created serious problems with equipment compatibility. As one FEMA report noted:

Standards are critical in many key areas. For example, in too many instances — including the response to the World Trade Center attack — first responders and government officials were not able to fully communicate because of differing communication standards, and mutual aid was hindered by incompatible equipment.³⁵²

³⁴⁸ *The Department of Homeland Security* (Washington, DC: The White House, June 2002).

³⁴⁹ Numbers are from the Center for Domestic Preparedness in Anniston, AL.

³⁵⁰ Numbers are from the Emergency Management Institute in Emmitsburg, MD.

³⁵¹ The standards are outlined in *Emergency Responder Guidelines* (Washington, DC: Office for Domestic Preparedness, 2002).

³⁵² *A Nation Prepared: Federal Emergency Management Agency Strategic Plan, Fiscal Years 2003-2008* (Washington, DC: FEMA, 2002), p. 3.

Indeed, communications systems at the local level are neither adequate nor interoperable. In particular, rural areas often can't afford modern technology and lack the communications infrastructure that supports security planning and operations.

Part of the problem is that there has been little cooperation between the federal government and the private sector — including equipment manufacturers and industry officials — to ensure common standards. The DHS can play a critical role in creating integrated equipment standards. Currently, the National Institute for Occupational Safety and Health (NIOSH) and the Occupational Safety and Health Administration (OSHA) have taken some steps in this direction. However, NIOSH is located in the Department of Health and Human Services and OSHA in the Department of Labor, and neither has the power or the authority to enforce standards. It would be helpful to have equipment standards set by one integrated federal agency that can enforce them. Standards should include equipment used for the detection of WMD, protection from toxic agents, and decontamination of WMD incidents. Without such equipment standards, there are several costs. First, it can be difficult for first responders purchasing equipment to know what works as advertised and is adequate for emergency response. Second, first responders may be trained on one type of equipment, but use incompatible equipment in their own jurisdictions. Third, problems encountered in New York City and Washington in September 2001 demonstrate that the absence of standards creates significant interoperability problems.

Finally, shortfalls continue to exist in the effectiveness, interoperability, and supply of PPE. Several first responders expressed concern that currently available PPE fails to offer adequate protection against biological and infectious disease emergencies, as well as the intense heat of fires. Following the September 11, 2001, attacks in New York City, emergency workers at the World Trade Center site noted that PPE provided little protection against the persistent dust and heat.³⁵³ Moreover, there is concern that federal caches contain an inadequate supply of PPE, and local responders and supplemental units are not fully equipped with ample boots, gloves, and powered air-purifying respirators (PAPRs).³⁵⁴

5. INITIATE STANDARDS FOR TRAINERS: The DHS should adopt common certification standards for domestic preparedness trainers. The current absence of certification requirements makes it difficult — if not impossible — to ensure that trainers are adequately qualified to teach first responders. Indeed, public school teachers throughout the United States must be certified following mandatory competency tests and professional coursework that develop skills needed for classroom teaching.³⁵⁵ This includes instruction in areas such as teaching methodologies, curriculum development, and classroom management. In the area of terrorism preparedness, standards should be developed to facilitate effective teaching and not to micromanage instructors. Domestic preparedness trainers should be competent in at least three areas. First, they need to possess the technical skills necessary to teach specific courses such as response to chemical or nuclear attack. Second, trainers should have real-world experience as first responders. Third, they must demonstrate at least a minimal ability to instruct others.

6. ESTABLISH A SINGLE INFORMATION SOURCE: The DHS should be the single point of contact (POC) for information on federal training programs and grants. First responders have repeatedly complained that the duplication of federal preparedness efforts makes it difficult, confusing, and inefficient to acquire information about training programs and grants. Small municipalities and states do not have the manpower to search for training and grant opportunities in every federal department and

³⁵³ Brian Jackson et. al. *Protecting Emergency Responders: Lessons Learned from Terrorist Attacks*, CF-176-OSTP (Santa Monica, CA: RAND, 2002).

³⁵⁴ On supply problems see *Arlington County: After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon*, pp. 13, A-16, A-18, A-41, A-43,

³⁵⁵ In the State of California, for example, the California Commission on Teacher Credentialing is responsible for conducting certification activities and developing preparation and performance standards for elementary and secondary teachers (see www.ctc.ca.gov).

agency. One office should be established in DHS that is the single federal point of contact for local and state agencies seeking information on training and grant opportunities for homeland security and related subjects. This office must provide its clients with real-time information about the availability of training programs and grants offered by all agencies of the federal government. While some first responders are able to acquire reliable information about grants and training from single POCs in their home states, there is no integrated federal source of information.

7. INCREASE INTERAGENCY EXERCISES AND EVALUATIONS: The DHS needs to increase the number and quality of comprehensive interagency field exercises and evaluations to monitor the preparedness of first responders and the effectiveness of its training programs and grants.³⁵⁶ With thousands of jurisdictions in the United States, it is not possible or even desirable for the federal government to administer exercises and evaluations to all of these entities. However, exercises are an invaluable way to assess the readiness of first responders and train them in ways that are more “realistic” than classroom settings.³⁵⁷ While some tabletop and field exercises have been performed in the last few years — such as the TOPOFF exercises in 2000 — there has been an insufficient number of interagency field exercises to evaluate the preparedness of responders for terrorist incidents.³⁵⁸

In addition to holding exercises, it is critical that self-evaluations are performed using informal “hot washes,” which give key leaders a chance to promptly assess the exercises in face-to-face settings, or more formal after action reviews (AARs). FEMA has begun to take some steps in compiling this information by establishing the Emergency Management Exercise Reporting System (EMERS), an automated system that records the results of state and local exercises and actual disasters in 13 functional areas. However, EMERS is designed only for state and local use. It is also important that the DHS work with other federal agencies involved in domestic preparedness to develop common standards for exercises and evaluations conducted throughout the United States.

Federal officials have acknowledged in interviews that they need to conduct more frequent and robust field exercises, and report that they are currently in the process of fixing the problem. At the same time, they note substantial barriers to holding effective exercises. For example, first responders must be freed from their daily responsibilities in order to participate. Policymakers have often been reluctant to bear the high costs of conducting such exercises and backfilling the on-call duties of those personnel involved in the exercises. Without these exercises and standards, however, the vast majority of jurisdictions will have an uneven level of preparedness at best. At worst, critical functions will not be exercised and evaluated.

VI. The Long-Term Success of DHS

The concluding section examines the terms and conditions under which DHS will be successful regarding domestic preparedness for terrorist incidents. It does this by asking a series of questions related to the recommendations outlined at the beginning of the report. Indeed, DHS’s ability to achieve its stated mission of coordinating a national homeland security strategy and ensuring greater accountability will

³⁵⁶ See also *Combating Terrorism*, GAO-01-822, especially pp. 59-89.

³⁵⁷ As one report on the September 11 attack on the Pentagon concluded, the Arlington County Fire Department was “a better-prepared and more capable response force on the morning of September 11 than might otherwise have been the case. Regular and frequent *participation in exercises* and other activities with neighboring jurisdictions has produced sound working relationships that were evident during the Pentagon response.” *Arlington County: After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon* (Arlington, VA: Titan Systems Corporation, 2002), p. A-74 (emphasis added). Also see p. A-77.

³⁵⁸ TOPOFF 2000 was a congressionally-directed field exercise in May 2000 sponsored by the Department of Justice and FEMA. It was designed to evaluate the nation’s crisis and consequence management capacity, and included three scenarios: a radiological incident in the Washington, DC metropolitan area; a chemical incident in Portsmouth, NH; and a biological incident in Denver, CO.

partly hinge on its success in decreasing duplication, increasing intelligence sharing, establishing common standards, centralizing information, and evaluating readiness.

CONSOLIDATION: The success of DHS will partly be a function of its ability to decrease egregious and unnecessary duplication among federal agencies. We expect DHS to take the necessary steps toward answering the following questions:

- Has DHS succeeded in reducing the duplication of missions among federal agencies?
- Do agencies such as FEMA and ODP continue to have overlapping missions regarding domestic preparedness for terrorist incidents?
- Do agencies have unnecessarily redundant programs such as training courses or grants?
- Are most federal programs centralized within one agency?
- Is there sufficient coordination among agencies involved in domestic preparedness?
- What clients do agencies serve? Do they overlap?

INTELLIGENCE SHARING: The terrorist attacks in September 2001 provided a strong incentive to increase intelligence sharing between federal agencies and state and local officials. Unfortunately, this has not happened. Intelligence sharing continues to be inadequate both horizontally (across federal agencies) and vertically (from federal to state and local levels):

- Is there a single federal repository and clearinghouse for data regarding cyber, chemical, biological, and other WMD threats?
- Is adequate intelligence information being distributed to state and local levels? Or is it a one-way process?

SINGLE SOURCE OF INFORMATION: One consequence of duplication is the absence of a single point of contact for state and local agencies searching for information on training and grant opportunities. As part of its mission to serve as the focal point for homeland security programs and operational issues, DHS should set up an office designed to ameliorate this problem. The following questions are therefore critical:

- Has DHS established one office that is the single POC for state and local agencies seeking real-time information on training programs and grants?
- Is it easily accessible by state and local agencies via such mediums as the internet?
- Is DHS doing all it can to ensure that state and local agencies are aware of this office and its services?

COMMON STANDARDS: DHS also needs to make notable progress in ensuring the existence of common standards in three areas: preparedness training, equipment, and trainers. Consequently, satisfactory answers to the following questions are important:

- Have minimal proficiency standards been developed for domestic preparedness training programs across the country?
- Are training courses available on weekends and at night near responders' jurisdictions so that they are accessible to volunteers and others with limited resources?
- What basic and essential functions should first responders in various areas -- search and rescue, triage, emergency medical services, decontamination, etc. -- be able to perform in response to terrorist incidents?
- Are baseline standards in place to ensure compatible communication and equipment?
- Have they been developed in collaboration with experts who will be expected to meet them?
- Is there a certification process to teach preparedness training courses?

READINESS AND EXERCISES: The establishment of common standards are a first step toward improving the capability of first responders. The next step involves testing and ensuring readiness through training, exercises, and evaluations.

- Is DHS ensuring that states, US territories, and major metropolitan areas are conducting an adequate number of exercises to prepare for terrorist incidents and ensure that standards are being met?
- Do the exercises involve all relevant agencies so that interoperability is maximized?
- Are there adequate after action reviews?
- Have quantitative measures been developed to assess the preparedness and vulnerability of states, cities, and regions for terrorist attacks?

APPENDIX J– U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES INITIATIVES TO SUPPORT STATE AND LOCAL TERRORISM PREPAREDNESS PROGRAMS

Introduction

In the aftermath of the September 11th and the anthrax-related attacks, it became abundantly clear that our public health system, which operates at the federal, state, and local levels, was ill prepared to respond to future terrorist attacks. Moreover, results from a recent study that relied on survey data gathered on behalf of the Gilmore Commission suggest that public health response capabilities at the local level have been inadequately addressed (Davis and Blanchard, 2002). The study’s authors conclude that local public health agencies and hospitals are “unaware of what types of capabilities or surge capacity may be required [and] do not have plans for communicating with other health providers, emergency responders, or the public.” Similarly, after years of cutbacks, state public health agencies’ efforts to confront the terrorist threat are now “beginning from a standing start” (Inglesby, 2002).

Hospitals, too, are ill prepared to respond to incidents involving chemical, nuclear, or biological weapons. A recent study of hospital emergency departments found, for example, that fewer than 20 percent had plans in place for addressing chemical or biological events, less than half had integral decontamination units, and most did not have adequate respiratory protective equipment for the emergency departments’ staff (Wetter et al., 2001).

Against this backdrop, we examined issues surrounding the nature and level of federal government support – provided through the U.S. Department of Health and Human Services (DHHS) – for state and local efforts to prepare for and respond to terrorist attacks. Under the Federal Response Plan – which assigns federal agencies, and some non-governmental organizations, with responsibility for leading the federal response to a wide range of emergencies – DHHS has been designated the lead federal agency for addressing the medical and public health consequences of all mass casualty events, regardless of their origins. DHHS is responsible for activities related to epidemic detection and response; maintaining and securing the National Pharmaceutical Stockpile; conducting research aimed at improving training and health services delivery; and assisting local, state, and federal agencies in their efforts to respond to emergencies (Thompson, 2002). The Department’s programs in these areas are administered by the Centers for Disease Control and Prevention (CDC), the National Institutes for Health (NIH), the Office of Emergency Preparedness (OEP), the Health Resources and Services Administration (HRSA), the Substance Abuse and Mental Health Services Administration (SAMHSA), the Agency for Healthcare Research and Quality (AHRQ), and the Food and Drug Administration (FDA) (Allen, 2002). In addition, in October 2001, the Secretary of the Department of Health and Human Services established the Office of Public Health Emergency Preparedness (OPHEP) to coordinate DHHS’ terrorism-related activities. In fiscal year 2002, DHHS spent \$3.0 billion for its terrorism preparedness activities; the President’s budget request for FY03 was \$4.3 billion.

The remainder of this paper is organized as follows. In the next section, we describe DHHS’ programs to support state and local governments’ efforts to combat terrorism. The following section describes the data sources and methods used to conduct the analysis. The fourth section reports our results, and the last section is devoted to discussing our conclusions and policy recommendations.

Description of Key DHHS Programs to Combat Terrorism

DHHS administers a range of programs that, broadly speaking, provide funds to state and local governments that can be applied to prepare for, and respond to, a broad range of terrorist attacks. For example, through the Centers for Disease Control and Prevention, DHHS expends over \$350 million annually to assist state and local health authorities in investigating and controlling outbreaks of

communicable diseases, chronic diseases, and preventable health conditions. Similarly, through DHHS' Health Resources and Services Administration's State Rural Hospital Flexibility Program, nearly \$25 million per year is spent on assisting states with rural communities to develop and implement rural health plans, develop networks of care, and improve emergency medical services, among other things.

While these and other DHHS programs clearly provide resources to states and local governments that can be brought to bear in preparing for, and responding to, terrorist attacks, there are a handful of programs that are more directly related to these objectives. These include the Metropolitan Medical Response System (MMRS), the National Disaster Medical System (NDMS), and the Disaster Medical Assistance Teams (DMAT). MMRS, which was established in 1996, focuses on enhancing emergency preparedness systems at the local level—in general, through the integration of local health and medical response system resources (both public and private) – to better respond to weapons of mass destruction (WMD) incidents. The program currently operates in 122 metropolitan areas nationwide.

The National Disaster Medical System, which is administered by DHHS' Office of Emergency Preparedness (OEP), is designed to offer a single, integrated medical response capability to assist state and local governments in providing medical services following a natural or terrorist-related disaster. The main objectives of the NDMS are as follows: to provide health, medical, and related social services to disaster areas; to evacuate patients who cannot be cared for in the affected areas; and to provide hospitalization services in both federal and non-federal hospitals that have agreed to accept patients from disaster areas (U.S. Department of Health and Human Services, 2002a). A key component of the NDMS is the Disaster Medical Assistance Teams, or DMATs. DMATs are groups of medical and support personnel that can be deployed to a disaster area on short notice, generally eight hours or less.

While technically distinct from one another, the MMRS and NDMS programs are designed to work together in some important ways. For example, in principle, when an incident occurs in an MMRS area, patients would be transported to regional hospitals using NDMS resources.

DHHS also funds several programs aimed at improving the level of electronic connectivity among public health organizations. Examples of these programs include the Laboratory Response Network (LRN), which connects over 80 public health laboratories in order to quickly identify pathogens used in bioterrorist attacks; the Health Alert Network (HAN), an Internet-based communications system to facilitate information sharing and distance-learning that links public health departments covering more than 90 percent of the nation's counties; the National Electronic Data Surveillance System (NEDSS), a federal initiative aimed at promoting the adoption of data and information system standards in disease surveillance systems used at the federal, state, and local levels; and the Epidemic Information Exchange (Epi-X), a secure, Internet-based system that enables state health departments to communicate with CDC. Additionally, DHHS, through the National Institutes of Health, is conducting research on bioterrorism agents and countermeasures that can be used to respond to the release of these agents. While this research program, which is mainly located within the National Institute of Allergy and Infectious Diseases, is not explicitly geared to supporting state and local efforts to prepare for and respond to terrorist attacks, clearly the expected outputs of the research program – including new vaccines and other therapeutic agents as well as diagnostic tests – will benefit state and local governments. In FY 2002, the NIH budget to support bioterrorism research was approximately \$275 million; the President's FY03 budget request for this research program is just under \$1.75 billion (National Institutes of Health, 2002).

Prior to September 11th, DHHS funding for state and local preparedness programs was quite limited. For example, in FY 2001, CDC allocated a total of \$66.7 million to support preparedness planning, surveillance and epidemiology; enhance laboratory capacity; and improve communications activities (see Salinsky, 2002; U.S. General Accounting Office, 2002). Additionally, the Office of Emergency Preparedness' (OEP) FY 2001 budget for programs aimed at combating terrorism amounted to just over \$27 million, over \$17 million of which went to the MMRS.

While the OEP budget nearly doubled in FY 2002, the cornerstone of DHHS support to states and local governments, and the main emphasis of our analysis of this support, is a set of bioterrorism preparedness cooperative agreements – focusing on public health and hospital preparedness – totaling just over a billion dollars. Initial grants of \$205 million were released to the 50 states, the District of Columbia, and 3 cities in late January 2002, an additional \$744 million was released in June, and approximately \$40 million remains to be distributed. The funds are to be spent by grantees by the end of August 2003.

CDC is administering the public health cooperative agreements, which account for approximately 87 percent of the \$1 billion awarded, while HRSA is administering the hospital preparedness agreements. It is interesting to note that DHHS chose cooperative agreements, as opposed to grants or contracts, as the funding vehicles. This choice represents a conscious decision on the part of federal officials to acknowledge the importance of creating federal, state, and local partnerships. As articulated in a guidance document for state officials: “A cooperative agreement is an award instrument of financial assistance where ‘substantial involvement’ is anticipated between the HHS awarding agency and the recipient during performance of the contemplated project or activity. ‘Substantial involvement’ means that the recipient can expect Federal programmatic collaboration or participation in managing the award” (U.S. Department of Health and Human Services, 2002). Under the agreements, states are not required to contribute their own funds to the program. However, federal funds cannot be used to supplant any current state or local public health-related expenditures.

The purpose of the CDC cooperative agreements is to “upgrade state and local public health jurisdictions’ preparedness for and response to bioterrorism, other outbreaks of infectious disease, and other public health threats and emergencies” (Centers for Disease Control and Prevention, 2002). CDC’s overall approach towards the cooperative agreements closely follows the recommendations made by its Strategic Planning Workgroup on preparedness and response to biological and chemical weapons (Khan et al., 2000).

Proposals were reviewed to ensure that 14 public health “critical benchmarks” (see Figure 1) were met and that applicants addressed the extent to which various “critical capacities” were in place and, if not, how they would be developed and implemented during the budget period. The public health cooperative agreements were designed to support state and local activities in the following “Focus Areas:” preparedness planning and readiness assessment, surveillance and epidemiology capacity, laboratory capacity (for both biologic and chemical agents), Health Alert Network/communications and information technology, communicating health risks and health information dissemination, and education and training.

Figure 1. Critical Benchmarks for Bioterrorism Preparedness Planning

Public Health Preparedness (CDC)

1. Designate a Senior Public Health Official within the State health department, to serve as Executive Director of the State Bioterrorism Preparedness and Response Program.
2. Establish an advisory committee with members from a variety of health agencies and first responders.
3. Prepare a timeline for the development of a statewide plan for preparedness and response for a bioterrorist event, infectious disease outbreak, or other public health emergency.
4. Prepare a timeline for the assessment of statutes, regulations, and ordinances within the state and local public health jurisdictions regarding emergency public health measures.
5. Prepare a timeline for the development of a statewide plan for responding to incidents of bioterrorism.
6. Prepare a timeline for the development of regional plans to respond to bioterrorism.
7. Develop an interim plan to receive and manage items from the National Pharmaceutical Stockpile, including mass distribution of antibiotics, vaccines and medical material.
8. Prepare a time line for developing a system to receive and evaluate urgent disease reports from all parts of the state (or city) and local public health jurisdictions on a 24- hour per day, 7 days per week basis.
9. Assess current epidemiologic capacity and prepare a timeline for providing at least one epidemiologist for each metropolitan area with a population greater than 500,000.
10. Develop a plan to improve working relationships and communication between Level A (clinical) laboratories and Level B/C laboratories, (i.e. Laboratory Response Network laboratories) as well as other public health officials.
11. Prepare a timeline for a plan that ensures that 90 percent of the population is covered by the Health Alert Network (HAN).
12. Prepare a timeline for the development of a communications system that provides a 24/7 flow of critical health information among hospital emergency departments, state and local health officials, and law enforcement officials.
13. Develop an interim plan for risk communication and information dissemination to educate the public regarding exposure risks and effective public response.
14. Prepare a timeline to assess training needs--with special emphasis on emergency department personnel, infectious disease specialists, public health staff, and other health care providers.

Hospital Preparedness (HRSA)

15. Designate a Coordinator for Bioterrorism Hospital Preparedness Planning.
16. Establish a Hospital Preparedness Planning Committee to provide guidance, direction and oversight to the State health department in planning for bioterrorism response.
17. Devise a plan for a potential epidemic in each state or region. Recognizing that many of these patients may come from rural areas served by centers in metropolitan areas, planning must include the surrounding counties likely to impact the resources of these cities.

Source: U.S. Department of Health and Human Services, HHS Fact Sheet, June 6, 2002.

The purpose of the HRSA hospital preparedness cooperative agreements is to “upgrade the preparedness of the Nation’s hospitals and collaborating entities to respond to bioterrorism ... The prime focus will be on identification and implementation of bioterrorism preparedness plans and protocols for hospitals and other participating health care entities” (Health Resources and Services Administration, 2002). As shown in Figure 1, three “critical benchmarks” were used to review the proposals submitted by the states, territories, and selected municipalities.

The HRSA cooperative agreements comprise two phases. The first consists of a needs assessment aimed at gauging the level of preparedness of hospitals and other medical services providers to respond to a bioterrorist attack. Once the needs are identified, a plan of action must be developed. The second phase involves undertaking activities to implement the plan developed in phase one. This phase is intended to result in states being able “to upgrade the ability of hospitals and other health care entities to respond to biological events, to develop a multitiered system in which local health care entities are prepared to triage, treat, stabilize and refer multiple casualties of a bioterrorist event to identified centers of excellence, or to develop multistate or regional consortia to pool limited funding to accomplish these goals” (Health Resources and Services Administration, 2002). State health departments are obligated to allocate the overwhelming majority of the funds they receive for hospital preparedness to hospitals, community and rural health centers, emergency medical systems, and poison control centers, provided these various entities support the hospital systems’ efforts to respond to a bioterrorist attack.

Data Sources and Methods

Our analysis of DHHS’ support of state and local governments’ efforts to prepare for, and respond to, terrorist events relied on information gathered through a series of interviews that we conducted between July and October 2002. In approximately half of the cases, a senior RAND staff member conducted the interviews in person. The remaining interviews were conducted over the telephone. Prior to conducting the interviews, we developed a list of candidate interviewees by contacting individuals who were experts in the field of emergency preparedness and response and asking them to identify appropriate people to interview in various DHHS agencies, state and local health departments, national organizations representing these departments, and academic institutions and research organizations. We then called these initial contacts, conducted interviews with them, and inquired about additional contacts. This process continued until we had contacted, and arranged appointments with, 23 interviewees who were judged to be extremely knowledgeable about the relevant issues.

The interviewees included seven federal health officials, five state and three local public health and emergency preparedness officials, five staff members of organizations representing state and local public health officials, two academics/health policy researchers, and one physician who directs several hospital emergency rooms in a major metropolitan area. The state and local health officials were drawn from agencies located in five states, and the emergency room physician worked in a sixth state.

The interviews varied considerably in length, but generally ran between 45 and 90 minutes. In addition to the interviews, we attempted to collect all relevant documentary evidence from DHHS and other sources, including copies of program descriptions, testimony before Congressional committees, policy analyses, position papers, and so on.

We used a semi-structured protocol to conduct the interviews, a copy of which is included in Appendix A. This protocol served to organize note taking, ensure that all relevant topics were covered, and provide a consistent approach to data collection across interviewees. The interviews covered a wide range of topics, including:

- background on the interviewees’ history with terrorism preparedness activities;
- the general policy making environment;
- descriptions of recent and current initiatives related to preparing for, or responding to, terrorist attacks;
- strategies for evaluating the initiatives;
- the roles played by various federal, state, and local stakeholders;
- the relationship between statewide and local initiatives; and
- areas for improvement in the quality and level of support that DHHS offers state and local governments for preparing for, and responding to, terrorist threats and attacks.

We provided all interviewees with a strict confidentiality assurance. We told them that we would neither cite them by name in our reports, nor provide any information in those reports that would allow readers to deduce their identity. Additionally, we promised not to share their comments with other interviewees or with individuals not directly involved with the analysis. For these reasons, we have not included a list of interviewees in this report.

In synthesizing the information generated through the interviews and the document reviews, we focused on identifying a set of themes or lessons learned regarding DHHS' role in terrorism preparedness that can be applied by the Administration, the Congress, and state and local public health policymakers.

As with any research methodology, the qualitative approach that we have taken in this analysis has certain inherent limitations. The study, for instance, was not designed to formally test research hypotheses or to be generalizable to the experiences of all state and local health officials who are grappling with the threat of terrorism. Resource constraints limited the number of individuals we could interview and the number of federal, state, and local agencies visited.

While we believe that we interviewed a sample of very knowledgeable and influential people, we recognize that we have no way of assessing whether their views on the issues discussed mirror those of the larger population of people who are responsible for formulating and executing public health policy towards terrorist events.

As a result of these limitations, we have taken conservative approach in reporting our findings and in crafting our policy recommendations. Specifically, we have chosen primarily to report those findings and make those recommendations that, in some sense, represent the majority point of view among interviewees. The one exception to this is that we have also reported findings and communicated recommendations that were generated either through our analysis of written materials or that were suggested by a relatively small number – in some case even one – interviewees who we judged to be either exceptionally knowledgeable about a particular issue or who expressed a viewpoint that we believed was critical to be heard.

Results

The results of the interviews revealed a remarkable degree of consistency with respect to a number of key issues. Not surprisingly, federal officials portrayed an overwhelmingly positive view of their programs aimed at supporting state and local bioterrorism preparedness efforts. On the other hand, state and local officials – as well as staff members of organizations representing these officials – presented a decidedly mixed picture of the federal government's performance in this area. Here, it is important to note that the primary focus of the interviewees was on the public health and hospital preparedness cooperative agreements, with far less attention being devoted to other DHHS initiatives that directly or indirectly affect terrorism preparedness. To a great extent, the disproportionate amount of attention being paid the cooperative agreements is due to the fact that the level of funding for these agreements far exceeds the sum total of the other initiatives, and that the agreements' objectives are viewed as critical to ensuring our nation's health and safety.

In general, our discussions with the stakeholders that we interviewed revolved around the following: the level and stability of DHHS support for terrorism-related activities, technical assistance, evaluation plans and objectives, and organizational and operational issues. In the subsections below, we address each of these topics, in turn.

Level and Stability of DHHS Support

There was a broad consensus among interviewees that DHHS should receive high marks for distributing both the public health and hospital preparedness cooperative agreement funds efficiently and equitably. In an uncharacteristic move, DHHS released 20 percent of the funds in late January 2002, weeks before the notice and guidance documents were issued and approximately two and a half months before the plans were due to DHHS (on April 15, 2002). Most of the remaining funds were distributed in June, with a small amount being held in reserve until additional requirements were met. A number of interviewees commented that they had never seen the federal government respond to any problem with such rapidity.

For the most part, interviewees believed that the roughly \$900 million in funding going to public health cooperative agreements was sufficient to make a meaningful start in the process of rebuilding and reconfiguring the nation's public health system to better respond to terrorist attacks. However, the majority of the interviewees suggested that this process was not something that could be accomplished overnight, as the public health system, in their view, has been largely decimated over the last 20 years. This view is consistent with the conclusions reached by the Institute of Medicine in their 1988 report *The Future of Public Health* (Institute of Medicine, 1988), which characterized the system as being in a state of "disarray," with little consensus on what constitutes the mission and content of public health, although there was general agreement that the public health system was in distress from diminished resources and declining public esteem.

The majority of the respondents expressed the concern that bioterrorism-related threats will receive a disproportionate level of attention and resources vis-à-vis other types of public health threats (including chemical and radiological attacks and naturally occurring disease outbreaks), despite the program's stated objective of including "other outbreaks of infectious disease, and other public health threats and emergencies." Others, however, argued that the public health infrastructure improvements that will be made using the grants could be equally applied to the full array of public health threats. Moreover, they maintained that it was appropriate for DHHS to focus on the bioterrorism threat because other agencies and funding sources – including FEMA, local "first responders," and others – have addressed chemical, radiological, and explosive threats to a greater extent than bioterrorist ones.

The degree to which the so-called "dual use" philosophy – where funds are used to support increasing the overall capacity of state and local governments in the areas of disease surveillance, infection control, risk communication, and the like as well as increasing their ability to respond to terrorist attacks – is embraced will vary from state to state and even across locales within a state. There was considerable concern, however, on the part of some respondents that the nature of the cooperative agreements program will bias states and locales against making investments in certain areas, such as increasing chemical and radiological laboratory capacity. They noted that the incentives created by the agreements will inevitably lead to distortions in the public health system as well as a series of "unintended consequences," in the words of one respondent. Here, a particular concern centered on the prospect that public health workers would be drawn, or bid, away from family planning, sexually transmitted disease, tuberculosis control, chronic disease programs, infant mortality reduction efforts, and other programs to fill bioterrorism preparedness positions.

On a broader level, an influential emergency preparedness policymaker argued that the bioterrorism preparedness program was misguided in that it further encouraged a "stove piping" mentality among officials at all levels of government, which, in turn, inhibited them from "ratcheting up the dialogue to talk about the entire threat matrix." This individual went on to state that DHHS has done a poor job in integrating both its programmatic efforts and the public health perspective, in general, into the overall emergency response structure. Evidence to support this assertion was provided by a number of interviewees who maintained that DHHS has done a very poor job in coordinating activities with FEMA,

in particular, as well as other federal agencies, including the Departments of Justice, Agriculture, and State.

There was a strong consensus among interviewees that it will take at least a five-year commitment, and approximately \$1 billion per year, on the part of DHHS to have a material impact on the degree to which states and local governments are prepared to respond to bioterrorist events. Interestingly, respondents also believed that the public health preparedness program was being funded at about the “right” annual level, arguing that while the need to develop the public health infrastructure to better prepare for and respond to terrorist acts was acute, it would be difficult to absorb the funds if the funding rate was increased appreciably. As it is, respondents reported that they were having difficulty finding qualified people to fill newly-created positions, evaluating and purchasing new communications and information systems, and so on.

There was a concern on the part of the vast majority of local officials interviewed that the distribution of funds between state and local governments favored the states because they were the formal grant recipients and, in the words of one respondent, tended to “take care of their needs first.”³⁵⁹ The cooperative agreement proposals showed considerable variation with respect to the proportion of funds that states planned to provide to local health departments. DHHS officials indicated that they would be monitoring the degree to which commitments to local public health agencies were met and to ensure that the fraction of funding going to these agencies increased over time.

In addition to providing the required resources and allowing sufficient time for the states and locales to hire staff and to acquire new equipment, a sustained funding commitment over a five-year period of time or greater was judged to be critical in allowing states and local governments to attract and retain first-rate individuals and to invest an appropriate amount of money in new technologies. Many reported that long-term funding uncertainties presented a formidable barrier in their attempts increase their levels of preparedness. This problem is further exacerbated by the presence of severe state budget constraints, which increase the difficulties associated with making long-term plans.

In contrast to the public health cooperative agreements, the hospital preparedness cooperative agreements were viewed as being inadequately funded (i.e., \$125 million for FY 2002), with many, if not most, of the respondents arguing that DHHS, and HRSA in particular, has unrealistic expectations for their program, as articulated in the guidance documents, given what was viewed as a relatively meager level of support.

Because relatively little money – on average, approximately \$25,000 per year – will be available for individual hospitals, several respondents noted that there may be a tendency to “go for the low-hanging fruit,” in the words of one, and purchase communications or decontamination equipment in instances where the money could better be used, say, to increase surge capacity, to upgrade and expand information technology systems, and to improve coordination among local hospitals and health care providers. In fairness, federal officials have recognized the inadequacy of the funding level; as a result, they have requested \$500 million for FY03. Still, some experts believe that even this level of funding would not be sufficient to prepare the nation’s 5,000 hospitals to handle mass casualty events, mainly because hospitals, like public health agencies, have responded to fiscal pressures by cutting back on staff and other resources and otherwise reducing “excess capacity” (O’Toole, 2002).

³⁵⁹ Separate grants were made to the three largest metropolitan areas: New York, Los Angeles, and Chicago. The degree to which these cities will coordinate their preparedness activities with their corresponding State efforts remains to be seen. Although DHHS encouraged applicants to coordinate activities within and between States – including those conducted by the Metropolitan Medical Response Systems (MMRS) – and required Governors to review all cooperative agreement proposals and, upon their approval, submit letters of support to DHHS, no formal mechanisms were established to ensure that such coordination actually takes place.

Technical Assistance

There was a broad consensus among respondents, including a number of key federal officials interviewed, that the quality and quantity of technical assistance provided by the federal government to both state and local governments was sorely lacking. Several respondents voiced the concern that the lack of technical assistance would cause states and locales to do a poor job in developing and executing their preparedness plans. Respondents identified a number of areas where there is a critical need for federally-provided technical assistance, including information technology, risk communication, program evaluation, education and training, and methods of establishing appropriate partnerships with private sector entities such as pharmaceutical and biotechnology companies, laboratories, managed care organizations, and physicians. That is, as mentioned above, while respondents generally believed that they were provided with a sufficient level of resources to begin the job of establishing a reasonable capacity for responding to a bioterrorist attack, many felt that they lacked the expertise to, for example, select among competing technologies, develop templates for communicating risks and information on actual events to the public, and provide adequate training to staff. All of this has been exacerbated by the fact that aggressive vendors have been inundating state and local officials with promotional materials and requests for meetings.

Along these lines, a number of interviewees suggested that federal officials should make a greater effort to establish standards for communications systems, information technologies, and even laboratory protocols. Critics also pointed out that the CDC needs to provide assistance in coordinating and connecting some of its own laboratory and disease surveillance information systems initiatives (e.g., NEDSS, LRN, HAN, Epi-X). In addition to the obvious efficiencies that would be achieved by preventing the 54 grantees from “reinventing the wheel,” the promulgation of standards would also reduce the training required when staff are transferred, or redeployed, from one state or locale to another, which would produce enormous benefits in the event of an actual attack.

Respondents were particularly concerned about the states’ ability to receive and distribute products from the CDC’s National Pharmaceutical Stockpile (NPS), which is composed of twelve 50-ton “Push Packages” of medical supplies placed throughout the country that can be deployed to any location within 12 hours. The NPS program is also responsible for storing and distributing smallpox vaccine. Once packages from the NPS arrive at an airfield, CDC transfers authority for managing the contents of the packages to state and local officials.

Federal officials indicated that a number of states came up short in their cooperative agreement proposals with respect to their plans for stockpile receipt and distribution, including the rapid vaccination of the entire population. Several interviewees suggested that there is an acute need on the part of state and local health officials for technical assistance in developing and exercising these plans, as they would be relied upon, for instance, to ensure that the entire population could be rapidly immunized in the event of a smallpox attack.

A final area where technical assistance of the part of the federal government is apparently lacking is in developing regional approaches to bioterrorism preparedness. That is, a number of respondents noted that to be truly effective, public health and hospital preparedness plans must account for resources that can either be borrowed from, or loaned to, neighboring states. Additionally, these individuals maintained that DHHS should be responsible for providing assistance on inter-state planning and for creating various mechanisms and forums for state and local officials to share ideas and best practices with their counterparts in other states and locales. The development of effective regional strategies may also require the federal government to provide technical assistance regarding appropriate legal frameworks to enhance both inter- and intra-state collaborations.

One potentially valuable source of technical assistance to the states and local governments is a system of 15 academic Centers for Public Health Preparedness, which are typically housed within schools of public health. In fiscal year 2002, DHHS, through CDC, spent \$20 million to support the Centers. The Centers' mission is essentially to ensure that the nation's public health workforce is prepared to respond to terrorist threats and events. The Centers plan to accomplish this by offering relevant courses (both on-site and through distance learning programs), conducting research and evaluation efforts, and disseminating best practices.

Evaluation Plans and Objectives

There is currently no framework in place for monitoring the states' progress in meeting the objectives of the cooperative agreements program and for evaluating states' performance with respect to various outcomes, although federal officials have indicated that they are working to develop evaluation protocols. Moreover, there is a general lack of understanding on the part of representatives from state and local governments on precisely what they will be held accountable for and how their programs will be evaluated.

It is important to recognize, however, that an appropriate balance needs to be struck between accountability and collaboration with DHHS and other federal agencies. That is, on the one hand, DHHS must ensure that the cooperative agreement funds are being spent appropriately. In this regard, DHHS must first perform essentially an auditing function to ensure that the funds are being devoted to activities designed to meet the objectives of the cooperative agreements and that the funds are not being used to supplant existing state commitments. Second, DHHS must make an effort to measure the effectiveness of each state's programs and to document the lessons learned for other states.

On the other hand, due to the nature of the cooperative agreements, DHHS has a responsibility for working hand-in-hand with the states to maximize their chances of success. This requires that DHHS use its resources to provide a myriad of types of technical assistance to the states. Here, it is interesting to note that DHHS has not identified the various processes and outcomes that it will be held accountable for, although the guidance documents list various activities that DHHS staff will undertake. Admittedly, from an evaluation perspective, it may be difficult to tease out the federal from state roles and contributions, but that should be of secondary importance relative to the overall goal of increasing our collective capacity to prepare for and respond to terrorist attacks.

Many of the respondents voiced a high level of frustration with respect to DHHS' evaluation plans, or more accurately the lack of such plans. One observer noted that DHHS needs to develop a common taxonomy for measuring program, as opposed to fiscal, accountability. Others expressed concern over the need for DHHS to articulate appropriate program outcomes, how one would go about measuring progress towards reaching them, and a time line for achieving particular milestones. One respondent went so far as to say that both HRSA and CDC have not heretofore articulated many of the critical ingredients comprising the various plans called for in the cooperative agreements' guidance documents.

Organizational and Operational Aspects of DHHS Support to State and Local Governments

To its credit, DHHS recognizes the need to better coordinate its public health and hospital preparedness functions, both internally and with other federal agencies. The founding of the Office of Public Health Emergency Preparedness (OPHEP) is an important step in this direction. However, much work in this area remains to be done. Key interviewees both within and outside of DHHS acknowledged, for instance, that the "disconnect in command and control within DHHS," as one interviewee put it, that was evident immediately after 9/11 and the anthrax attacks has yet to be fully corrected. Several respondents noted that there is still considerable uncertainty regarding the CDC's and OPHEP's roles in coordinating DHHS' bioterrorism preparedness activities. This uncertainty has led to a number of problems on the part

of state and local public health officials. Several such officials expressed a high level of frustration with respect to the ability to gain access to, and communicate with, federal officials who are in a position to render timely decisions on a range of issues. In other words, DHHS has not yet been able to offer cooperative agreement recipients “one-stop shopping.” As a result, state and local public health officials reported that they often find themselves in the position of searching for appropriate contacts in the Office of Public Health Emergency Preparedness, CDC, OEP, and HRSA to have their questions answered and to obtain technical assistance.

DHHS has taken a number of steps to encourage collaboration within states. For instance, as noted above, there is an expectation that states will devote a significant, and growing, proportion of their funds to local public health agencies. Second, in developing their cooperative agreement proposals, states were required to provide evidence demonstrating their plans for coordinating their preparedness activities with local public health agencies, as well as a plan for integrating funds received from HRSA for the hospital preparedness program, CDC for the public health preparedness program, and OEP for the Metropolitan Medical Response Systems. Furthermore, the cooperative agreement proposals were reviewed by inter-agency DHHS teams to ensure that the individual proposals complement one another and that other federal public health preparedness activities are adequately addressed and accounted for.

Another area where improved coordination is critical is the nexus between first responders and public health agencies. Here, both the public health and hospital preparedness cooperative agreements were viewed by many as providing an opportunity to, in many ways, legitimize and promote the function of public health officials in the eyes of first responders. By providing resources to add to and upgrade local information technology and communications systems, DHHS has, in effect, enabled public health officials to increase their visibility at the local level and to make more explicit the nature of the contributions that they can make to enhancing overall local preparedness to respond to terrorist attacks. Concomitantly, local public health officials acknowledged that their role in this regard still requires clarification, and they are looking to DHHS for guidance on how their relationships with local law enforcement agencies and emergency medical services units can be improved.

While coordination between and among all levels of government is vital to establishing an effective national response to terrorism, perhaps an equally vital component is a common strategic vision and plan. In this regard, DHHS efforts have been disappointing, as many interviewees – even some of the federal officials interviewed – lamented the absence of a comprehensive vision and plan, which, in their view, should cover at least a five-year time horizon.

On a more concrete level, several respondents noted that DHHS even failed to prioritize the various components of the cooperative agreements, leaving state and local official in a quandary over where they should devote their resources. Additionally, DHHS has not effectively defined roles for federal, state, and local public health officials. Moreover, with the exception of the hospital preparedness cooperative agreements that require states to work with hospitals, DHHS has offered states virtually no guidance to states on how, and with whom, to establish private sector partnerships. Finally, a number of key policymakers pinpointed information technology as an area in desperate need of a long-range vision and plan, with one observer noting that despite years of trying, CDC has been unable to create a unified public health information system. This individual went on to describe the current patchwork of such systems simply as “a mess.”

Conclusions and Policy Solutions

Our analysis of DHHS’ role in supporting state and local efforts to plan for, and respond to, terrorist attacks leads to a number of conclusions and policy recommendations. First, the federal government, in general, and DHHS, in particular, should be commended for rapidly implementing a series of cooperative agreements with the states that promises to make an enormous contribution toward increasing our nation’s

capacity to protect our citizens from terrorist acts. Second, while we have identified specific areas for improvement, it is clear that DHHS officials are acutely aware of many of them and are currently in the process of taking measures to rectify any perceived deficiencies. In fact, in the few short months that this project was underway, we have already seen evidence of these actions.

At the same time, it is clear that in the rush to distribute funds, DHHS has failed to address certain critical issues – ones that will ultimately determine the degree we are successful in increasing the capacity of state and local governments to respond to terrorist events. To begin with, under ideal circumstances a strategic vision and plan would be in place before the first dollar is expended, or at least very early on the funding process. Such a plan would detail the goals and objectives of the programs; the roles to be played by federal, state, and local officials; how individual components would be integrated with one another; how public health and hospital preparedness plans would dovetail with those of first responders; and measures that could be undertaken to ensure that investments made to counter each type of public health threat (e.g., bioterrorism) could be contribute to countering other types of threats.

Second, DHHS has fallen short in its efforts to provide states and local governments with an adequate level of technical assistance. It is not enough to simply distribute large sums of money and trust that the recipients will know how the funds can best be applied, especially in an area as complex as countering terrorist threats.

Third, it is critical for officials at all levels of government to obtain information on effective and ineffective practices. Toward that end, DHHS must develop and implement a comprehensive evaluation framework and provide technical assistance on evaluation issues and strategies to state and local officials so that they, too, can play a role in evaluating the programs they initiate. Moreover, an effective dissemination strategy should be put in place to ensure that all stakeholders know how to they are expected to contribute to the evaluation effort and understand precisely what they will be held accountable for.

In light of our findings and conclusions, we believe that the following recommended courses of action would speed DHHS' progress in supporting state and local governments' terrorism preparedness activities:

- The Congress and the Administration should make a long-term commitment to fund state and local programs to prepare for, prevent, and respond to bioterrorist and other potential terrorist attacks (including chemical and radiological). The commitment should last for at least five years, with an annual funding level of approximately \$1 billion.
- DHHS needs to articulate a clear, long-term vision of a system for preparing for and responding to terrorist events – including specifying the roles of federal, state, and local agencies – and to provide a strategic plan for developing that system.
- DHHS should increase its efforts to meet state and local technical assistance needs related to all of the public health cooperative agreements' Focus Areas (i.e., preparedness planning and readiness assessment, surveillance and epidemiology capacity, laboratory capacity, Health Alert Network/communications and information technology, communicating health risks and health information dissemination, and education and training). Furthermore, to support the hospital preparedness program, DHHS should also provide technical assistance to states and hospitals that have received state funds. In particular, hospitals need technical assistance in developing surge capacity, linking hospital disease surveillance systems with public health surveillance systems, identifying rare diseases, training staff, enhancing facility security, creating regional partnerships, and developing the ability to quickly deliver medications and vaccines to a large populations.

- DHHS needs to create a detailed plan for monitoring, and evaluating the effectiveness of, the state and local governments' performance under both the public health and hospital preparedness cooperative agreements. The criteria for evaluating performance need to be made explicit and communicated clearly and effectively.
- The Administration should delineate its plans for holding DHHS accountable for expenditures made under, and outcomes that result from, the public health and hospital preparedness cooperative agreements.
- The Administration should assign an individual to each state to serve as that state's liaison for public health preparedness. The liaison would be responsible for ensuring that state public health officials have timely access to appropriate federal officials, that all questions regarding the use of cooperative agreement funds and program objectives are addressed, and that the state's technical assistance needs are met. The state liaisons should also be responsible for creating linkages between the federal government and other state public health functions to minimize the degree to which "stove piping" of various public health activities occurs.
- Given the natural tension that exists in conducting cooperative agreements between program monitoring and evaluation and the degree of collaboration between federal officials and grantees, DHHS should contract with an external research organization to conduct an evaluation of the preparedness cooperative agreements program. Such an evaluation would be aimed at improving the performance of both DHHS and the grantees.

Finally, we believe that the Gilmore Commission should undertake additional research on DHHS' terrorism preparedness programs. Specifically, we recommend that a project be undertaken to examine, in detail, how individual states are using the federal bioterrorism preparedness funds. In particular, such a study should seek to: 1) understand how the states are modifying their public health systems to respond more effectively to a terrorism attack; 2) examine the external environmental factors influencing states' spending decisions; 3) assess the internal organizational dynamics of public health agencies and hospitals that constrain a state's ability to respond to terrorism and other public health threats; 3) identify alternative organizational structures for delivering public health services; 4) recommend concrete strategies for addressing the implications of terrorism-related threats to public health; and 5) identify how states have reached out to the private sector in an effort to enhance their ability to respond to a terrorist attack. The study should also address the degree to which the funds are being applied to prevent and combat bioterrorism-related threats vis-à-vis chemical, radiological, and explosive ones; the overall level of preparedness for responding to each of these types of threats; the extent to which state and local governments have embraced the "dual use" philosophy in their efforts to rebuild and strengthen their public health systems; and the degree to which some of the "unintended consequences" referenced earlier have arisen.

TAB 1—INTERVIEW GUIDE FOR DHHS REVIEW

Programs in Support of State and Local Efforts to Respond to Terrorist Attacks

I. BACKGROUND

- A. History of the respondent's activities
 - 1. Previous involvement in area
 - 2. Changes in strategies over time

- B. The general policy environment
 - 1. How would you characterize the general policy environment, that is, the way in which supporting state and local needs is talked about?
 - 2. Have there been changes in the policy environment during the last year?

II. CURRENT AND MOST RECENT INITIATIVES

- A. Describe your current initiatives aimed at supporting state and local efforts to respond to terrorist attacks:
 - 1. Factors that motivated the initiatives
 - 2. Alternatives considered (probe why not pursued)
 - 3. Goals of the initiative
 - 4. Anticipated outcomes of the initiative
 - 5. Measures of success
 - 6. Strategies for evaluating or monitoring the initiative
 - 7. Resources allocated
 - 8. How is function organized within agency?
 - 9. Support or interference during development of the initiative

- B. Sources of information motivating the initiative
 - 1. Mechanisms used to understand state and local needs (e.g., formal needs assessments) and sources of information relied on in deciding which initiatives to pursue
 - a. Names of groups or individuals consulted
 - b. General strategies recommended by these groups
 - 2. Sources of information used in constructing the initiative

- C. Strategies for implementing the initiatives
 - 1. Surveys of public attitudes
 - 2. Studies showing costs and benefits of selected and alternative strategies
 - 3. Changes in strategy or planned changes since inception
 - 4. Barriers to effective implementation
 - a. Vocal opposition from stakeholders
 - b. Other political barriers
 - c. Legal challenges to the initiative
 - d. Economic barriers
 - e. Social/cultural barriers
 - 5. Evaluation strategies
 - a. Evaluation requirements and approach--outcome measures
 - b. Identification of long-term and interim goals
 - c. Specified process for implementation
 - d. Analysis of strategies

- D. Stakeholder roles
 - 1. Role respondent played in developing and implementing the initiative
 - 2. Anticipated future role for respondent
 - 3. Previous respondent involvement
 - 4. Perception of roles played by other key participants in the development and implementation process
- E. Knowledge about other agencies' public health-oriented activities
 - 1. Alternative strategies being pursued by other agencies
 - 2. Intergovernmental cooperation at the state, local or regional level

III. RELATIONSHIP BETWEEN STATEWIDE AND LOCAL INITIATIVES

- A. Historical relationship
- B. Predicted response from the state and local governments to current initiatives
- C. Evidence on the relative effectiveness of state vs. local strategies

IV. SPECIFIC AREAS OF INTEREST

- A. FDA's role in state/local efforts (food supply safety)
- B. National Pharmaceutical Stockpile (state/local implications)
- C. Relationship to private-sector stakeholders
- D. Communications issues among federal, state, and local agencies
- E. Adequacy of resources to meet state/local needs
- F. Methods for improving federal/state/local partnerships

V. MISCELLANEOUS

- A. Available documentary material
- B. Other potential respondents to interview

TAB 2—REFERENCES

Allen, C. “HHS Efforts to Prepare Against Bioterrorism,” Testimony before the House Subcommittee on Labor-HHS-Education Appropriations, May 5, 2002.

Centers for Disease Control and Prevention, Guidance for Fiscal Year 2002 Supplemental Funds for Public Health Preparedness and Response for Bioterrorism, Atlanta, GA, Centers for Disease Control and Prevention, February 15, 2002.

Davis, LM and Blanchard, JC. “Are Local Health Responders Ready for Biological and Chemical Terrorism?” Issue Paper IP-221-OSD (2002), Santa Monica, CA, RAND, 2002.

Health Resources and Services Administration, Bioterrorism Hospital Preparedness Program, Cooperative Agreement Guidelines, Rockville, MD, Health Resources and Services Administration, February 15, 2002.

Inglesby, TV. “The State Public Health Preparedness of Terrorism Involving Weapons of Mass Destruction: A Six Month Report Card,” Testimony before the Senate Committee on Government Affairs, April 18, 2002.

Institute of Medicine, The Future of Public Health, Washington, DC, National Academy Press, 1988.

Khan, AS, Levitt, AM, and Sage, MJ. “Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response,” Morbidity and Mortality Weekly Report, 49(RR0):1-14, April 21, 2000.

National Institutes of Health, “Press Release for the FY 2002 President’s Budget,” Rockville, MD, National Institutes of Health, February 4, 2002.

O’Toole, T. “Department of Health and Human Services Budget Priorities for FY03,” Testimony before the U.S. House of Representatives Committee on the Budget, February 28, 2002.

Salinsky, E. “Public Health Emergency Preparedness: Fundamentals of the ‘System,’” National Health Policy Forum Background Paper, Washington, DC, National Health Policy Forum, April 3, 2002.

Thompson, TG. “HHS Efforts to Coordinate and Prepare for Bioterrorism,” Testimony before the Senate Committee on Governmental Affairs, April 18, 2002.

U.S. Department of Health and Human Services, “Bioterrorism Hospital Preparedness Program, Summary Guidance for Award and First Allocation,” DHHS/HRSA, 2002.

U.S. Department of Health and Human Services, Web site www.dhs.gov, 2002a.

U.S. General Accounting Office (GAO), “Bioterrorism: Federal Research and Preparedness Activities,” GAO Report (GAO-01-915), Washington, DC, September, 2001.

Wetter, DC, Daniell, WE, and Treser, CD. “Hospital Preparedness for Victims of Chemical or Biological Terrorism,” American Journal of Public Health, 91:710-716, 2001.

APPENDIX K- MEDICAL AND PUBLIC HEALTH WORKFORCE PREPAREDNESS

Overview

The events of Fall 2001 prompted much speculation regarding the U.S. healthcare and public health systems' capacity to respond to future terrorism and bioterrorism attacks, as well as a wide range of manmade and naturally occurring public health emergencies. As a result, a number of groups are examining the issue of healthcare and public health workforce (referred to as workforce throughout this paper) preparedness as it relates to their various constituencies and many are already implementing programs aimed at enhancing response capability. The Federal government, for example, has funded new academic centers for public health preparedness, provided over \$1 billion to the states to enhance bioterrorism preparedness, and is working with several national associations to build new medical volunteer efforts. Healthcare trade associations are developing recommendations and training activities for their respective members aimed at assessing and enhancing their preparedness. Many of these initiatives were developed in the immediate aftermath of the 2001 attacks.

Purpose

Little is known about the level of health workforce preparedness nationwide—or even how to define “preparedness”—and whether the range of important issues related to system preparedness, adequacy of the workforce's knowledge and skill sets, and overall availability of manpower are understood or are being examined in a comprehensive manner. We sought to better understand the workforce response to the Fall 2001 terror attacks and the activities underway to enhance preparedness for potential future public health emergencies—natural and manmade. Therefore, we undertook a preliminary study with the following objectives:

1. To summarize lessons learned to date from the Fall 2001 terrorism and bioterrorism attacks about the workforce's current response capacity;
2. To summarize selected pre- and post-9/11 Federal, state, local, and private-sector efforts aimed at enhancing workforce surge capacity³⁶⁰ and preparedness; and
3. To make proposals for facilitating workforce preparedness, including appropriate foci for future activities (including research) and steps that need to be taken to enhance the effectiveness of activities currently underway or under development.

Methods

Although conducting a systematic literature review with formal inclusion and exclusion criteria was beyond the scope of this project, we conducted a review of selected professional literature and publicly available documents and websites providing background information and describing relevant programs. We also interviewed 14 individuals involved in enhancing workforce preparedness at various levels (state health department, trade association, Federal government) to learn about their activities, concerns, and unmet needs around response to the potential threat of terrorism, bioterrorism, and other public health emergencies. We developed two formal interview scripts—one for state health officials and another association or academic institution representatives. Our interviews with Federal officials were organized around questions related to specific Federal initiatives. Each interview lasted approximately one hour; four were conducted in person and the rest via telephone. While our interviews were aimed at discussing workforce issues as interviewees saw them, few could speak only about workforce preparedness versus

³⁶⁰ The term “surge capacity” is sometimes used to address the ability of hospitals to meet the needs of incoming patients (bed capacity) and sometimes used to refer to the number of healthcare staff available at to meet patient needs in an emergency. The latter definition is the one that we use in this report.

preparedness in general. Additionally, most were able to address preparedness issues almost solely as they relate to bioterrorism preparedness.

Section II of this paper begins with an overview of the state of the healthcare and public health workforce, brief background information on what is known about workforce preparedness for terrorism and other public health emergencies, and a discussion of what can (and can not) be learned about medical and public health workforce preparedness from the events of Fall 2001. Section III summarizes the findings from the interviews that we conducted as well as our literature and document review, and provides proposals for facilitating workforce preparedness based upon these findings.

Although we sought to address workforce preparedness for a range of public health emergencies, examples in this paper are mostly from the realm of bioterrorism preparedness. This reflects the Department of Health and Human Services (HHS)—and our interviewees’—substantial focus on this aspect of preparedness during recent months. Indeed, the infusion of funds from HHS to the states during 2002 was specifically designated for bioterrorism preparedness activities. However, realizing that readiness to respond to a bioterrorism attack is just one component of workforce preparedness, throughout this paper we seek to highlight issues that are relevant to a range of public health threats—natural and manmade.

Key Themes

In the course of our work, four key themes arose. The suggestions and possible policy options listed Section IV are organized around these themes.

1. Federal, state, and local agencies, as well as many private sector entities, have not articulated, and therefore do not share, a common understanding of the meaning of a “prepared workforce.” HHS and other agencies should fund research and information sharing aimed at better understanding what a workforce “prepared” to address a range of health threats would look like in size, competencies, composition, and geographic distribution.
2. HHS needs to assess and respond to—or fund others to do so—state and other grantee needs around technical assistance, evaluation methodology, and other resources needed to enhance the efficiency and effectiveness of workforce development and preparedness activities nationwide. Additionally, HHS should articulate a plan to evaluate the range of preparedness activities that it is funding and/or implementing, including efforts around the development of volunteer response teams.
3. All of those involved in enhancing workforce preparedness should continue to emphasize the need to continue to build bridges between the public health and emergency management and response fields and upon building expertise to respond to public health emergencies within both of these fields.
4. HHS and other Federal agencies need to adequately fund the range of preparedness efforts being undertaken by state health departments and private organizations, where appropriate. Additionally, they should explore the potential advantages of expanding the role of existing programs to meet evolving public health threats as well as the day-to-day needs of the public health system.

Introduction to the Healthcare and Public Health Workforces and Their Level of “Preparedness”

In conducting this study, we sought to describe efforts underway to enhance preparedness for potential future public health emergencies—natural and manmade—and to make recommendations based upon what we learned. It became immediately clear in undertaking this project that there is no single definition of a “prepared workforce,” because, as noted above, there is no consensus on what being prepared is. The word “prepared” is used loosely in many documents and is not accompanied by a concise definition. Additionally, there are not yet widely-agreed upon metrics by which to assess levels of preparedness

among the workforce, although there are some aimed at particular sectors, discussed in more detail later in this paper, that are being developed or piloted. Just as we do not know what “preparedness” looks like, we also know little about the numbers of professionals needed to respond to different public health emergencies. Indeed, according to the United States General Accounting Office (GAO), as of 2002, “There is no consensus on the optimal number and ratio of health professionals needed to meet the population’s health care needs,”³⁶¹ even in the absence of the threat of bioterrorism and naturally occurring health catastrophes. Later in this section, we will review some data that we did find related to current levels of preparedness. However, it is instructive to begin with a brief overview of the general state of selected sectors of the healthcare workforce in the United States.

Brief Introduction to the Healthcare and Public Health Workforce (Selected Sectors)

For the purposes of this report, we focused on the following professions: physicians; nurses; emergency medical services; pharmacists; the public health workforce; laboratory workers; and veterinarians. None of the individuals that we interviewed—nor many of the documents that we reviewed—noted a strong link between overall health workforce shortages and emergency preparedness. Many are more concerned about the impact of any shortages upon other day-to-day functions of the healthcare and public health systems. Furthermore, we did not identify studies that had quantified the gaps between the current workforce and that needed to respond to a range of public health emergencies at the national level, so it is impossible to draw conclusions about the size and scope of the shortage as it relates to this topic. Empirical work to generate this type of data is critically needed.

In January 2002, the Center for Health Workforce Studies at the New York State University at Albany published an analysis of Bureau of Labor Statistics (BLS) Occupational Projections for the health care industry through 2010, centered on 68 health-related occupations. The report notes that over five million healthcare workers “will be needed to fill the job openings created by departures and increases in new positions in health occupations between 2000 and 2010.”³⁶² The need will be particularly intense for all categories of nurses (RN, LPN, and nurse aides), physician assistants, and several other categories of workers not directly relevant to this report. A 2001 American Hospital Association (AHA) survey of 715 U.S. hospitals reported growing workforce shortages in that setting, noting that in 2001, there were up to 168,000 unfilled positions in U.S. hospitals, approximately 75% of which were for registered nurses.³⁶³ Forty-one percent of surveyed hospitals reported that emergency department overcrowding occurred “as a result of workforce shortage impacts,” and 28 percent reported having reduced the number of staffed beds. The report noted that these problems have the greatest impact upon more urban, overcrowded hospitals; indeed, 57 percent of surveyed urban hospitals reported emergency department overcrowding, reportedly as a result of staffing shortages. It is also important to note, however, that overcrowding, increased wait times, and other problems tied to workforce shortages in the AHA survey also result from a number of other factors endemic to the U.S. healthcare system such as lack of coordination of care and a primary care system that is unable to meet the needs of all Americans.

A 2000 companion document to the *Healthy People 2010* report—published well before more substantial attention was being paid to many public health hazards—described the need to enhance the healthcare

³⁶¹ United States General Accounting Office. 2001. Health workforce: ensuring adequate supply and distribution remains challenging. Report No. GAO 01-1042T. Available online: <http://www.gao.gov/>. Accessed September 15, 2002.

³⁶² Center for Health Workforce Studies. 2002. Health care employment projections: an analysis of Bureau of Labor Statistics Occupational Projections, 2000-2020. Available online: <http://chws.albany.edu/reports/012002/blsproj2002.pdf>. Accessed August 7, 2002.

³⁶³ American Hospital Association. 2001. Workforce survey. Available online: http://www.hospitalconnect.com/aha/key_issues/workforce/resources/FactSheetB0605.html. Accessed October 1, 2002.

workforce while working toward the substantive goals set forth in *Healthy People 2010*.³⁶⁴ *Healthy People 2010*, an effort led by the Office of the United States Surgeon General is “a comprehensive set of health objectives for the nation to achieve over the first decade of the new century. Created by scientists both inside and outside of Government, it identifies a wide range of public health priorities and specific, measurable objectives.”³⁶⁵ The document included an entire section related to strengthening the nation’s public health infrastructure and three objectives directly addressing workforce issues:

- Increase the number of under-represented minorities entering health professions programs;
- Increase the number of public health agencies offering continuing education courses; and
- Increase the number of public health agencies building personnel and training systems around competencies in the essential public health services.

The companion report made recommendations and offered specific examples around what public health agencies could do to further progress toward reaching these goals, noting that, “A diverse and prepared workforce is the key to achieving the goals of Healthy People 2010 as well as many other health improvement initiatives.” The report makes a direct link between an adequate workforce and ability to address arrange of public health emergencies, further stating:

“There is an ongoing need to train and educate people who are currently employed in public health as new areas, problems, threats, and potential disasters emerge. For example, the threat of bioterrorism or the increased impact of any natural and technological disaster will require different training and areas of expertise so that public health workers can detect problems early, communicate rapidly, and respond effectively.”

In the following paragraphs, we provide brief data describing the current state of each of the sectors of the workforce included in our review. We provide the information for background purposes only. We do not make judgments about the implications for response to public health emergencies because we know of no estimates of the gap between the size of the current workforce and the size needed to respond to specific natural and manmade public health emergencies. Conducting analyses aimed at quantifying this gap—if it exists—was beyond the scope of this project but is a critical area for future research.

The Physician Workforce. According to the U.S. Department of Labor (DOL), in 2000, there were 598,000 jobs held by practicing physicians and surgeons in the U.S, with approximately 35 percent in primary care.³⁶⁶ According to DOL, despite an oversupply of physicians in recent years (which is being questioned as the U.S. population ages), “The number of physicians in training has leveled off and is likely to decrease over the next few years, alleviating the effects of any physician oversupply.” Key concerns about the physician workforce focus not on an overall shortage, but on the distribution of physicians across the U.S. and, specifically, the undersupply of physicians in rural and other underserved areas. Additionally, a trend toward fewer physicians choosing to enter primary care practice raises concerns about access to basic healthcare in certain parts of the U.S.

³⁶⁴ United States Department of Health and Human Services. Health Resources and Services Administration. 2000. The key ingredient of the national prevention agenda: workforce development. a companion document to Healthy People 2010. Available online: <http://bhpr.hrsa.gov/oldhealthworkforce/hp2010.htm>. Accessed September 15, 2002.

³⁶⁵ United States Department of Health and Human Services, Office of Disease Prevention and Health Promotion. 2001. What is Healthy People 2010? Available online: <http://www.health.gov/healthypeople/About/hpfact.htm>. Accessed October 16, 2002.

³⁶⁶ U.S Department of Labor, Bureau of Labor Statistics. 2001. Occupational outlook handbook: physicians and surgeons. Available online: <http://stats.bls.gov/oco/ocos074.htm>. Accessed October 11, 2002.

The Nursing Workforce. Few sectors of the healthcare workforce have received as much attention over the past several years as nursing. In a July 2002 report, the Health Resources and Services Administration's (HRSA) estimated that while the current nationwide demand for nurses outweighs the supply by just six percent today, this disparity is expected to increase to 12 percent and 20 percent by 2010 and 2015, respectively.³⁶⁷ Driving this shortage are inadequate pay and benefits, unpleasant and even hazardous working conditions, and a plethora of non-clinical employment opportunities for nurses. There is no reported significant geographic variation in the nursing shortage: in 2000, fully 30 states had nursing shortages, while this is projected to increase to 44 states and the District of Columbia by 2020.

The Pharmacist Workforce. A HRSA report summarizing the 2000 national Study of the Supply and Demand for Pharmacists³⁶⁸ noted that there is a current shortage of pharmacists, resulting not from a decrease in individuals entering the field, but from an "unprecedented demand" for these professionals. The report noted that approximately 60% of pharmacists are employed in retail or community settings, and 29% are in hospitals or other institutional settings. The 2001 AHA workforce survey reported a 21 percent vacancy rate for pharmacists in the hospital setting alone,³⁶⁹ with the shortage being most severe in rural areas.

The Laboratory Workforce. According to the BLS, laboratory technicians and technologists filled approximately 295,000 jobs in 2000.³⁷⁰ While approximately half were employed by hospitals, others were in medical offices, research laboratories, and public health settings. BLS expects about average growth in the demand for laboratory workers over the next decade, although this projection was made prior to the Fall 2001 attacks, when many laboratories were overwhelmed. A 2001 American Hospital Association workforce study reported a 10 percent vacancy rate among laboratory technologists in urban hospitals and 15 percent in rural hospitals. The GAO reports that although, "Higher vacancy rates and declining numbers of new workers to the laboratory profession...have been reported by provider and professional associations...employment and earnings data for laboratory technicians and technologists does not produce a clear picture of the balance of supply and demand for these workers."³⁷¹

The Public Health Workforce. The "current best estimate" of the size and composition of the public health workforce was presented in a December 2000 report by HRSA and the Columbia University School of Nursing. This report defined the public health workforce broadly to include paid and unpaid workers in both official agencies and voluntary organizations involved in the public health system—a "network linked by common interest and in some cases, by law, in pursuit of improved health for all."³⁷² It stated that there were 448,254 individuals in salaried public health positions in 2000, supplemented by over 2.8 million volunteers (this does not include fire or EMS workers or others who occasionally contribute to maintenance of public health). However, the report offered many caveats vis-à-vis its

³⁶⁷ U.S. Department of Health and Human Services. Health Resources and Services Administration. 2002. Projected supply, demand, and shortages of registered nurses: 2000-2020. Available online: <http://bhpr.hrsa.gov/oldhealthworkforce/rnproject/report.htm#chart1>. Accessed October 11, 2002.

³⁶⁸ Health Services and Resources Administration. 2000. Report to Congress. The pharmacist workforce: a study of the supply and demand for pharmacists. Available online: MORE

³⁶⁹ American Hospital Association. 2001. AHA poll finds workforce shortage hurts hospitals now and will get worse. June 2, 2001. Available online: http://www.hospitalconnect.com/aha/jsp/display.jsp?dcrpath=AHA/NewsStory_Article/data/aha_news_now/AHAN_EWSNOW1230&domain=AHANEWS. Accessed August 15, 2002.

³⁷⁰ U.S. Department of Labor, Bureau of Labor Statistics. 2001. Occupational outlook handbook: clinical laboratory technologists and technicians. Available online: <http://stats.bls.gov/oco/ocos096.htm>. Accessed October 9, 2002.

³⁷¹ U.S. General Accounting Office. 2001. Supply of selected health workers. Report No. GAO-02-137R. Available online: www.gao.gov. Accessed October 1, 2002.

³⁷² Center for Health Policy, Columbia University School of Nursing. 2000. The public health workforce: enumeration 2000. December 2002.

methodology and recommended that the actual “size and composition of this workforce should be identified, and should be tracked over time in order to develop appropriate plans for workforce development, recruitment, and retention.” Despite the limitations, several findings are relevant to this report. First, the researchers found that epidemiologists—“those working specifically in what is described as the core science of public health”—account for “far less” than one percent of the total public health workforce. Indeed, “epidemiologists, biostatisticians, and infection control/disease investigators are just over one-half of one percent of the workforce. Given the centrality of the activities encompassed by these occupations, this finding supports the common observation that at the local level, much of public health work is performed by generalists rather than specialists.”

The Emergency Medical Services (EMS) Workforce. According to the Bureau of Labor Statistics (BLS), EMS workers filled approximately 172,000 jobs in 2000. This includes both emergency medical technicians and paramedics. EMS workers are vital first responders in the event of public health emergencies. BLS projects that over the next few decades, “Population growth and urbanization will increase the demand for full-time paid EMTs and paramedics rather than for volunteers. In addition, a large segment of the population—the aging baby boomers—will further spur demand for EMT services, as they become more likely to have medical emergencies.”³⁷³

The Veterinary Workforce. According to the BLS, there were approximately 59,000 filled veterinarian jobs, with 800 in Federal government roles, in 2000.³⁷⁴ Employment of veterinarians “is expected to grow faster than the average for all occupations through the year 2010. Job openings stemming from the need to replace veterinarians who retire or otherwise leave the labor force will be almost as numerous as new jobs resulting from employment growth over the 2000-2010 period.”

What is a “Prepared Workforce?”

Just as we found no studies estimating the size of the healthcare workforce needed nationally to be ready to respond to natural and manmade public health emergencies, we found no single, agreed upon definition of the characteristics of a healthcare workforce adequately “prepared” to respond. Additionally, there are no standardized and widely used credentialing standards for medical and public health workers to meet in this area though efforts to develop them are underway. However, those that we interviewed for this study seemed inclined for now to use the “critical capacities” outlined in CDC’s bioterrorism funding guidance to states as benchmarks for their success in preparing the workforce for bioterrorism specifically following receipt of funding. We therefore briefly summarize below a sample of the relevant bioterrorism funding focus areas paying particular attention to those critical capacities and critical benchmarks that directly address workforce development and preparedness. Critical benchmarks are those items that CDC required states to complete *prior to* submission of their requests for funding; these items are in bold type below. The table is organized by the focus areas contained within the guidance to states and lists the contained critical capacities and benchmarks relating to workforce preparedness contained within the respective focus area. Focus Areas C, D, E, and F did not contain critical capacities and benchmarks directly related to this report so they are not included in the table.

³⁷³ U.S. Department of Labor, Bureau of Labor Statistics. 2002. Occupational outlook handbook: emergency medical technicians and paramedics. Available online: <http://stats.bls.gov/oco/ocos101.htm>. Accessed October 11, 2002.

³⁷⁴ U.S. Department of Labor, Bureau of Labor Statistics. 2002. Occupational outlook handbook: veterinarians. Available online: <http://stats.bls.gov/oco/ocos076.htm>. Accessed October 11, 2002.

Table A. CDC Bioterrorism Funding Guidance: Selected Critical Capacities Related to Workforce Development/Preparedness

<p>Focus Area A: Preparedness Planning and Readiness Assessment</p>	<p>Designate a senior public health officials to serve as executive director of the bioterrorism preparedness and response program</p> <p>Establish an advisory committee made up of a variety of stakeholders in each state</p> <p>Assess existing state and local public health leadership and management capacity; develop specialized state and local public health leadership and management training in advanced concepts of incident command and bioterrorism communication</p> <p>Identify a dedicated preparedness and response staff to oversee preparedness planning/workforce readiness</p> <p>Identify an emergency response coordinator in each local public health agency</p> <p>Develop and expand the capacity to address worker health and safety issues related to bioterrorism</p>
<p>Focus Area B: Surveillance and Epidemiology Capacity</p>	<p>Ensure the existence of systems to provide disease surveillance and epidemiology training for public health, clinical, and other professionals and to develop subject matter expertise within the public health system</p> <p>Assist in the provision of sufficient, competent, trained staff to managed the National Electronic Disease Surveillance System (NEDSS)</p> <p>Assess current epidemiologic capacity and prepare a timeline for achieving the goal of providing at least one epidemiologist for each Metropolitan Statistical Area with a population > 500,000</p> <p>Ensure that a full-time response coordinator for bioterrorism and other infectious disease outbreaks, and other public health threats and emergencies has been designated at the appropriate state and/or local levels</p> <p>Train state and local public health staff who would respond to a bioterrorism event in their roles and in the specifics of your jurisdiction's plan</p>
<p>Focus Area G: Education and Training</p> <p>Focus Area G: Education and</p>	<p>Prepare a timeline to assess training needs—with special emphasis on emergency department personnel, infectious disease specialists, public health staff, and other healthcare providers</p> <p>Develop an ongoing plan for meeting training needs through multiple sources</p> <p>Develop the capacity to facilitate or provide education and training sessions and services on bioterrorism, other infectious disease outbreaks, and other public health threats and emergencies; this should include a trained distance learning coordinator and access to distance learning capabilities</p> <p><i>(The following items are designated “enhanced activities”)³⁷⁵</i></p>

<p>Training (Cont'd)</p>	<p>For the purpose of targeting education and training activities, develop and regularly update an online public health workforce profile that lists all available manpower, including staff, contractors, community partners, private practitioners, academic partners, and others</p> <p>For the purpose of identifying and addressing critical personnel shortages, with local health agencies, conduct a staffing needs assessment which identifies the number, qualifications, and geographic distribution of public health personnel required to meet state and local public health service needs.</p> <p>Based on the findings of the staffing and training needs assessments, and with local public health agencies, develop and annually update a workforce preparedness plan; components of this plan should include strategies to address shortage areas, recruitment and retention, and surge capacity. Implement strategies to ensure workforce competency</p> <p>Evaluate the effectiveness of training and education programs on individual staff using formal pre- and post-test instruments, practice-based skill reviews, peer observations, and other scientifically validated and relevant health education tools</p> <p>Conduct an annual evaluation of all activities undertaken in support of the workforce preparedness plan using formal measures and indicators identified in the National Performance Standards Program</p> <p>Collect data to develop and strengthen the relationship of workforce performance, organizational effectiveness, and health outcomes</p>
---------------------------------	---

³⁷⁵ “Enhanced activities are those that are over and above critical capacities and are to be addressed only after critical capacities are achieved. We list them because of their direct relevance to this report. We believe that these items should be implemented earlier in the process to ensure that workforce development and education efforts are designed around actual identified needs.

The capacities and benchmarks are heavily process-oriented, rather than outcome-oriented. That is, they set a requirement for a number of activities and plans to be completed by the states, but say little about the end results in terms of enhanced competencies among a state’s healthcare workforce, for example.

What Do We Know About Current Levels of “Preparedness?”

Although, as noted above, there is no agreed-upon definition for a “prepared” workforce, several recent reports suggest that current members of the workforce are not adequately prepared to respond to a public health emergency, including a terrorism or bioterrorism attack. Even several years ago, authors concluded that there was much work to be done to enhance preparedness. Indeed, McDade (1999) noted that “Preliminary assessments of our nation’s capabilities for responding to possible bioterrorist attacks have identified many deficiencies, including inadequate surveillance systems; lack of rapid diagnostic techniques...and insufficient training of physicians, epidemiologists, and laboratorians.”³⁷⁶ Furthermore, he pointed out the necessity of incorporating dual use strategies into bioterrorism preparedness activities and noted the similarities to the activities needed to enhance general infectious disease surveillance: “Improving capabilities and capacities for responding to one issue will almost certainly benefit the other. For example, developing rapid diagnostic techniques that would make it possible to quickly detect bioterrorist attacks involving anthrax, plague, or Q fever would have considerable usefulness in the routine clinical diagnosis of pneumonia. Distribution systems set up to deliver antimicrobial agents and vaccines after bioterrorist attacks would be indispensable in delivering antiviral compounds and influenza vaccine during a large pandemic.” Clearly, without a stronger public health infrastructure, carrying out and maintaining the steps needed to enhance bioterrorism and other public health emergency preparedness will do little good.

The recent investment of HHS funds makes clear that the Federal Government believes that the workforce and the public health system are not currently prepared for a bioterrorism attack, specifically. However, it is important to note that this investment is aimed at enhancing preparedness at the state level and will not necessarily directly address the communication and line of authority issues that hindered response efforts during the Fall 2001 attacks—especially those taking place with Washington, DC postal workers (issues that are beyond the scope of this report). Further, there are many pressing questions about whether the enormous infusion of funds will lead to the intended results. Salinsky (2002) voices three key concerns that we would echo: “Will the funding go where it is most urgently needed, or will politics and existing power structures prevail and distribute resources regardless of real need and assessed risk? Can organizations break out of their traditional silos, overcome turf battles, and resist ‘business as usual’ to develop new relationships, or will insularity prevent the true transformation of working relationship? Can an appropriate balance be struck between responding to the threat of bioterrorism and ensuring an effective public health response to the health problems facing the nation on a daily basis, such as HIV/AIDS and heart disease?”³⁷⁷ This raises several additional questions that must be addressed at the national level: Who will decide what the “real” needs and “real” risks are? Can Federal funding “force” states and organizations to “break out of their traditional silos, overcome turf battles, and resist ‘business as usual’?”

³⁷⁶ McDade JE. 1999. Addressing the potential threat of bioterrorism—value added to an improved public health infrastructure. *Emerging infectious Diseases*. 5:591-2.

³⁷⁷ Salinsky E. 2002. Will the nation be ready for the next bioterrorism attack? Mending gaps in the public health infrastructure. *National Health Policy Forum Issue Brief*. No. 776, June 12, 2002.

What Can We Learn about Workforce Preparedness from the Events of Fall 2001?

The healthcare and public health response systems were not fully tested on September 11 nor during the subsequent anthrax attacks. In the case of the attacks at the World Trade Center and the Pentagon, there were many deaths, but relatively few individuals with serious injuries or illness requiring emergency or long-term medical care. According to the New York City Department of Health (NYCDOH), just 1,103 injured survivors were treated in the emergency departments or burn centers closest to the World Trade Center within 48 hours of the attack, although these and other facilities had mobilized to receive many more casualties.³⁷⁸ NYCDOH staff collected detailed data on all survivors receiving treatment at five Manhattan hospitals and found that of 1,103 survivors, 810 were treated and released, 181 were hospitalized, and four died. Survivors seeking care peaked within two-to-three hours after the attacks and then slowly tapered off over the next two days. Whereas past multicasualty disaster reports, “commonly describe a first wave of survivors with minor injuries, a second wave of more severely injured survivors, and subsequent waves of survivors rescued during extraction from the disaster site,” this one “describes one large wave of survivors and a second wave the next day comprised largely of rescue workers.”

Therefore, the September 11 experience is perhaps most instructive in terms of a typical health workforce response to terrorism if this is indeed the type of attack to expect in the future, but less so for dealing with very different scenarios.³⁷⁹ Indeed, CDC summarizes its report noting that “admission rates associated with terrorist bombings should be compared with caution because the number at risk, the location of survivors at the time of the attack, and building and blast effects vary with each event.” Additionally, although many emergency rooms were overwhelmed in response to the anthrax attacks, most of this activity was due to false alarms sounded by the “worried well” that resulted in part from the lack of a cohesive, timely public communication strategy. The “worried well” are the responsibility of the health care system and their needs must be met, but they exert very different demands upon the system than those exerted by individuals who require actual therapeutic intervention in addition to diagnostic testing and reassurance. The Fall 2001 attacks tell us less about the workforce response needed in the case of other types of attacks or large-scale naturally occurring emergencies, when acute and long-term care settings would be overwhelmed along with emergency departments. So although the events certainly did tax components of the involved systems, future attacks with many additional casualties are likely to tax entire systems and continua of care in ways that have not previously been experienced, including within the public health system—which was not widely tested following the Fall 2001 attacks. Additional study is needed to develop plans around different potential scenarios, especially efforts to model the potential healthcare and public health workforce response levels needed.

Detailed Study Findings and Proposals for Facilitating Workforce Preparedness

In this section, we present our key findings from the interviews that we conducted as well as our literature/document review. These are organized under the four key themes that we identified and are followed by relevant bulleted proposals for facilitating workforce preparedness.

Key Theme 1: Federal, state, and local agencies, as well as private sector entities, have not articulated a common understanding of the meaning of a “prepared workforce.” HHS and other agencies need to fund research and information sharing aimed at better understanding what a workforce “prepared” to address a range of health threats would look like in size, competencies, composition, and geographic distribution.

³⁷⁸ Centers for Disease Control and Prevention. 2002. Rapid assessment of injuries among survivors of the terrorist attack on the World Trade Center—New York City, September 2001. MMWR. 51:1-5.

³⁷⁹ Centers for Disease Control and Prevention. 2002. Rapid assessment of injuries among survivors of the terrorist attack on the World Trade Center—New York City, September 2001. MMWR. 51:1-5.

Finding: There is no current, comprehensive, national enumeration of the public health workforce (including the public health laboratory workforce). Similarly, there is no detailed enumeration of the range of public health infrastructure issues, including funding for public health generally.

As described in Section II, the “current best estimate” of the size and composition of the public health workforce is found in a December 2000 report by HRSA and the Columbia University School of Nursing. Given the methodological and definitional issues inherent in trying to assess the size and scope of the public health workforce, the report offered many caveats vis-à-vis its methodology and findings and summarized that the actual “size and composition of this workforce should be identified, and should be tracked over time in order to develop appropriate plans for workforce development, recruitment, and retention.” Clearly, without a current, comprehensive, and methodologically rigorous study of today’s public health workforce and public health departments in general, the impact of the new bioterrorism funds on the development of this workforce—and the public health infrastructure in general—will be impossible to quantify. It will also be impossible to compare the relative size of public health departments across states and to make recommendations about what works well given the size and needs of communities. With respect to laboratories, according to APHL, CDC and the Association of Public Health Laboratories are still working on a definition for “public health laboratory”; therefore, there is currently there is no definitive figure for the number of public health labs in the US.

Finding: There is no credentialing body for public health, per se, although core competencies for public health workers are being piloted. Additionally, the current lack of core competencies for public health departments in the area of bioterrorism preparedness makes evaluation of their preparedness efforts—and benchmarking against other departments—particularly challenging.

Over the past several years—and especially since Fall 2001—organizations involved in advancing the field of public health have paid increased attention to issues around credentialing this workforce. The Columbia Center for Workforce Preparedness has developed and piloted core competencies for public health workers around emergency preparedness, as well as specific bioterrorism preparedness competencies. The competencies include those that are: generic to all public health workers; specific to public health administrators; specific to public health professionals; and specific to public health technical and support staff. They include such items as: “All public health workers must be competent to describe the agency chain of command in emergency response;” and “All public health leaders/administrators must be competent to assure that the agency regularly practices all parts of emergency response.”³⁸⁰ The Center expects to make specific bioterrorism competencies available to the field. Other organizations are working on developing various competencies for public health professionals (a detailed list of such competencies can be seen in the recent Institute of Medicine report “The Future of the Public’s Health in the 21st Century”³⁸¹). We also learned that some states are pursuing their own public health credentialing activities. For example, Illinois and Missouri are developing credentialing boards for public health administrators, New Jersey is developing standards and qualification criteria for public health workers, and Michigan’s Public Health Institute is working on a local public health worker accreditation program.

Others are developing competencies by which health departments can gauge their level of preparedness, beyond workforce preparedness. For example, the National Association of City and County Health

³⁸⁰ Columbia University Center for Health Policy. 2001. Emergency preparedness: core competencies for all public health workers. Available online: <http://cpmcnet.columbia.edu/dept/nursing/institute-centers/chphsr/compbroch.pdf>. Accessed July 15, 2002.

³⁸¹ Institute of Medicine, Committee on Assuring the Health of the Public in the 21st Century, Board on Health Promotion and Disease Prevention. 2002. The Future of the public’s health in the 21st century. Available online: <http://books.nap.edu/books/0309086221/html/index.html>. Accessed November 25, 2002.

Officials (NACCHO) is working with public health partners “to develop a module of performance measures, as part of the National Public Health Performance Standards Program, that will assist communities in assessing their capacity to respond to bioterrorist disease threats.”³⁸² The goals of this project are to identify possible capacities, prioritize these capacities, and gather the input of stakeholders with the aim of reaching consensus. This is the first attempt at developing a potential credentialing process for public health departments, and the group hoped to implement field tests in late fall or early winter of 2002.

Finding: Vaccines, protective equipment, childcare, and other mechanisms aimed at protecting and incentivizing healthcare workers are the subjects of much debate. Although we could not find studies that had examined this issue, we heard from some that providing these types of supports might indeed aid mobilization and retention of healthcare workers during a public health emergency and, in turn, enhance preparedness. However, these strategies are likely to be daunting and expensive prospects and are unnecessary if one believes that responding to events is part of the responsibility of any healthcare provider.

We learned that American Nurses Association (ANA) members have mentioned personal protective issues as important considerations in their ability to respond to bioterrorism attacks, and are potentially important to other health care professionals as well. Nurses have voiced concerns about not being able to reach their children in the event of a hospital lock-down. We also learned that the American Hospital Association has been involved in leading joint role-playing activities and developing guidelines around the workforce issues that need to be addressed in order to enhance the ability to respond to events. For example, they have recommended getting various community organizations involved in planning and thinking about who could check on healthcare providers’ children in the event of an attack.

Finding: Interviewees reported a substantial shortage of individuals qualified to fill new epidemiologist positions within state and local health departments. Departments report a lack of applications for these positions and they need to hire individuals that do not necessarily meet the qualifications, thus creating an additional training burden. Further, we found no studies aimed at quantifying the gap between supply and demand of epidemiologists nationwide. Empirical research aimed at quantifying the actual number of epidemiologists needed has not been carried out.

Little is known about the actual number of epidemiologists needed within the public health system, because no empirical studies have explored this to date. Most of the state health department representatives with whom we spoke reported major difficulties finding and hiring qualified epidemiologists. In one state, recruitment for epidemiologist positions has been “spotty”; the department often does not draw any “stellar” applicants. Individuals who apply for the positions are generally not trained epidemiologist, but have instead been veterinarians, statisticians, and individuals with PhDs in related areas. However, that state’s interviewee noted that this has always been the case and that they “rarely find a trained epidemiologist.” Additionally, the 2000 report aimed at enumerating the public health workforce referenced in Section II of this report noted that less than one-half of one percent of public health workers were trained epidemiologists that year.

During a discussion of bioterrorism and public health at the American College of Epidemiology meeting in September 2002, panelists and other meeting participants discussed the implications of these developments for epidemiology, and the implications of these issues for doctoral level training in epidemiology was a focus of the working group discussions. In addition to using the Fall 2001 experience to illustrate the interface between epidemiology and bioterrorism, participants reiterated the

³⁸² National Association of City and County Health Officials. 2002. National Public Health Performance Standards Program. Available online: <http://www.naccho.org/project48.cfm>. Accessed November 14, 2002.

great need for epidemiologists to fill positions in state and local health departments created by recent federal funding programs. The American College of Epidemiology and the Association of Schools of Public Health, are organizing a follow-up workshop in December to discuss doctoral education in epidemiology, with part of the meeting focusing on bioterrorism.

Finding: There are a number of efforts under development aimed at organizing and being able to mobilize volunteer healthcare providers to respond to public health emergencies when they arise, including those that occur outside the geographic area in which they generally practice. However, it is unclear how these efforts will be evaluated or what metrics might be used in such an evaluation. There are many unanswered questions around the legal, credentialing, and liability issues related to using non-local healthcare workers during health emergencies, although some efforts are underway to address them.

Through our interviews, we learned about three key efforts underway to organize and be able to mobilize groups of volunteer healthcare providers to response to public health emergencies. The Medical Reserve Corps (MRC) program was announced by HHS in Summer 2002 as “units composed of community-led, community-based volunteers who may assist medical response professionals and facilities during large-scale local emergencies, such as naturally occurring influenza epidemics, hazardous materials spills or acts of terrorism.”³⁸³ HHS announced awards totaling \$2 million to 42 community organizations on November 1, 2002. The size of the grants ranged from \$36,900 to \$50,000 and awardees included health departments, emergency management agencies, police departments, hospital districts and others. The MRC effort will be developed locally, make use of local resources, and serve as a citizen/civilian groups of volunteers who would assist in public health-related issues. The MRC’s focus will not be limited to bioterrorism, but rather will encompass a range of potential public health activities. Therefore, the MRCs will provide an opportunity to examine and strengthen the public health infrastructure in local communities. It remains unclear whether, and the extent to which, MRCs may be deployed outside their local areas if needed, which raises important concerns about credentialing issues.

Additionally, the American Nurses Association is working with HHS to develop National Nurses Response Teams, which will be comprised of 200 nurses per region (2,000 nurses in total) who will receive standardized education aimed at preparing them to assist with mass vaccination and chemoprophylaxis efforts. As of July 2002, 840 nurses had applied to participate. Finally, the American Pharmaceutical Association is working with HHS’s Office of Emergency Preparedness and several colleges of pharmacy to develop National Pharmacy Emergency Response Teams (NPRT). The goal of the program is to sign up and credential 2,000 pharmacists who can be mobilized to help respond to public health emergencies. Currently, pharmacists that wish to contribute to emergency response efforts in other states must request emergency clearance from that state’s pharmacy board, which can be a slow process. However, we were told that the NPRTs will be federalized to deal with emergency issues, with emergencies suspending licensure problems.

Finding: Some state health department representatives note confusion around their departments’ role in helping hospitals within their state prepare their workforces to respond to bioterrorism. Additionally, some states express concern about not receiving detailed information regarding the staffing needs associated with HHS’s hospital bed capacity requirements.

Some state public health officials are unclear about their role in assisting with planning for the staffing of hospital beds in the state and otherwise becoming involved in surge capacity issues, although they do

³⁸³ Department of Health and Human Services. 2002. HHS to offer grants to assist local communities in developing volunteer medical reserve corps. Available online: <http://www.hhs.gov/news/press/2002pres/20020719.html>. Accessed July 19, 2002.

work closely with some hospitals. One stressed that assessing and staffing needs, gaps, and issues in a large state is overwhelming at the state level, and really needs to be addressed at the local/regional level. However, one state health department is playing a role by hiring an emergency room planner and pharmacist who will have primary responsibility for planning with hospitals around potential use of the National Pharmaceutical Stockpile.

HHS did not ask states to develop workforce surge capacity, *per se*, but is requiring them able to staff 500 critical beds in 2002 and 1,500 by 2003. HHS is not providing models, algorithms, or other guidance as to how where to locate the beds and how to staff them; state and local governments need to figure out how best to achieve this. The exception is the guidance that HHS provided to states regarding setting up and staffing smallpox mass vaccination clinics. The Smallpox Vaccination Clinic Guide, released in September 2002, provides specific guidance regarding the number and type of clinical staff needed given specific assumptions about the number of individuals that would seek vaccination following a known smallpox attack. The model that HHS provides would lead to an output of vaccination of one million persons over 10 days per clinic. The methodology used to generate these estimates included a review of previous clinic models and publications, considerations of the technical issues associated with administering the vaccine, and “computer modeling for clinic flow and output estimates with different example staff numbers.”³⁸⁴

Proposed Solutions

- HHS should fund studies aimed at modeling the size and scope of the healthcare and public health workforce response needed to respond to a range of public health emergencies and day-to-day public health issues. Without the kind of data that will result from such studies, it is impossible to quantify the gap between the current workforce and a workforce “prepared” to address these issues. HHS’s Smallpox Vaccination Clinic Guide is an example of practical guidelines around workforce preparedness based upon modeling the needed workforce response to one such threat.
- HHS should fund research aimed at understanding the psychological, emotional, and practical benefits and costs around providing incentives to healthcare and public health workers to enhance their willingness to prepare for and respond to public health emergencies.
- CDC and HRSA should fund research aimed at enumerating the public health and public health laboratory workforce as well as enumerating the range of public health infrastructure issues, including funding for public health generally. This will enhance the ability to evaluate current preparedness efforts and serve as a benchmark for those seeking to enhance their preparedness. A nationally representative workgroup should be convened prior to the implementation of the study to resolve the key definitional and methodological issues.
- CDC and HRSA should convene a panel of public health experts to debate the pros and cons of credentialing public health workers and widely adopting competencies under development for public health workers and health departments. This should include a consideration of the appropriate credentialing body. Their discussions should be guided by preliminary, collaborative work already undertaken in this area.
- Associations and organizations with a responsibility for furthering public health practice (such as the American Public Health Association, the Council of State and Territorial Epidemiologists, the American College of Epidemiology, and the Association of Schools of Public Health) should convene a taskforce aimed at addressing the steps needed to recruit and train additional epidemiologists and determining the number of epidemiologist needed to fill positions currently and at ten and twenty years into the future. They should also consider the role of masters,

³⁸⁴ United States Department of Health and Human Services. 2002. Smallpox vaccination clinic guide: logistical considerations and guidance for State and local planning for emergency, large-scale, voluntary administration of smallpox vaccine in response to a smallpox outbreak. September 16, 2002.

doctoral, and continuing education in the preparation of professional epidemiologists. Federal funding will likely be needed to support these efforts.

Key Theme 2: HHS needs to assess and respond to—or fund others to do so—state and other grantee needs around technical assistance, evaluation methodology, and other resources needed to enhance the efficiency and effectiveness of workforce development and preparedness activities. Additionally, HHS should articulate a plan to evaluate the range of preparedness activities that it is funding and/or implementing, including efforts around the development of volunteer response teams.

Finding: With the influx of CDC and HRSA bioterrorism preparedness grant funds, state and local health departments are implementing a wide range of activities around workforce development and preparedness. Although many of these are much-needed programs, several state health officials are concerned about their ability to recruit the needed staff, as well as the extent to which they are creating redundancy given a lack of information about what other states are doing. Additionally, they believe that they need additional technical assistance in many areas, especially around evaluation of these new activities.

We interviewed public health officials from several states to learn about workforce development and preparedness activities at the state and local level. Most striking was their focus on hiring and training staff, although in some cases their approaches differ substantially. Each state has been able to advertise for and/or hire additional staff to support bioterrorism preparedness efforts, although they have taken different approaches and have had varying levels of success. One interviewee reported some difficulty locating potential applicants for any of the new positions because they are “just not out there.” Another state’s bioterrorism division, which had five staffers prior to receipt of the CDC funds, will have 28 employees when fully staffed. The focus since receipt of the CDC funds has been to support local workforce development and preparedness, so the department is adding an additional 60 individuals to its staff and is developing “regional response teams” to improve surveillance for areas that do not have local health departments. Each team will include an epidemiologist, public health nurse, and public health technician. Another interviewee noted that their department is caught “between a rock and a hard place” because they are not able to hire for bioterrorism positions until they have completed an assessment of their needs in this area. They have permission from the Governor to “fully staff the bioterrorism effort” but at the same time are being told that department positions are being reduced overall. Therefore, they also have had to accomplish most hiring at the local level.

In addition to hiring new staff, states are implementing a wide range of preparedness activities but have had little opportunity to share this information with colleagues in other states. Most involve training activities to enhance health department employees’ basic public health and emergency preparedness skills. One department is providing training to epidemiology staff at the local level and is placing a strong emphasis upon infrastructure development. For example, state lab capacity is being fostered through funding of laboratory enhancement activities at the regional level. Another state started an intensive, five-day field epidemiology course, to which members of their new regional response teams were invited. The course covered surveillance, statistics, infectious disease, and enhancing communication skills and had a key goal of getting the new hires to “think the same way.”

Several interviewees noted unique aspects of their states’ plans from which other states might draw ideas if they were aware of them. One state, home to a very large metropolitan area and well as very impoverished areas, is acutely aware of the need to develop preparedness capacities across the entire state, which is a major challenge. There is a lot of pressure from large communities to make preparedness efforts population-based, but the interviewee noted that attention must also be paid to the rural areas of

the state—which are also potential sites of manmade and natural public health emergencies. Another noted that the level of collaboration with the veterinary community in their state is fairly unique. While each county has had a medical officer for several years—with varying degrees of success—the interviewee noted that new veterinary officers selected in each region may be able to help with a variety of public health activities and provide back-up to medical officers.

Interviewees generally commented that they had not yet had asked for much technical assistance from CDC nor had much interaction with other state health departments, but would find such networking useful. One explained that they have good connections, but have not yet asked for support as they are “marching ahead with their own plans.” They noted that they do not have a good sense for the kind of support they would need, although they are not currently good at demonstrating links between training and performance. They are also interested in evaluation strategies and benchmarks for workforce development success and need guidance on how to measure performance issues.

Finding: Many agencies and organizations are implementing workforce preparedness activities without first conducting needs assessments to understand the baseline knowledge levels and learning styles of their audiences and without regard to the teaching methods that are most effective for these audiences. In addition, many are implementing the programs with little attention to evaluation other than measuring changes in knowledge. They are struggling with how to assess actual outcomes of these programs, especially in the absence of a bioterrorism or other event for which the audience is being prepared.

Many of the individuals that we interviewed expressed their belief in the importance of evaluating programs, but most agreed that doing so is particularly challenging given the low likelihood of a bioterrorism event. A belief among the workforce that an event may not ever happen can lead to complacency in terms of maintaining adequate levels of skills and knowledge and an understandable desire to focus instead on being prepared for the day-to-day realities of one’s job. However, some interviewees described evaluation plans that are in the early stages of development. One department is working with a local school of public health to look at previous evaluation efforts and determine what they can teach them about preparedness prior to Fall 2001. They believe that this will allow for a more meaningful evaluation of their new activities, as they hope to be able to establish some baseline levels of preparedness. They would like additional assistance with evaluation in two distinct areas, including the core capacities by which individuals should be evaluated and an evaluation framework for how well they are doing more globally in carrying out the “business of public health.” Another department does not have a formalized evaluation plan in place to specifically assess its bioterrorism preparedness efforts, but they are developing a list of target capacities around bioterrorism and general public health response and plans to evaluate the public health workforce using testing around these capacities.

At the Federal level, HHS plans to adopt a four-tiered approach in evaluating states’ efforts. The CDC bioterrorism grants set forth 17 preparedness benchmarks that were to be accomplished even before funding was received, (several of which are noted in Table 1 of this report) and is also requiring additional specific deliverables post-funding, with specific timelines for achieving them. We were told that the department will ask for its money back if states fall short although it is unclear how and when this would occur. As guidance to states, CDC had previously developed Public Health Response and Capacity Inventories, a resource “to help state and local public health agencies assess their preparedness to respond to a public health emergency.” CDC notes that “the emphasis of the inventories are on those priority agency capacities which ensure rapid response capability including detection of biologic threats,

communication of information regarding threats, and control of human consequences arising from threats.”³⁸⁵

Proposed Solutions

- CDC and its partner agencies within HHS should continually assess and determine ways to respond to states’ needs for technical assistance, including assistance with issues related to recruiting qualified public health staff.
- HHS should designate and adequately fund either an internal or external organization to function in a clearinghouse capacity for information about state and local health workforce development and preparedness activities. This could be an appropriate locus for information sharing about evaluation and metrics.
- HHS should fund studies to develop and test appropriate metrics by which to assess the range of professional and volunteer healthcare provider efforts under development to enhance bioterrorism and other emergency preparedness.
- The Federal government and state/local governments should continue to give issues around credentialing, licensure, and legal issues related to medical volunteers high priority, with input from the appropriate professional groups.
- CDC and its partner agencies should continue to offer technical assistance around workforce surge capacity and encourage dialogue among states and communities around the best way to achieve it. The Smallpox Vaccination Clinic Guide demonstrates the ability to model staffing needs around particular assumptions about an event. Therefore, these agencies should encourage further study into the appropriate levels and mix of staff needed to respond to different public health threats so that they can provide additional guidance to states.
- Although HHS has set forth critical capacities and benchmarks for states receiving bioterrorism funding from CDC, we are not aware that a specific long-term evaluation strategy—or methods by which to enforce compliance with the guidelines set forth in the grants—has been developed or articulated. HHS should engage its public health partners in convening an evaluation advisory body to ensure meaningful evaluation of the use of this unprecedented influx of funding. This body should include individuals with evaluation and training expertise to ensure that it is able to adequately advise HHS.
- On the whole, the critical capacities and benchmarks set forth with the CDC guidance to states seem to appropriate and comprehensive process-oriented tasks that cover a wide range of public health functions from management capacity to information technology to disease surveillance. However it is vital that HHS reevaluates and supplements these capacities and benchmarks in subsequent years of funding, particularly by adding a focus on outcome-oriented deliverables.

³⁸⁵ Centers for Disease Control and Prevention, Public Health Practice Program Office. 2002. Public health preparedness and response capacity inventory. Available online: <http://www.phppo.cdc.gov/od/inventory/relationto.asp>. Accessed November 25, 2002.

Key Theme 3: All of those involved in enhancing workforce preparedness should continue to emphasize the need to build bridges between the public health and emergency management and response fields and upon building expertise to respond to public health emergencies within these fields.

Finding: The respective “languages” and command structures used in public health and emergency management are different and can present substantial challenges in the course of training and collaborative emergency response. Several initiatives are underway to address this challenge.

Infusion of emergency management principles and practices into all levels of public health training and education is more common since the Fall 2001 attacks. One program doing work in this area is the CDC-funded Center for Public Health Preparedness at Columbia University’s Mailman School of Public Health. Their key activity to date has been the development of a basic training program for emergency preparedness in the public health realm. This program was first piloted in June 2001, when it was administered to school health nurses employed by the New York City Department of Health. It focused on basic emergency preparedness principles, specific key competencies, recognition of deviations from normal circumstances, and communication techniques. The Center is now working with the New York State Department of Health to develop versions of the curriculum that can be customized by other agencies and eventually to make it available nationwide.

The most recently funded Center for Public Health Preparedness—at the University of Pittsburgh Graduate School of Public Health—also plans activities aimed at bridging the gaps between theory and practice and between the fields of emergency management and public health. Among other activities, the Center will “provide ongoing crisis leadership training for senior officials in the fields of public health, emergency management, emergency medical systems and hospital emergency departments; and direct a surge-capacity training program for medical professionals such as physicians and nurses, who would assist public health officials during a bioterrorism emergency.”³⁸⁶

Finally, the Public Health Foundation’s Training Resources Center is marketing a CDC and Association of Schools of Public Health-funded model curriculum for schools of public health that includes modules on types of hazards and disasters, the role of public health in disasters, and evaluation methods for assessing disaster response.³⁸⁷ Other curricula are under development.

Finding: Many perceive a disconnect between public health theory and practice that can make education and training materials inadequate to address the needs of public health practitioners in the field.

We learned that state health departments often do not have time to play a role in translating theoretical educational materials into practical ones. One interviewee noted that his health department has done some work with academic centers for bioterrorism preparedness, but has concerns about the disconnect between the department’s day-to-day work and the materials that are produced by academia. They rely on schools of public health to develop curricula, but some perceive that educational institutions teach things for different reasons and have different goals; they seek to enhance understanding versus “doing.” On the other hand, the department does not have the capacity or resources to take educational materials and turn them into practical training materials. Additionally, one interviewee noted that materials that the state provides to local health departments are “one size fits all,” despite the different issues faced in different parts of the state. They simply do not have the human resources capacity to customize materials and do not have enough people to teach programs even when materials exist.

³⁸⁶ UPMC Health System. 2002. New center to train public health workforce in responding to bioterrorism. Available online: http://www.upmc.edu/NewsBureau/gsph/gsph_preparedness_grant.htm. Accessed October 16, 2002.

³⁸⁷ Public Health Foundation. 2002. Disaster preparedness in schools of public health: a curriculum for the new century. Available online: <http://bookstore.phf.org/prod170.htm>. October 1, 2002.

Finding: Currently, most state public health laboratories are reportedly underfunded and lacking the necessary human resources to adequately respond to a potential bioterrorism attack. Furthermore, recruiting qualified laboratory workers into state public health laboratories is becoming more and more challenging, particularly given the low salaries offered by most state health departments.

A representative of the Association of Public Health Laboratories (APHL) described the human resources challenges faced by many state public health laboratories. One can have sophisticated equipment, but you need sophisticated people to interpret and communicate the information that comes from the equipment. Public health laboratory salaries are generally very low—one state is trying to hire a PhD-level lab director at \$50,000—but they interviewee noted that this is an issue that must be addressed at the state level. In addition, there are skills related to working with bioterrorism agents that lab workers need for which training is not currently available or widespread, including the use of personal protective gear and the ability to detect and identify different agents. To address some of these issues, APHL developed the National Laboratory Training Network, designed to identify gaps in training and practice and to offer continuing education programs in those areas. Many state lab workers had participated in the Network’s anthrax training just prior to the Fall 2001 attacks and, according to APHL, their skills proved invaluable during that crisis.

The Laboratory Response Network (LRN) was created three years ago as a joint CDC, APHL and FBI effort as they charted a plan for bioterrorism readiness in the state public health laboratories. Now the LRN is comprised of 115 state, county, city, and federal laboratories with the capacity and expertise to analyze dangerous biologics such as anthrax, botulism, plague, tularemia, and brucellosis. Because the LRN was in place at the time of the anthrax attacks, LRN labs tested over 110,000 suspicious samples. They also communicated threats and needs to state and federal officials. However, APHL believes that there are still unmet needs around public health laboratory preparedness, especially around the need to develop new public health laboratory leaders. To begin to address this need, APHL submitted a proposal to CDC to develop the National Center for Public Health Laboratory Leadership. This center would “provide a central source of information, training, technical assistance, and best practices regarding the administration of public health laboratories.”

Proposed Solutions

- Efforts underway to teach current and future members of the public health and healthcare workforce about the language and command structures of emergency preparedness should be widely adopted or adapted elsewhere assuming rigorous evaluation can demonstrate their effectiveness.
- Public health departments and their emergency management counterparts at the state and local level should develop or expand opportunities for internships and rotations through their departments, as well as opportunities for joint emergency response exercises, so that those in other fields can gain a better understanding of their day-to-day activities and their role in a potential emergency.
- National public health leadership organizations should design and encourage additional efforts to bridge the gap between public health theory and practice. With private public health partners, CDC should sponsor health department internships for public health students, modeling them after current fellowship programs administered under a cooperative agreement with the Association of Schools of Public Health. However, these internships should take place in state and local public health departments in addition to CDC headquarters.

Key Theme 4: HHS and other Federal agencies need to adequately fund the range of preparedness efforts being undertaken by state health departments and private organizations while continuing to demand accountability for the effective use of these funds. Additionally, they should explore the potential advantages of expanding the role of existing

programs to meet evolving public health threats as well as the day-to-day needs of the public health system.

Finding: A number of the organizations involved in implementing workforce development and preparedness activities perceive that they are not receiving adequate funding for these efforts.

We learned that a number of organizations are enhancing or developing workforce preparedness activities in light of the Fall 2001 attacks in spite of the fact that they report not having received substantial amounts of additional funding with which to do so. For example, the Association of State and Territorial Health Officials (ASTHO) has since 1999 been tasked under a cooperative agreement with CDC to staff the Public Health Workforce Collaborative. When the Collaborative was developed, there were scarce resources available for public health workforce development activities, and CDC, ASTHO and several partner organizations believed that the Collaborative would be the wisest use of the funds. The Collaborative functions as a clearinghouse for training and other materials and hosts annual meetings for its partners and its public health audience. Initial funding was for general workforce activities. However, following the events of Fall 2001, CDC approached the Collaborative and said that it would be more useful if it expanded its role to include serving as an advisory body for a global and national workforce development plan. Initially, CDC did not offer additional funding to support this expansion, although discussions are underway to address this issue.

We also learned that many private organizations (such as physician and nurse trade associations) engaged in developing training programs aimed at enhancing the preparedness of specific sectors of the healthcare workforce are trying to do so within their regular operating budgets—or with limited additional funds—and are looking for additional funding to continue this work. Many of these organizations have not received funds directly from HHS nor through states' bioterrorism grant funding.

Finding: Many individuals and organizations voice major concerns about the sustainability of new health department positions and preparedness efforts.

We heard much concern about the sustainability of the new efforts underway to enhance preparedness. When asked about the sustainability of the state's bioterrorism preparedness and workforce development efforts, one interviewee noted that they have the same question and as yet have no approach for ensuring sustainability. New positions being filled at the state level are project positions funded specifically through the Federal bioterrorism grants, so while they are focusing resources on filling the "people gap," if the money goes away, so do the people and presumably, the programs. In another state, the interviewee noted that the level of funding received for workforce development is "adequate," but the real concern is the challenge of getting individuals' salaries up to the appropriate level. They were initially able to hire people under contract at any salary level, but now that these positions are being converted to permanent state positions, the salaries being offered are very low. When the department requested additional state funds to supplement CDC funds, this request was rejected because the state legislature was not interested in supplementing what already sounded like a very substantial level of support. We also heard concerns about the sustainability of efforts given a Federal leadership vacuum in the area of workforce preparedness. Because of recent changes in HRSA's level of funding in general, one interviewee voiced concerns about its future contributions—financial and otherwise—to workforce preparedness efforts.

Finding: Aside from terrorism preparedness, there are other pressing public health concerns that have gone unaddressed as the nation's public health infrastructure has functioned with a substantial lack of resources over the past several decades. Any efforts to strengthen workforce preparedness will accomplish little if the entities lack the basic infrastructure needed to maintain the health of the public on a daily basis.

Everyone that we interviewed agreed with the need to ensure that workforce development and preparedness activities have a dual-use component—that they generally are aimed at strengthening the ability to respond to a range of public health issues. All of the new bioterrorism positions within one state health department are being filled with dual-use and infrastructure development in mind. Another state has made an effort to address dual use issues for each focus area of the CDC bioterrorism grant and to integrate new activities into those already taking place within the department. For example, in the risk communication area, they have hired a public information officer devoted to bioterrorism issues, but this individual will actually support all of the department’s information efforts. Most of the interviewees agreed that tasking new hires with responsibilities not related to bioterrorism will increase the likelihood that they will be better integrated into their health departments and are therefore more likely to continue in their positions even if bioterrorism funding is no longer available. However, they did voice concerns about the ability to sustain these positions without such funding.

Finding: The United States Public Health Service Commissioned Corps may be able to make potentially make a substantial contribution to public health preparedness and may not currently be utilized to its full potential.

For over two centuries, Public Health Service Commissioned Corps officers have “served their country by controlling the spread of contagious diseases such as smallpox and yellow fever, conducting important biomedical research, regulating the food and drug supply, providing health care to underserved groups, supplying medical assistance in the aftermath of disasters, and in numerous other ways.”³⁸⁸ Deputy Surgeon General Kenneth Mortisugu explained that the response to September 11 and the Fall 2001 anthrax attacks was the Commissioned Corps “finest hour,” although it was lucky that the events took place in New York City and Washington, DC—cities with stronger public health infrastructures and/or proximity to members of the Corps (indeed, another interviewee had noted that the Commissioned Corps response would have been an altogether different challenge if attacks had occurred in 40 cities). One thousand of the 5,700 members of the Corps were mobilized to respond, leaving their regular duties within various HHS agencies. Dr. Mortisugu explained that the benefits of the Corps are that they are on call around the clock and that unlike a civilian force, can be ordered to action and mobilized quickly. Dr. Mortisugu noted that the Corps could potentially play a broader role in the improving the nation’s health, either through enhancing its direct service capacity or through providing technical assistance to those providing direct services. Given these benefits, drawbacks, and potentials as well as the Corps’ experience in responding to the Fall 2001 attacks, HHS is currently working on a plan for the future role of the Corps in terrorism preparedness and general enhancement of the nation’s health and public health infrastructure.

Proposed Solutions

- HHS should adequately fund the activities of organizations asked to enhance responsibilities around bioterrorism preparedness. Additionally, it should expand its funding to encourage preparedness for other manmade and naturally-occurring public health threats.
- Federal funding to states for public health preparedness efforts should be multiyear and contingent on state matching funds³⁸⁹ to help enhance sustainability and encourage state involvement in the process.
- CDC and its partner agencies should provide adequate funding for efforts that are aimed at enhancing the nation’s laboratory infrastructure and workforce and subject them to rigorous evaluation.

³⁸⁸ Office of the United States Surgeon General. 2002. History of the Commissioned Corps. Available online: <http://www.usphs.gov/html/history.html>. Accessed October 14, 2002.

³⁸⁹ As an example, States must contribute 10 percent of the amount of Federal funding received for the design, development and installation of immunization registries; and States must contribute at least one dollar for every three Federal dollars spent on the State’s breast and cervical cancer early detection program.

- CDC, HRSA and other Federal funding bodies should continue to require grantees to demonstrate that each of the efforts that they are taking to enhance workforce development and preparedness around bioterrorism will also enhance their have a ability to respond to public health challenges more generally. This is particularly important for state and local health departments, and should also be considered in cases when non-governmental entities receive grant funds.
- The Office of the Surgeon General should consider the potential advantages/drawbacks of making the Commissioned Corps a permanent force of individuals trained to respond to bioterrorism and other threats to public health and implement recruiting and retention activities that make expansion of its role feasible.

APPENDIX L- PROTECTING CRITICAL INFRASTRUCTURE AGAINST TERRORIST ATTACKS

Introduction

The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction sought to assess the nation's capability to respond to the terrorist threat to our critical infrastructure and report its recommendations for action to the President, Congress, and the public. The material presented in this appendix supported the panel's assessment.

Cyber security for critical infrastructure has received national-level emphasis for some time, while physical protection for critical infrastructure is a much more recent concern. Because of this difference, the Advisory Panel took a different approach to developing its recommendations in each of these areas. This appendix documents the source material for each area that was considered by the Advisory Panel in support of its analysis.

Objective of the Advisory Panel's Work on Critical Infrastructure Protection

The Advisory Panel sought to assess our capability to respond to the terrorist threat to our critical infrastructure and report its recommendations for action to the President and Congress.³⁹⁰ Critical infrastructure can provide an attractive target for a sophisticated terrorist adversary relying on an asymmetric strategies because of the

- Consequences of attacks that can propagate and grow over time, particularly those involving our economy and public confidence;
- Concentrations of people and function that makes many infrastructure targets "lucrative" from an terrorist's point of view, particularly if they intend to use weapons of mass destruction;
- Pervasiveness and size of our infrastructures which can provide ample opportunity for attack because the difficulty protecting all possible targets; and
- Interdependence of our infrastructures that can provide amplified and unanticipated effects.

Terms and Concepts

Several terms and concepts were important to the Advisory Panel's deliberations. While many of them are frequently used in policy discussions, it is helpful to highlight the aspects of these that are germane to the Advisory Panel's analysis. These are outlined below.

"Critical" Infrastructure

Infrastructure refers to transportation and energy systems, defense installations, banking and financial assets, water supplies, chemical plants, food and agricultural resources, police and fire departments, hospitals and public health systems, government offices, and national symbols. Much of this infrastructure is owned and operated by the private sector. "Critical" infrastructure refers to those assets,

³⁹⁰ As indicated, this work focuses on terrorist attacks against the United States. This should be distinguished from the broader, and perhaps more important, issue of the strategic threat posed to our critical infrastructure (as well as to its citizens and to other assets valuable to our nation) by nation-states. While the two may be related, and even used against us in combination, they are distinct components of the challenge we face in the new security environment.

systems, and functions so vital to the nation that their disruption or destruction would have a debilitating effect on our national security, economy, governance, public health and safety, and morale.³⁹¹

Infrastructure Sectors

The Advisory Panel's analysis has been focused on the infrastructure sectors currently used by the White House Office of Homeland Security which are outlined in the new National Homeland Security Strategy. These expand on the original sectors defined in the 1996 Presidential Decision Directive (PDD-63), the original formal guidance on critical infrastructure protection. The current sectors include:

Agriculture and Food

Banking/Finance

Chemical/Hazardous Materials

Communications

Defense Industry

Emergency Response

Energy

Government Facilities

Law Enforcement

Medical Services/Public Health

National Symbols

Transportation (including the Postal System and package shipping)

Water

Partnership with the Private Sector

The need to protect critical infrastructure from terrorist attack is the result of a new security environment shaped by a new adversary using a new way of fighting. This is not the larger threat that nation-states might pose in more traditional state-to-state crises, but in many ways is more difficult to counter.

This new threat requires a new approach to security. As described in the President's *National Strategy*, one of the more challenging aspects of this new approach is the need for a "new level of cooperation and partnership" between the government and industry, particularly with the owners and operators of the nation's critical infrastructure.³⁹²

In considering what would be needed to attain this new level of cooperation and partnership, senior representatives of industry invited by the White House Office of Homeland Security to a workshop to discuss the issue, identified a number of key provisions that would help to provide the environment necessary to foster such a relationship. This concept of a security partnership with the private sector would involve the following:

³⁹¹ This definition was used by the Office of Homeland Security in its work to define the infrastructure protection aspects of the new Homeland Security Strategy and the detailed plans needed to implement that strategy. This work was centered on a series of workshops conducted in the spring and summer of 2002.

³⁹² *National Strategy*, p. 29.

- **Government Must Decide on Clear Objectives:** The government has been struggling with policy in this area for the last 5-6 years, in part because there has been little consensus on objectives. It understands that there must be a process of mutual deliberations and decision-making on both objectives and strategy. In this situation it is problematic for the private sector to take action to comply with government requests.
- **A Paradigm Shift of Attitudes Must Take Place:** Both government and industry must reevaluate their priorities with respect to Homeland Security. Accordingly, both sides must adapt the way they view interacting with each other and make concessions to enable a true partnership.
- **Better Coordination of Homeland Security and Related Regulatory Efforts at the Federal Level:** The private sector has expressed an increasing sense of micro-management with respect to infrastructure security because of the seemingly growing number of government agencies to which it must answer at the local, state, and now federal levels.
- **Improved Two-way Flow of Security Information:** The private sector needs actionable information that provides greater clarity, i.e. intelligence, analysis, more specific threat warnings. Conversely, the private sector would share security information more freely if it were to receive information of value in return and if it were to be assured protection from the potential legal risks of doing so.
- **Meaningful Private Sector Contribution and Reliable Government Feedback:** The private sector further indicated that it would like more input into how the security information it provides is utilized. Instead of simply providing information to the government with no further feedback, industry would also like to be involved in the assessment and development of a response regarding security information it provides voluntarily, i.e. regulations/standards to be mandated, actions to be taken, and crafting of threat warnings so that they use language that is meaningful to the private sector. At the very least, the private sector would like assurance of reliable government feedback, or a sense of what to expect in return, when they voluntarily provide security information to the government.
- **Private Sector Involvement in Crafting New Legislation:** The private sector must have the opportunity — and conversely the discipline — to stay engaged in the development of new infrastructure assurance policy and legislation lest Congressional and regulatory agencies be left to craft solutions in a vacuum.
- **Attention to Individual Industry Needs (and “Don’t-Needs”):** Private sector representatives point out that a prudent security investment for one facility in one industry may be neither needed nor practical for another facility in another industry. Currently available threat information is usually non-specific. As a consequence, there is concern as to whether the security investments the private sector is asked to make will actually reflect a specific need and or ultimately have any impact. Many have put off making security investments until there is a clearer delineation of what will be required.

Strategy, Planning and Implementation

In its initial report, the Advisory Panel recommended developing a *strategy* for homeland security that is truly national in scope. Recently the Administration has implemented this defining task for improving the nation’s ability to respond to terrorist acts. To be effective, this national strategy must be underpinned by a *plan* that organizes efforts and marshals resources to prevent attacks, to protect people and assets, and to ensure prompt recovery after an attack. To have effect, the elements of the plan dealing with critical infrastructure protection must be *implemented* not only at the federal level, but also at the state, local, and territorial government level, and within the private sector firms that own and operate most of our critical infrastructure.

Approach

Cyber security for critical infrastructure has received national-level emphasis for some time, including emphasis in a Presidential Decision Directive in 1998. Physical protection for critical infrastructure is a much more recent concern, with national-level emphasis reaching a comparable level only since the attacks on New York and Washington on 9/11.

Because of this difference, the Advisory Panel took a different approach to conducting its analysis and developing its recommendations in each of these areas.

Physical Protection

For physical protection of critical infrastructure, the Advisory Panel needed to assess the capabilities of an effort that was still in the process of being defined and implemented. To do this, it reviewed two bodies of analysis undertaken for the Office of Homeland Security in the spring and summer of 2002. The first was an analysis of past panels, studies, and commissions that have examined critical infrastructure protection. The second was an associated series of workshops and interviews that engaged federal, state, local, and private sector security experts on the physical protection of critical infrastructure.

The analysis of past commissions and studies included the following sources as reflective of the central body of recent work on critical infrastructure protection:

- Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, October 1997 ("PCCIP Report").
- The Clinton Administration's Policy on Critical Infrastructure Protection, Presidential Decision Directive 63, The White House, May 1998 ("PDD 63").
- Defending America's Cyberspace: National Plan for Information Systems Protection (Version 1.0 – An Invitation to a Dialogue), The White House, 2000 ("National Plan v.1").
- Cyber Threats and Information Security: Meeting the 21st Century Challenge, Center for Strategic and International Studies, A. de Borchgrave, F. Cilluffo, S. Cardash, , M. Ledgerwood, December 2000 ("CSIS Report" or "CSIS").
- Road Map for National Security: Imperative for Change, the Phase III Report of the U.S. Commission on National Security/21st Century, February 15, 2001 (the "Hart-Rudman Commission Report" or "Hart-Rudman").
- Third Annual Report to the President and the Congress, Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, December 15, 2001 ("Gilmore Commission Third Report" or "Gilmore III").
- Defending the American Homeland, a Report of the Heritage Foundation Homeland Security Task Force, L. P. Bremer, E. Meese, January 2002 ("Heritage Report" or "Heritage").

The workshop series engaged over seven hundred experts from the private sector; state, territorial, and local governments; and federal agencies with infrastructure protection responsibilities. These participants identified a broad range of problems and candidate solutions for infrastructure protection.

Both of these efforts had limitations for the Advisory Panel's purposes. Previous commissions and studies had focused mainly on cyber security. And, many of the solutions put forth by the workshop series participants were not appropriate for the Advisory Panel's focus on the President and the Congress. This was because their work was intended to take a wide-ranging inventory of possible problems and potential solutions. As a consequence, part of the Advisory Panel's assessment was to decide on which of these candidates, or combinations of these potential solutions, were of such significance that they called for a recommendation to the Congress or to the President.

In preparation for this assessment, RAND researchers supporting the Advisory Panel developed a more specific set of physical protection measures for Advisory Panel consideration using the study review and the results of the workshops. This set, reported in this appendix, focused on matters that would allow the federal government to enable and enhance the response capabilities of other stakeholders – state and local governments, and private sector.

Cyber Security

In the case of the cyber security, the Advisory Panel needed to assess the efficacy of a policy approach that has been underway for some time. Concerns focused particularly on the effectiveness of the strategic approach we have taken and concerns about the rate of progress that has resulted.

To do this, the Advisory Panel examined the fundamental characteristics of the current approach to cyber security, and considered alternatives to that approach that were developed by a group of RAND analysts with experience in cyber security.

Organization of this Appendix

This appendix presents the material that the Advisory Panel considered in coming to its recommendations; it is organized in the following manner:

Physical Protection

- Resource Issues and Burden Sharing
- Training and Preparedness
- Intelligence, Information, and Communication
- Identification and Access Control
- Control of Critical Functions and Substances
- Legal, Regulatory, and Economic Issues
- The Role of the Public, Localities, States, and the Federal Government
- Research and Development

Cyber Security

- Current Approach
- An Alternative Approach
- Proposed Solutions

The reader may find that many of the candidate solutions address areas that are consistent with, and often expansions of, the Advisory Panel's previous recommendations. Additionally, many of them apply more broadly to countering terrorists' use of weapons of mass destruction than critical infrastructure protection. This reflects both a consistency in what state, local and private sector experts characterize as their needs and the fact that many of the problems that need to be addressed in critical infrastructure protection are actually systemic problems that are not limited to infrastructure protection in their affect.

Physical Protection

Physical protection issues and candidate solutions were drawn from analysis done in conjunction with a series of workshops and interviews conducted in support of the Office of Homeland Security. Workshop participants and agency interviewees considered four metrics in determining what was important enough to be reported for their specific sectors: loss of human life (or impact on health), economic consequences, impact on public confidence, and effects on our national security capabilities. In addition to this

judgmental assessment of consequences by sector experts, the problems and candidate solutions listed below here were evident across several different infrastructure sectors.

Each candidate solution is associated with a federal agency or department that would be responsible for leading the Federal government's efforts to implement the solution.³⁹³

Resource Issues and Burden Sharing

Issue: State and local governments and private firms, not the federal government, bear most economic costs associated with enhanced infrastructure protection. This fact leads to the danger that security and protection measures will be under-provisioned, as security can be viewed as a cost-center by many businesses.

Proposed Solution: DHS should determine an appropriate balance between state and local needs for streamlining direct federal funding. States and local governments offer different solutions for streamlining federal funding. State homeland security officials recommended that federal block grants should be provided to local communities primarily through the states. By contrast, local government representatives suggested that whenever possible federal fund should be distributed directly to local governments, bypassing the states. An important step toward a solution could be an effort to ensure flexibility and a funding approach that encourages regional collaboration.

Issue: There are currently heavy, perhaps unprecedented, demands on state resources. New financial mechanisms and/or funding vehicles will be necessary to stabilize the financial framework for state-level action in support of homeland security. Currently state-level fiscal resources are subject to unprecedented demands. Declines in revenues mean that states lack the resources to undertake fundamentally new activities in critical infrastructure protection. The federal government may need to deploy its skills and technologies to increase state capabilities to increase infrastructure protection. The other necessary part of stabilizing the funding environment is closer coordination of homeland plans and programs so as to ensure that federal and state governments both understand future spending commitments. A multiyear funding program for homeland security would bring predictability.

Proposed Solutions: DHS and OMB should institute new funding and cost reimbursement mechanisms for homeland security. It is vital that initiatives in homeland security be adequately provided with resources. Because many of the states are already under severe budgetary pressure to fund emergency response and homeland security plans and programs, federal assistance may be necessary to enhance further these capabilities. Establishing a stable and predictable funding environment for homeland security activities at the state level means that a framework must be established to determine reimbursement rates and protocols for activities already undertaken and for possible new roles and missions that states may be asked to undertake.

OMB, and if necessary Congress, should develop explicit and expedited methods for determining eligibility and paying states for homeland security costs that will be reimbursed by the federal

³⁹³ The entities named as the candidate for leading the Federal government's efforts is based on the following assumptions:

- That an Office of Homeland Security (OHS) would continue to exist in the Executive Office of the President and fulfill a role similar to the National Security Council;
- That agencies moved into the new Department of Homeland Security (DHS) would retain their current names;
- That the congress would organize its committee structure still further, rendering the naming of specific committees of congress unhelpful; and
- That significant functions relevant to homeland security would still be conducted within Departments and Agencies other than the Department of Homeland Security. If an existing agency that is to become a part of DHS is named as a candidate responsible for one of the recommended actions, both DHS and that agency is named.

government. Existing mechanisms have operated too slowly and place the states in the position of making unfortunate funding choices for the provision of public safety and emergency response capabilities based on expectations that, while reasonable, have proven to be incorrect. The federal government should provide assistance to leverage state funding in homeland security areas in order to improve capabilities.

Training and Preparedness

Issues: Institutional barriers may impede rapid response and recovery in the aftermath of a terrorist attack. Obstacles to response and recovery are hindering institutional relationships at the state and local level, between the federal and state governmental levels, and within the federal government. Coordinated prior planning involving all levels of government is vital to ensuring timely and effective post-incident response.

Some of the most problematic infrastructure protection issues are infrastructure-specific, and even equipment-specific. While the problems listed above are crosscutting in that most of them apply to a several key infrastructures or to most infrastructures, many protective-measure problems are sector-specific (affecting only one sector as opposed to several). Nonetheless, these do have potentially significant consequences if not addressed, and as a result may warrant national-level attention. An illustrative list includes: Aircraft vulnerability to exploitation in hostage, bomb, and weapons delivery vehicle scenarios; the potential for mass casualties from an incident involving shipping containers with explosive or WMD cargo; the potential for mass casualties from the exploitation of a nuclear power plant; dams that enjoy less emphasis than is warranted by their potential for exploitation because no one sector fully includes all their functions; food industry and water infrastructure personnel and regulators that do not conduct threat-based inspections due to underdeveloped relationships with the intelligence community; a water sector that lacks laboratory capacity for conducting a wide range of tests on potential contaminants.

Proposed Solution: DHS should create a long-term process to identify and update an inventory of key infrastructure nodes of national significance. While several states have developed inventories of key infrastructure nodes, and the federal government has conducted surveys of these vulnerabilities on a sector-by-sector basis, these efforts have not been coordinated or integrated across all states and sectors. These existing efforts are sufficient for the short-run, but a long-term, continuing effort should be undertaken to build and update a comprehensive inventory of critical infrastructure across the states and sectors, which involves full participation by the states and substantial private sector involvement.

Issue: Multiple approaches to response plans and incident response procedures encourage lack of uniformity in national preparedness. While all local entities cannot, and should not take the same approach to response planning and procedures, some level of standardization is necessary for a coherent response capability nationally. Rectifying this situation will require the coordination of ongoing efforts at improving emergency response capabilities organized by entities such as the National Governors Association, the Federal Emergency Management Agency, and the Office of Homeland Security.

Proposed Solutions: DHS should showcase selected state pilot systems for assessing security needs for other states and the territories. A number of the states and localities have experience in assessing the security of critical infrastructures within their jurisdictions. Sharing these insights and capabilities could provide a means of accelerating progress in vulnerability and risk assessments while also leveraging the skills in these areas that already exist outside the federal government.

DHS and DoJ should coordinate the National Homeland Security Alert System with infrastructure response plans. Where possible, infrastructure incident response and reconstitution planning should be

closely coordinated with pre-programmed responses promulgated under the National Alert System. Collaboration on these efforts in advance of a crisis will enable it to respond in a timely and flexible way during emergencies.

DHS and FEMA should build upon the current federal/state approach to natural disasters. Several state officials and their federal counterparts observed that the existing approach used by federal agencies and the states for cooperating during natural disasters works well. The states know how to seek various types of assistance from the federal government, particularly by going through the FEMA structure, which has a fairly mature and well-functioning response and recovery model. FEMA also has a well-developed structure that enables it to "reach down" and interact with local organizations.

DHS should take advantage of established federal expertise and support by using offering it in support of realistic training exercises at the state and local levels. Training and exercises, which test the capabilities of emergency response plans and personnel, are critical to assessing required improvements in preparedness. The federal government has established expertise in national defense planning facilitated through exercises. This experience should be shared with the states through a program of exercises designed to allow state and federal agencies to interact in scenarios where common intelligence, response, and vulnerability problems can be examined.

Issue: Although improving, the public health system is still largely unprepared for its role as critical responder in cases of biological, toxic materials, or radiological attack. Missing and under-developed capabilities exist in the public health sector that could seriously impede responsiveness during a national emergency. Among the shortfalls are: limited lab capacity for testing, non-compatible communications links with first responder, law enforcement and federal agencies, shortfalls in the number of skilled personnel available, and possible shortfalls in stockpiles of supplies and medical equipment.

Proposed Solutions: DHS and HHS should develop standardized protocols for dealing with emergency situations, especially those involving biohazards. Incident response requires consequence management and emergency management plans to be in place prior to an event. Protocol development will provide a vehicle to develop such plans and exercise them to improve first responder and emergency manager capabilities during an emergency.

DHS and EPA should focus on first responder training, with an emphasis on unique hazards associated with Chemical, Biological, Radiological and Nuclear (CBRN) contamination. Training of medical and public health personnel for dealing with CBRN contamination events should be a high priority. The utility to terrorists of chemical and biological agents should be taken seriously. This means an important near-term effort to expand capabilities at the state and local level, and increase collaboration with the chemical industry, should be launched.

Issue: Shortages of skilled personnel limit the ability to respond to threats. State and local governments as well as private sector firms that might be targeted frequently lack the skilled personnel necessary to conduct response efforts after a terrorist attack. A carefully coordinated attack consisting of many different incidents, or a single attack using a weapon of mass destruction (WMD), could quickly exceed the capabilities of local first responder organizations.

Proposed Solution: DoJ should create a certification regime or provide appropriate training programs for private-sector security professionals. Private security professionals make up a large portion of the security force in America. In some states, the private security professionals outnumber the number of local law enforcement officers. Federal certification/training should make clear the authorized roles of private security officers (i.e., use of deadly force) and address liability issues.

Intelligence, Information, and Communication

Issues: Information sharing and data protection practices are not up to the task. Information sharing between the public and private sectors is less efficient than it must be if critical infrastructure protection objectives are to be achieved. Basic agreement on what information should be shared, and how such information is to be protected is also lacking. There is a critical need for two-way sharing, between the federal government and those outside it (both state and local governments and private sector firms) but the underlying impediments are substantially different.

Government Sharing with non-Federal entities: A coherent federal government system to provide threat information to state and local governments as well as industry and other private sector entities does not exist. Federal rules on security classification seriously impede information sharing between federal, state, and local governments. It is not clear that the proliferation of national security clearances is an adequate solution for effectively sharing the type of information that is needed at the state level. Coordination of efforts among different levels and agencies of government is poor. Security clearance issues and rigidities in the classification of sensitive data actively hinder information sharing between public agencies at the federal and state level. Private sector access to threat information held by law enforcement and intelligence agencies is also inhibited by an absence of security clearances among critical infrastructure personnel in key positions. Current intelligence and information-sharing practice is frustrating to state-level agencies.

Industry Sharing with Government: Commercially sensitive data are also not properly handled under the current system, with possible disclosures of intellectual property placing at risk the economic prospects of private firms. This information is critical for proper vulnerability and threat assessment, particularly in the case of the cyber threat to infrastructures. Good threat information will only be available when the private sector shares its information on the attacks it is experiencing with a central entity that can sift and analyze this information, and then integrate it with information that comes from other sources to produce an informed threat assessment. The federal government needs to foster sharing information like this by addressing industry concerns about business and regulatory penalties possibly accompanying their disclosure of information. The Y2K disclosure act is viewed as a model framework for promoting information sharing between the private sector and the government while also minimizing liability, anti-trust, and FOIA risks to industry.

There is no mechanism currently in place for the critical infrastructure sectors to share pertinent security information with each other. Yet it has been well established that a disruption in one sector can have a cascading effects in other sectors. This shortfall is more notable because of the ready mechanisms that could be used to address it. Among these are: Create the capability for various sector-ISACs to share security information with each other through cooperative agreements. Establish a coordinating structure similar to the Y2K Coordination Center to facilitate sharing this information. Pattern such a sharing arrangement on the Area Police Private Sector Liaison (APPLE)/Councils used in law enforcement.

Proposed Solutions: OHS should set forth a policy for its intent and activity for sharing homeland security information with state authorities. Information sharing and intelligence interaction between states, federal agencies, local authorities and the private sector needs to take place within a new framework where categories of acceptably sharable data are decided in advance, and where processes for dissemination of warnings and risk assessments are routinized and incorporated into regular exercises and training. This policy would identify the principal topics on which sharing is likely to take place, name the principal entities with which federal agencies would interact on a regular basis to share threat and alert information, and create a framework within which sensitive private sector information would be shielded from FOIA and other information disclosure mechanisms.

OHS and NSC should create a dedicated homeland security classification system for sensitive information. The national security classification system is ill suited for information categorization and management in the homeland security domain. Information on threats and vulnerabilities in critical infrastructures is not easily classifiable and thus is in need of a different framework for protection. A dedicated classification system for homeland security would a means to implement domestic and commercial information protection objectives *and* to implement the policy for domestic threat and vulnerability information sharing. Other aspects of a proposed system include special measures for sharing sensitive information with state and local law enforcement and first responder agencies as well as private sector security managers; and design and modification of information “vehicles and frameworks” to facilitate the “two-way” flow of information between intelligence agencies and state and local law enforcement entities.

The NCTC should develop a new working arrangement for collecting, sharing, and protecting intelligence information across all levels of government. Such a new system should be based on coordination protocols and procedures agreed upon by all. It should provide for coordination among federal agencies (e.g., ATF, FBI, CIA, and NRC) on information collection, classification, and disseminated. Additionally, intelligence gathered by federal agencies should include local, national, international sources that can be shared with state and local law enforcement for operational purposes. The new arrangement should recognize that local law enforcement also needs intelligence resources for education and training of local law enforcement, for informing local intelligence gathering, and for proper dissemination of information.

DHS should use existing state pilot systems for information sharing as examples of pro-active efforts that can inform other states and the territories. A number of states already collaborate on information sharing for law enforcement and emergency response purposes. These initiatives create a basis for experimentation to discover the most effective ways to maximize information sharing among states and local governments – with a view to expanding the quality of information shared, and linking sharing mechanisms to federal and state homeland security priorities and plans.

Issue: The intelligence community needs to better understand state and local intelligence needs. The current system for collecting intelligence information is inadequate for the local-level homeland security operations. Intelligence information passes from the federal to the local levels in an ad hoc, poorly structured manner that is unlikely to address conceivable terrorist attacks. At present, the intelligence community lacks requisite understanding of the state and local authorities’ (including private sector security managers) needs for intelligence information relevant to supporting local homeland security operations. As no close relationship exists between the agriculture sector and the intelligence community, state agricultural inspectors conduct their surveillance and inspections without benefit of knowledge of the threats that are likely to be posed by terrorist organizations targeting their area.

Proposed Solution: DHS, NIPC and the NCTC should integrate domestic operational-level needs into the determination of intelligence collection requirements for protecting critical infrastructure. Essential elements of intelligence information for homeland security should be predicated, in part, on the operational needs of local-level security authorities. These should result in actionable intelligence on what types of terrorist groups might be working in a local authority’s area and what types of targets and attacks they may be planning. Current, general information provides an adequate background, but is inadequate for investments, precautionary security actions such as inspections and monitoring, and alert-response actions. This is largely because it is not informed by an understanding of the activities that local authorities engage in during routine and crisis operations. More useful information that can inform local-level operations should be collected and disseminated.

Issue: Collection of information developed at the local level that should be of interest to the intelligence and federal law enforcement communities is ad hoc. Protocols for reporting incidents (outbreaks of disease, toxic materials incidents, etc.) are lacking. Additionally, the importance of local intelligence derived through local law enforcement may be overlooked; federal needs for information generated by local law enforcement are largely determined by local authorities guessing what might be needed by federal authorities, and seldom receiving any feedback.

Proposed Solution: NCTC should integrate local law enforcement and the private sector in the intelligence collection process for securing critical infrastructures. While this entails a need to assimilate a great deal of local-level reporting, and raises the question of what organization is responsible for such analysis, it relies on the precept that most domestic human intelligence is collected, by design or inadvertently, at the local-level. Local law enforcement authorities have the contextual appreciation that allows seemingly unremarkable information to be used effectively. They have contacts that allow tips and leads to be solicited in support of an overall collection plan. The current system uses these assets by exception, rather than on a routine basis and needs to take fuller advantage of them if we are to have the level of improvement in our domestic collection capabilities that is required to secure our critical infrastructures.

Issue: Threat warnings have little relevance for industry and local authorities. General statements of heightened risk are not easily operationalized if concrete responses to them (and to associated changes in alert) are not worked out beforehand. The new national homeland security warning system can cause confusion because there has not been a willingness on the part of the federal government to help local government and private security authorities define what actions are appropriate for the different threat levels. Coupled with the high uncertainty associated with the threat, this makes it difficult for local authorities and private sector security representatives to maintain public confidence while trying to describe public risk realistically.

Proposed Solutions: DHS should provide templates or protocols and training on how to respond to various incidents, which states can adapt as necessary. Federal expertise in incident response needs to be made available to the states on expedited basis. Outreach by the federal government should be designed to communicate the details of established templates for responses to terrorist threats (i.e., CBRNE). A dialogue between the federal government and the states on these topics would help to embed these common experiences into the emergency planning of all involved jurisdictions.

USDA, FDA, and EPA should develop plans for communicating to the public about food and water safety. Plans and procedures for industry/government coordination during food and water security threats or incidents are needed. The government should take responsibility for communications to maintain public confidence in the food and water supply. Plans should include communications about food and water security risks, threats, incidents and appropriate public response and action.

Issue: Problems in communications interoperability among first responders, federal emergency management agencies, and state entities need to be resolved. Communications interoperability is a critical problem in emergency response. Different agencies use incompatible communications systems, introducing difficulties and barriers in information exchange and operations. Secure communications are a requirement; some state homeland security directors have already experienced falsified messages via e-mail. Standardized communications systems would enhance incident response, and promote efficient planning and training at the state and local level, and would allow federal agencies to communicate in a timely fashion with state counterparts during emergencies.

Proposed Solutions: DHS should invest in a secure, integrated communication system for first responders and others involved in responding to the terrorist threat. Participants at our state

workshop argued that the most important contribution from the federal level would be to develop a single communication system that links all levels of homeland security entities including first responders, infrastructure security managers, law enforcement, and state homeland security agencies. Secure communications should be an integral part of the system. Secure systems would allow for connectivity during periods in which normal civil communications links are disrupted. It is also important to take advantage of available technology that will obviate the need to abandon the communication systems' investments that state and local governments have recently made.

DHS, DoD, DoJ, and NIST should promulgate interoperability standards to ensure compatibility of communications systems used by state and local authorities, and by federal agencies. The diversity of communications system used by law enforcement, fire, emergency medical authorities across the United States could impede communications in a terrorist contingency. To overcome this difficulty, the federal government should seek to foster standards in communications equipment, protocols, and frequency utilization. First-responder investments in existing communications equipment will need to be accommodated during a transition to a more common (or at least, interoperable) homeland security communications environment. During this period federal capabilities in information sharing and cross-frequency message transmission would be used to facilitate communications among disparate agencies.

Issue: Industry's current efforts in critical infrastructure protection have gone more or less unacknowledged. Senior industry leaders have expressed frustration that there has been no acknowledgement of the very large investments already in progress by private institutions to upgrade security based on lessons learned on and since September 11th. Because of the government's lack of attention to changes that the private sector has already made or put into motion, private sector workshop participants expressed a concern that their proactive responses will be discounted and that the government will mandate additional investments, promoting activity over outcome. Industry representatives also indicated that there is little reciprocity for the investments of time and money that is put into assisting the government with intelligence gathering. Further, government feedback on security information provided by industry is erratic at best. For example, a hospital in DC sent several samples to be tested for anthrax to the FBI, but the hospital only heard back from the government on one of them and that was one of the earliest cases. The hospital is not even sure whether the subsequent specimens were ever tested.

Proposed Solutions: No potential solutions were put before the Advisory Panel.

Identification and Access Control

Issue: Authentication of identities for personnel operating systems and working in (and on) critical facilities and is inadequate. Problems of insider compromise of critical systems – perhaps allowing systems to be commandeered for attacks – are exacerbated by the lack of a unified, rigorous identification system for authenticating the identities of staff in critical areas and the designers of infrastructure facilities and systems. The problem is acute in situations in which strangers must operate together in a trusted manner either on a regular basis (such as passing custody of a gasoline tank truck) or in crisis (such as the situation that exists for law enforcement, fire and emergency response personnel working in an incident management situation).

Proposed Solutions: DoJ should facilitate the development of a nation-wide law enforcement/first responder identification system. The federal government should facilitate the development of a uniform national means of checking identities of law enforcement and first responder personnel. The system must be able to be effectively used during mutual aid operations and other cooperative efforts between the different levels of government and between different government entities at the same governmental level. It should be developed and implemented in close coordination with a homeland security classification system. It should be capable of enhanced site control that would facilitate investigations at the site of

terrorist incidents. Technologies that might be included in this identification scheme might include: biometric identifiers, magnetic strips, microprocessors embedded in a “smart” card, and other systems.

DoJ and DoT should consider a national transportation identification card. The federal government should create a single “National Transportation Identification Card” issued by the U.S. Department of Transportation that is duly recognized by state departments of transportation and relied on by the associated private industry (e.g. shipping company dispatch offices). The identification would be used by all that have control of vehicles, vessels, aircraft or transportation systems that could be used as weapons or jeopardize a significant number of passengers. This effort is currently in progress, but would gain from enhanced legislative treatment.

USDA, FDA and Customs should require tightened security and identification requirements for access to food supplies. Physical security measures are needed to assure that unauthorized individuals do not have access to areas in which food is produced, prepared, or stored.

Control of Critical Functions and Substances

Issue: Despite national-level emphasis on screening, current practice still relies on unproductive procedures and does not adequately cover key vulnerabilities. Progress in meeting baggage screening goals has been slow; full-manifest screening of vessels and aircraft is not routinely used; baggage-matching is still reliant on *ad hoc* systems, and major vulnerabilities, such as passengers and cargo of large passenger/vehicle ferries, are not adequately screened.

Proposed Solutions: DHS, TSA, Customs, and INS should perform balanced screening of cargo and persons that go aboard aircraft and vessels. Screening of this type means that an overall assessment of likely threats and coincident vulnerabilities should be undertaken, and that screening procedures should be appropriately tailored to the particular transportation mode or infrastructure situation. For example, screening of cargo and passengers for aircraft and large ferries probably warrants more depth than screening for inter-city buses, due to the potential consequences of an incident involving the former. Additionally, balanced screening should be informed by an overall assessment of the threat and vulnerability situation, including, for example, assessments that evaluate not only individual passengers, but also the entire manifest of passengers to identify flights or voyages with unusual profiles (e.g. multiple last minute, cash ticket purchases) that might be of concern.

DoJ should harmonize personnel surety policies and programs across all critical infrastructure sectors. Facilitating a dialog among infrastructure principals about personnel surety issues would help to close gaps in standards and help address resource shortfalls articulated by business regarding the adequacy of background checks for occupants of critical job categories.

DoJ should establish a system of personnel background checks for individuals with access to sensitive facilities and systems. Individuals with access to key facilities and control systems and those who design and build such systems should be subject to timely and affordable background checks to ensure employee reliability. Such checks should adhere to common standards across infrastructure sectors for similarly sensitive positions and have varying degrees of investigative depth which is matched to the level access associated with the position in question.

DHS, DoT and DoC should develop a trusted/non-trusted shipper list. Such a system would allow for trusted shippers to operate while the maritime infrastructure was on a heightened state of alert. Ports would have to develop different layouts – isolating trusted shippers from non-trusted ones, and allowing for inspection and measurement of freight traffic into and out of secure areas.

Issue: Chemical, biological, radiological, and explosive (CBRNE) storage and transportation policies may emphasize safety to the detriment of security. Visible placards on trucks and rail car, while aiding safety may also identify targets for terrorist attack. Similarly, safety procedures and requirements may hamper protection and recovery efforts. While safety measures should not be disregarded in the pursuit of security, both safety and security must be part of the overall equation. Innovative approaches, especially those relying on technology and information that can enhance both, should be sought wherever possible.

Proposed Solution: DoT, DoE, NTSB, and NRC should review chemical, biological, radiological, and explosive (CBRNE) storage and transportation policies. The federal government should review these policies, and launch a 90-day risk, threat, and vulnerability assessment review for all transportation modes. Contingency plans relating to transportation, storage, and delivery of CBRNE should be identified. The assessment review and contingency planning efforts should significantly involve the private sector if their business operations involve storage or transport of the materials in question.

Legal, Regulatory, and Economic Issues

Issue: Regulatory, liability, anti-trust, and FOIA concerns limit cooperation with the private sector. The federal government does not yet have an adequate framework for managing the FOIA, regulatory, anti-trust, and liability concerns of industry associated with information disclosure for critical infrastructure protection. Current administrative and legal rules do not allow private sector entities to share information with confidence that they will not suffer economic or legal costs due to the broader dissemination of sensitive information. This, and its chilling effect on public-private sector cooperation, is one of the most significant, pervasive, and enduring problems constraining the ability to improve protection for our critical infrastructure.

Proposed Solutions: Congress should consider liability protection. Commercial firms are concerned that any information or assessments that they disclose for homeland security/infrastructure protection purposes could be used against them. This concern has two aspects. First is the concern that private actors could use publicly disclosed information in legal cases against infrastructure operators. A second concern is that regulatory agencies could use information disclosed for homeland security purposes in order to launch enforcement actions – with possibly significant financial and business implications for the firms concerned. Legislation protecting firms from legal and regulatory actions in cases of “good faith” information provision were forthcoming during the Y2K process. Similar guarantees are sought for homeland security purposes.

DoJ, and if necessary Congress, should explore anti-trust exemption. Participants asked for explicit relief, similar to that gained during the Y2K remediation process, so that they would be able to share information with commercial competitors without fear of anti-trust litigation. Exemptions of this type were seen as key to private sector management of risk and liability issues in the terrorism/critical infrastructure protection domain.

DoJ, and if necessary Congress, should provide freedom of Information Act (FOIA) relief and provide protection against inappropriate disclosure. Freedom of Information Act disclosure of sensitive infrastructure planning documents and incident data was identified as a significant problem by private sector participants in our workshops. Concerns exist in three areas. First, infrastructure owners and operators are concerned that sensitive information about vulnerabilities might be used as potential target lists for terrorists. This information therefore requires special protection due to the potential for its misuse. A second concern is that this information might be used for purposes other than critical infrastructure protection, possibly in support of civil litigation. A third concern is that of inappropriate disclosure that might advantage competitors. Plans and programs for critical infrastructure protection

require the exchange of commercially sensitive data that require protection from inappropriate disclosure. The tradition of government “leaks” and the apparent lack of consequences for government officials who cause them, even with highly sensitive national security information, does not instill a sense of confidence or trust in the private sector. FOIA rules should be clarified and clearly enunciated to allay some private sector fears that the government will fail to protect sensitive information. A policy on inappropriate disclosure of proprietary information should be formulated and put into practice. The new Bioterrorism Act provides information security for vulnerability assessment submitted by utilities to EPA and exempts them from FOIA rules. This may serve as a good model for other sectors.

Issue: First-responder units have liability concerns that impede participation in mutual aid agreements with neighboring communities. Legal liability concerns, together with resource shortfalls at the local level, create disincentives for first responders to fully implement mutual aid arrangements with neighboring communities. This situation could further strain units that will be tasked frequently and for extended periods during regional or national emergencies.

Proposed Solutions: Congress should ensure liability protection for emergency responders when they cross jurisdictional lines. Despite current agreements, concerns remain about liability and indemnification of responders when they operate across political boundaries to execute a mutual aid agreement or perform a federal function. Response to terrorist acts requires an unprecedented level of cooperation and sharing of resources. Very similar concerns exist for volunteers, and how to organize and utilize them effectively during a crisis. Liability and indemnification applicable to mutual aid agreements should be broadly examined on the national- and state-levels. Issues arising from this review should be identified and addressed to clarify guidance and practice and actions should be taken to resolve those that act as impediments to mutual aid operations. Both the federal and the state governments may need to develop and enact legislation to resolve these issues.

OMB should seek better integration of life-cycle security issues in the government acquisitions process. Concerns exist that the pursuit of efficiency and low cost in procurement may have occurred at the risk of lower levels of security in the contractor and subcontractor elements of the defense industrial base. Flexibility in the acquisition regulations needs to be communicated to procurement officers in throughout the government, and used as a lever to improve security and information assurance performance in the government’s relations with contractors.

EPA, FDA, NRC and FCC should investigate the feasibility of expediting or waiving the permit process to enable more rapid reconstitution of critical infrastructure services following a terrorist attack. Regulatory agencies (federal, state and local) often control go-ahead authority and even access to incident sites to ensure reconstitution is not used as a way to by pass regulatory requirements. In times of crisis, these restrictions may be waived for the good of the public, but such situations seldom present themselves in day-to-day life. As a result, procedures for use of such waiver authority are often not practiced or even planned for, resulting in potentially crucial delays in reconstitution or damage limitation in the event of a terrorist attack. This is of particular concern in cases of biological attack in which there may be a need for access to the incident site to contain the spread of an contaminant or agent, but little, if any visible evidence to convince regulatory authorities that such contamination exists.

The Role of the Public, Localities, States, and the Federal Government

Issue: There is no single, unified approach to infrastructure protection that integrates physical and cyber elements. This significantly impedes national planning on homeland security. An artificial separation between physical and cyber infrastructures is unsuitable due to the fact that most sectors are adopting cyber control for physical systems. Many of the private sector representatives who attended the workshops noted that interacting with the federal government twice – once for physical security matters

and once for cyber security matters resulted in a duplication of effort and costs that they strongly objected to. The convergence of cyber and physical systems is reflected in the way most of the private sector has organized its approach to security and many felt that it should be reflected in the organizational forms chosen by the federal government to combat potential terrorist attacks on critical infrastructures.

Proposed Solution: The President should establish a single integrated approach to cyber and critical infrastructure protection. The current bifurcated approach creates duplication in information requests to the private sector, and fosters confusion among stakeholders on who it is that speaks authoritatively for the federal government on critical infrastructure matters.

Issues: Some infrastructure sectors may still fall outside the formal definition of critical infrastructure and thus receive insufficient priority. The new homeland security strategy initiatives have included several new sectors (and sub-sectors) heretofore not included in infrastructure protection planning and initiatives. Among these are food and agriculture, water, and postal services. However, an examination of what we depend on for critical functions that support our well being, economic efforts, way of life, and security reveals the absence several other industrial sectors that might warrant further consideration. For example, because dams cut across many infrastructure sectors, they enjoy less emphasis than warranted by their potential for exploitation by terrorists. The real estate industry is not identified as a critical infrastructure sector. However, it may provide a means to organize the protection of population targets such as malls, high-rise towers, and other high occupancy buildings.

Federal and state roles and responsibilities *vis a vis* Native American tribal governments need to be clarified. Clarification of roles and responsibilities in working with tribal nations on response and recovery is needed. States are often grantees for tribal nations in distributing federal money and are thereby responsible for overseeing that the money is spent appropriately. However, tribes are sovereign entities and the states have no way to hold tribes accountable for how they spend the money.

U.S. Territories are isolated and therefore the normal terms of reference for infrastructure protection often cannot be applied. In general, territories do not enjoy the same level of system infrastructure as do most states and are therefore starting at a deficit. Their closest neighbors can be countries other than the U.S. and so they require special authorities from the Department of State before entering into mutual aid agreements with other nations. Due to their special status, territories can be back doors into the US and therefore warrant additional consideration, resources, and assistance in protecting their infrastructure and borders.

Localities have specific and distinct infrastructure to protect and unique circumstances to address “one size fits all” solutions may not be effective. For example, the lock and dam system on Mississippi River is critical to commerce and health throughout the Midwest. In the state of Virginia, cities and counties are completely separate entities, and not connected in any way. Communication problems result due to independent structures, agencies, and jurisdictions that do not coordinate with one another on a regular basis. Funding formulas, in particular, must recognize this distinction. Specific concerns were voiced for certain local critical infrastructure assets, including:

- Water treatment plants;
- Aquifers;
- Nuclear power plants;
- National Labs, especially biohazard laboratories;
- Ports;
- Amusement parks and sporting events facilities;
- Bridges;
- Agriculture;
- National parks;

- Indian Heritage areas;
- Federal prisons;
- Chemical/propane facilities;
- Technology facilities; and
- Schools.

Proposed Solution: OHS should provide a clear delineation of the roles and responsibilities of the various levels and kinds of governments and delineate the role of the private sector. We are currently operating without a clear understanding of homeland security roles and responsibilities – who should protect which critical assets (including private assets), who is responsible for paying for that protection, who is in charge of different kinds and phases of incidents, who will talk to the public on specific matters and when. The federal government needs to clearly establish a well-understood and predictable framework within which public and private sector entities can understand their roles, responsibilities, and missions to protect homeland security.

Research and Development

Issues: Planning for the protection of interdependent power generation and distribution systems in the future may not fully consider the impact of new technology and associated investment incentives. The energy sector has well-developed and tested plans for system restoration and reconstitution for natural events, and this has been demonstrated over the years mainly through tests during storms. The sector recognizes the new and poorly defined threats resulting from terrorism and sabotage. It is studying means to mitigate these threats, with development of appropriate additional plans, operational processes, analytical tools, and equipment. However, deregulation and new technologies such as fuel cells and superconductivity may change the configuration of the grid and investment profiles in important ways, resulting, for example in distributed generation or multiple redundancy. However, there is no national-level effort to understand the impact of these future configurations on security. Issues that need to be analyzed in planning for future system protection are: what cost-effective mix of future technology, grid configuration, and interconnection would foster a more robust energy system, and what incentives are necessary for the private sector to bring about private investments to enhance security in the energy sector, and whether or not there should be a national policy to provide such incentives.

Control systems and centers may present lucrative targets for attack. Computer network controls over critical infrastructure systems are present in a number of different sectors. Control systems concentrated in a small number of critical nodes or facilities are potentially vulnerable to disruption during a single or small number of severe destructive incidents. Such attacks may produce effects that reach well beyond the immediate control center. SCADA (supervisory control and data acquisition) systems may actually increase the vulnerability of infrastructures that do not historically use networked computer controlled operational systems (such as the natural gas sector). The use of commercial, off-the-shelf technologies for SCADA-type controls and communications systems without adequate security enhancements, can significantly limit available approaches to protection, and may increase the pool of potential attackers able to disrupt critical systems. Complicating this problem is the fact that the concern for this problem emerged as a national-level concern over a half-decade ago, yet relatively little progress has been made in resolving the problem. Neither market forces (based on a concern that business would be interrupted by capricious or malicious attack) nor government actions (e.g. inclusion in the Clinton Administration's Policy on Critical Infrastructure Protection) have significantly improved the situation.

Operational communication equipment lacks common standards or market-based commonality. The lack of interoperability in communications equipment can seriously impede close collaboration between first responders, state emergency management personnel, and federal officials during and in the aftermath of a terrorist incident. Terrorist responses can be further complicated if differences in

communications connectivity are themselves a target for terrorist exploitation. The lack of common technical standards for this equipment or a market-dominating low-cost configuration of the equipment that would motivate purchases of compatible equipment (or even a research commitment to develop such low-cost equipment) prolongs this problem.

Mission-critical personnel need greater protection. First responder personnel who undertake significant risks during terrorism incidents must be adequately protected. At present state, local and private sector personnel often have only limited access to modern personal protective equipment (PPE). This shortfall limits their effectiveness in the field, and may create situations where local law enforcement and fire resources will be less useful for incident management.

Proposed Solutions: Congress should investigate specific liability limits for vendors of remediation/security technologies. Developers of technologies used to enhance critical infrastructure protection and homeland security have identified potential liability problems arising from the experimental nature of the technologies in play. The federal government should examine this issue, and seek to develop mechanisms that reconcile homeland security objectives with product and technology liability requirements (insurance and indemnification are two areas where policies are necessary).

DHS and other R&D agencies should provide federal support for homeland security research and development.³⁹⁴ The federal government should launch a specialized research and development activity aimed at enhancing homeland security and critical infrastructure protection. Plans should also be in place to migrate technologies from the defense (in the case of technologies applicable to national security and homeland security) and other government efforts to the private sector for use in infrastructure protection. A key area of emphasis in this research should be to lower the costs of a given (and sufficient) level of technological performance, rather than to strive for ever-more elegant performance. This is cost-reduction strategy is a necessity if technology and advanced equipment are to be pervasively adopted and employed by local authorities and the private sector, due to the very limited nature of capital investment budgets of these organizations. Alternative strategies, such as federal funding for local acquisition of existing high-tech equipment may be necessary in the short-run, but may lock-in aging technology and dampen innovation over longer time frames.

DHS and NIST should develop standards in security technology for both physical and information infrastructure. A lack of RDT&E (research, development, testing, and engineering) on security was identified as a significant shortfall in our current posture. Standards development would allow the federal government to encourage the private sector to provide products essential to enhancing the security of infrastructures and of the interdependencies among them.

DHS should undertake a comprehensive analysis of critical infrastructure interdependencies with a view to identifying cross-infrastructure links that could exacerbate human loss of life and material destruction. This analysis should be used to prioritize response plans to enable rapid recovery from terrorist attacks and optimal information dissemination on infrastructure threats.

DoE, and EPA should investigate and design responses to the vulnerability of refineries, chemical plants, and other industrial facilities to terrorist attack. These assaults could be launched from the

³⁹⁴ Other departments and agencies currently involved with R&D applicable to homeland security and counter terrorism are: Department of Agriculture, Department of Commerce, Department of Defense, Department of Education, Department of Energy, Department of Health and Human Services, Department of Housing and Urban Development (HUD), Department of the Interior, Department of Justice, Department of State, Department of Transportation, Department of the Treasury, Department of Veterans Affairs, Environmental Protection Agency, National Aeronautics & Space Administration, National Science Foundation, Nuclear Regulatory Commission.

ground, or might involve aircraft. In either case, comprehensive vulnerability assessments and defense planning need to be undertaken to avoid possible catastrophic losses in service.

USDA, FDA, and DoT should conduct a comprehensive risk assessment for the food transport, processing, distribution, and retail system. The assessment might best be conducted by an independent body such as the National Research Council, but would necessarily draw on government and industry expertise.

USDA and HHS should launch an initiative to improve surveillance, detection, and verification capabilities – with a view to providing tools and resources to the agriculture and public health sectors. State and local response agencies, as well as farmers, need access to improved technological and communications tools to secure the food supply.

The Special Case of Cyber Security

The Current Approach

Progress since the Last Report

As pointed out in the last Commission Report, cyber security is an extremely complex topic that touches all infrastructure sectors and spans national security, law enforcement, civil liberties, commercial and other private-sector interests. Any improvement in cyber security will require unprecedented partnerships between government and private entities. Additionally, the report points out that the pace of technological advance in the cyber field compounds the problem. There are no easy solutions and little historical precedent that can guide our efforts to enhance cyber security while balancing other interests and considerations.

While it could be argued that the greatest part of the problem rests on organizational practices and individual behavior which might be easily changed, the fact that many do not institute precautions in the routine use of cyber systems argues that such changes are motivated by incentives that are perceived (correctly or not) to be of greater value than security measures, rendering such changes unlikely unless this perception is changed.

Nonetheless, progress has been made on the recommendations outlined in the previous Commission reports in four key areas:

1 – Improving National Coordination: The Commission recommended that the Federal government should - **Include private and State and local representatives on the interagency critical infrastructure advisory panel. Create a commission to assess and make recommendations on programs for cyber security.** Progress in these areas has mainly taken place in the context of the White House Office of Cyber Security's efforts to develop a national strategy for cyber security. These have included a series of "town hall" meetings to engage not only State and local representatives, but also the private sector including private citizens and the continuance of the President's Council on Critical Infrastructure Protection (PCCIP) which addresses the latter issue to some extent.

2 – Enhancing Detection, Alert, Warning, and Response: The Commission recommended that the Federal government should - **Establish a government funded, not-for-profit entity for cyber detection, alert, and warning functions.** Progress in this area is exemplified by the government's efforts to develop a cyber warning and alert network (CWAN). However, this is envisioned to be a federal government program that would be available to some private organizations. Another model, closer to that envisioned by the Commission, is provided by CERT and its Coordination Center (CERT/CC). Its 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 the security

changes needed in networked systems. CERT also publishes research and training materials on cyber security. The center is funded by the federal government and operated by Carnegie Mellon University. Additionally, the security and infrastructure assurance structure set up by PDD-63, which includes the National Infrastructure Protection Center (NIPC), the Critical Infrastructure Assurance Office (CIAO), and the industry-centered Information Sharing and Analysis Centers (ISACs), has evolved over time to provide much of the functions suggested by the Commission.

While it may be argued that these structures could improve their warning capabilities, experts point out that the most important threats, sophisticated attacks by organized, well-funded adversaries, possibly backed by a foreign government, will most likely not be detected until after the fact unless an aggressive intelligence program is successful in forewarning of such attacks. Warning systems are unlikely to be sufficient for this purpose, even with a substantial increase in intelligence collection efforts above current levels.

3 – Improving Legal and Law Enforcement Processes: The Commission recommended that the Federal government should - **Convene a “summit” to address Federal statutory changes that would enhance cyber assurance. Create a “Cyber Court” patterned after the court established in FISA.** No action has been taken on these recommendations.

4 – Fostering an Effective Research and Development Agenda: The Commission recommended that the Federal government should - **Develop and implement a comprehensive plan for cyber security research, development, test, and evaluation.** Progress in this area is exemplified by the efforts of the Institute for Information Infrastructure Protection (I3C), a not-for-profit organization established by Congress. It is currently in the formative stages – developing a National Cyber Security R&D Agenda focused on areas underserved by ongoing public or private efforts to develop tools, practices or other research-based capabilities. The first version of this Agenda is expected in December 2002, but with the advent of a new office of Homeland Security, its continuance and funding remains to be determined.

It is of particular importance here to note that good data on the cyber threat are very limited. While private sector firms undertake assessments of attacks that threaten substantial business interests internally, the results are (understandably) rarely made public. In recent reports, even private sector firms specializing in marketing such data have indicated that existing data have real limitations, and that they are mainly “suggestive.” The federal government research program should support more extensive efforts to analyze the nature and objectives of cyber attacks with full involvement of the intelligence and federal law enforcement communities.

Assessment

The positive effects of these actions have substantial lead times and are, in essence, investments taken for strategic, long-term effect. While we are seeing some dividends from them in the short term, their real payoff in enhanced cyber security will play out over a number of years, and many initiatives are still in their implementation phase. One short-term development that may indicate progress is that the private sector has recently demonstrated a willingness to invest in cyber security – software, firewall appliances, and monitoring services. One of the few information technology sectors to thrive during the recent economic downturn and the dot-com bust is the security sector. Several indicators (revenues, earnings, stock prices, and employment) suggest that this sector is doing well, or at least much better than other infotech sectors. Another indicator of progress is that the private sector is showing signs that it believes that cyber security offers investment opportunities, which is essential for dealing with cyber threats over the long-term. Since government funding will, by necessity, be a small part of the total funding required to make networks secure, this is an important development. Some indicators of this are that major firms have also acquired companies that have demonstrable cyber security skills or technologies on favorable

terms (e.g. cash buyouts at prices that reflect substantial future business). Such acquisitions in the current economy are a serious indicator of market expectations.

Despite the understanding that the greatest payoffs to current cyber security initiatives will be in the long-run and these short-term indicators of progress, there are concerns. As we assess our progress in cyber security, it is clear that some aspects of the initial phase of the nation's efforts are constraining the progress. The most telling constraint is the overall approach that we have taken with cyber security to date. Briefly this could be characterized as emphasizing and distinguishing cyber security in ways that have isolated it from other security considerations and from the operational functions that it protects. This has been useful during the initial phase of our efforts when we were defining and explaining a unique and complex aspect of the security equation, educating the public and the government as to the threats we face, and planning. However, this utility has changed to a hindrance as we try to *implement* cyber security measures throughout the public and private sectors.

The Concern as We Move Ahead

In short the concern is that the current approach has not yet provided consequences for the private sector or ignited the market forces that they respond to, or for accountability for the government. As a result cyber security has been relegated to an inconsequential status that has been overcome by what are perceived as more consequential events.

This current approach can be defined by the following characteristics:

- Regarding cyber security as an isolated and specialized field, thus limiting its perceived relevance to day-to-day outcomes and even its relevance to what are viewed as clear and present security threats.
- Creating a separate strategy and executive branch organizational structure that has reinforced the isolated and add-on nature of cyber security to the extent that it draws criticism from the private sector as burdensome bureaucratic layering, and significantly detracted from its relevance.
- Focusing on the need for public-private partnership so intensely that the government has largely failed to exercise any of its powers other than persuasion. The result has been that there are essentially no consequences for those who fail to take prudent cyber security actions.
- Applying this same standard to the public sector to the extent that there is no accountability for cyber security lapses and there are essentially no consequences for Federal government agencies that do not take prudent cyber security actions despite OMB rules to the contrary.
- Relying on self-verification or security provider verification to the extent that there is no objective, independent, third-party source of checks and balances in the current approach to cyber security. This is equivalent to allowing the consultants to also be the auditors.

The unique nature of the cyber threat – complex and difficult to understand to many, rare in its extreme occurrence, and usually of such small consequence to individual decision makers that it warrants only moderate security investments of either time or money – coupled with the approach described above has limited progress in several ways. It has precipitated criticism of the Federal government by the private sector and local and state authorities for doubling the bureaucratic burden imposed on them for coordination, seeking resources, and attending meetings. It has motivated a cynicism and a subsequent desire to handle the problem in ways that resource decisionmakers feel are effective and that they can afford. As a result, many private sector security managers (and even the Information Sharing and Analysis Centers in some cases) have chosen to integrate cyber security and physical security in their overall security operations – in sharp contrast to the Federal government's bifurcated approach – and to invest in it accordingly. There has also been an impact at the Federal level as evidenced by the difficulty engendered by this approach in designing a practical way to implement a separate approach to cyber security. This, in turn, has impeded (now for several years) the ability to define a national cyber security strategy that could move beyond a draft stage. Ironically, while the draft strategy's inability to move

beyond exhortations has been viewed as the result of a desire to assure industry that the government will not over regulate cyber security matters, privately industry sources criticize the draft as lacking sufficient mandates to have any affect. Perhaps the most telling argument that a bifurcated approach to security is not optimal deals with the threat itself. Sophisticated attackers, our principal concern, will know that they get the greatest return from a combined cyber and conventional attack since the critical nodes in any given infrastructure are likely to be more vulnerable to one mode than the other

An Alternative Approach

In light of these concerns about the effectiveness of the current approach in implementing cyber security measures, the Advisory Panel is urged to consider an alternative approach be undertaken in conjunction with the recommendations it has already made. The characteristics of an alternative approach that could better address the concerns outlined above are:

- As proposed in the previous section of this report, integrate cyber security for critical infrastructure protection into Federal strategy, planning and organization for homeland security.
- For the immediate future, identify and focus only on a limited set of key government and infrastructure areas that 1) are clearly related to the well-being of the U.S., 2) have a national-level impact, 3) are manageable in number, and 4) provide a clear linkage between cyber security failures and outcomes such as the disruption of a critical function or service, for example public information systems, the banking and finance infrastructure, and electricity generation and distribution.
- With regard to the private owner-operators of critical infrastructure, focus on outcomes in areas more concrete to private sector decisionmakers – such as interruption of electric power, failure of voice and data communications, or disruption of the banking and finance sector.
- With regard to the government, focus on outcomes that are clearly linked to agency mission accomplishment – such as an inability to communicate within the FBI’s law enforcement network, intrusion into DoD systems, corruption of FAA data, failure of Federal government agencies or entities like TVA or AMTRACK to provide critical power or transportation, or denial of service in proposed homeland security networks connecting state and local authorities with Federal authorities.
- Rely on market-based and monetary mechanisms such as realistically limited liability, specified and delimited fines, and insurance rates to the greatest extent possible. Cause these mechanisms to be tied to failure to deliver critical functions or services, and base the relationship to cyber security on a failure to meet clearly defined standards and certifications, which are based on research and empirical evidence.
- Any liability regime should be rationally structured and bounded, but should provide incentives to companies and individuals to adopt better security.

The effect of this change in approach is both more practical and more modest than the implied objectives of current efforts and draft plans which can be interpreted as seeking high levels of security for everyone from private individuals to those national-level entities that are critical to national and homeland security. This change seeks to simply raise the level of security in manner that is related to the criticality of the system involved in an affordable way. It also changes the focus of security responsibility from cyber service, hardware, and software providers to those providing final services or functions to the public or government. Particularly, it seeks to thwart attacks based on *existing and known vulnerabilities* in pervasively sold and used information/communication systems by using economic incentives passed on through final service providers who would suffer consequences unless they rely on cyber service, hardware, and software vendors who can offer objective, independent evaluations of their products. This implies that infrastructure function and service providers (including government infrastructure providers) will be held accountable for a failure to provide critical functions to the public or government. If they choose to use cyber service or software providers who provide products that result in security breaches they must resolve the resulting liability consequences with their providers – either by choosing more secure products (and declining to purchase from less secure software providers) or by insuring

themselves against such failings. The same paradigm would apply to infrastructure providers' choices about linking their system to the Internet through insecure Internet Service Providers (ISPs) – the ultimate infrastructure function or service provider would be held accountable for a failure to provide a concrete and measurable level of service. If they make poor choices about links to the Internet or the manner in which they did so, they must resolve the issue with their ISPs.

Actions Required to Initiate an Alternative Approach

Such a revised approach would require three major incentive structures, which will, in turn, require the actions listed under each:

1) Allow decision makers both inside and outside the government to make security resource allocations and other investment decisions that are informed by costs and benefits that reflect the consequences of a failure to accomplish a mission or provide critical functions to the public and the government. The Executive Branch (to include the Departments, Independent Agencies, and Executive Office of the President Offices) should address the bulk of cyber security issues as an integral part of a Telecommunications and Information Technology infrastructure sector. Cyber security matters associated with other sectors should be addressed in parallel with (and balanced against) physical security and other components of the overall security picture.

The Congress should consider legislation to define specific and fixed liability on the part of the function or service providers that will compensate those who suffer if existing regulators or oversight bodies find that providers fail to provide the specified level of service (relying importantly on any currently established critical levels of service) for situations in which an information/communications system is involved, and the provider is found to employ an information/communication system that does not meet established standards. The public customers and/or the government customers should be the beneficiary of this compensation.

The Department of Commerce in conjunction with the insurance industry should examine the viability of an insurance market to cover this well-defined and specified liability for failing to meet system standards in situations where critical levels of functions and services are not provided and an information/communications system is involved.

2) Provide for consequences for those not complying with standards, if an outcome, such as failing to provide a specified level of a critical function, is found to involve an information/communications system. The existing government oversight bodies in both the Legislative Branch and the Executive Branch should assess whether they need to create new ways to determine what specific levels of critical service or function are needed for public safety or national and homeland security. The existing regulatory and oversight bodies should consider whether new mechanisms are needed to determine if a specified level of critical service or function is not being provided and if there are adequate mechanisms to determine if a) an information/communications system is involved in the failure (*but not necessarily the cause of the failure*), and b) if the information/communications system is in compliance with standards.

3) Provide for objective, independent third-party determination of standards or certification criteria based of research and empirical evidence.

The Department of Homeland Security should invest in R&D to be conducted by the National Institute of Standards and Technology to define, in partnership with the private sector, appropriate standards of security for information/communications system software, architecture, and configuration. The

Department of Commerce in conjunction with the software industry should examine the viability of an objective and independent “Underwriters Laboratory” approach determining system compliance with

standards in a standard systems' interface environment (due to the problem of compatibility). Part of this viability examination should determine the practicality of ultimately funding this service with users' fees.

The Congress should consider legislation to require standards compliance by either NIST or an objective, independent laboratory as a prerequisite for engaging in either interstate commerce or providing a critical infrastructure function or service to the public or the government.

Proposed Solutions

To initiate this alternative approach to cyber security for our critical infrastructure, the Advisory Panel should consider the following proposed solutions:

The President consider the change in the nation's approach to cyber security as outlined above and charge the Department of Homeland Security to work with Executive Branch departments, agencies, and EOP offices to incorporate such an approach in the National Homeland Security Strategy and its supporting plan. Further, the President should charge the Department of Homeland Security to work with the Congress to develop legislation as outlined above to underpin this change in approach to cyber security. And finally, that the Congress that it examine the suggested approach and consider the legislation that would be necessary to operate such a system as outlined above on market-based mechanisms with strong private sector involvement, rather than through regulatory actions by the Executive Branch.

APPENDIX M– CRITICAL INFRASTRUCTURE INFORMATION

An Extract of Pub. L. 107-296 (H.R. 5005, 107th Congress, 2nd Session), November 25, 2002

Subtitle B--Critical Infrastructure Information

SEC. 211. SHORT TITLE.

This subtitle may be cited as the 'Critical Infrastructure Information Act of 2002'.

SEC. 212. DEFINITIONS.

In this subtitle:

- (1) AGENCY- The term 'agency' has the meaning given it in section 551 of title 5, United States Code.
- (2) COVERED FEDERAL AGENCY- The term 'covered Federal agency' means the Department of Homeland Security.
- (3) CRITICAL INFRASTRUCTURE INFORMATION- The term 'critical infrastructure information' means information not customarily in the public domain and related to the security of critical infrastructure or protected systems--
 - (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;
 - (B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or
 - (C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.
- (4) CRITICAL INFRASTRUCTURE PROTECTION PROGRAM- The term 'critical infrastructure protection program' means any component or bureau of a covered Federal agency that has been designated by the President or any agency head to receive critical infrastructure information.
- (5) INFORMATION SHARING AND ANALYSIS ORGANIZATION- The term 'Information Sharing and Analysis Organization' means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of--
 - (A) gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof;
 - (B) communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure or protected systems; and

- (C) voluntarily disseminating critical infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).
- (6) PROTECTED SYSTEM- The term `protected system'--
- (A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and
- (B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.
- (7) VOLUNTARY-
- (A) IN GENERAL- The term `voluntary', in the case of any submittal of critical infrastructure information to a covered Federal agency, means the submittal thereof in the absence of such agency's exercise of legal authority to compel access to or submission of such information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.
- (B) EXCLUSIONS- The term `voluntary'--
- (i) in the case of any action brought under the securities laws as is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47))--
- (I) does not include information or statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(I)); and
- (II) with respect to the submittal of critical infrastructure information, does not include any disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities; and
- (ii) does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.

SEC. 213. DESIGNATION OF CRITICAL INFRASTRUCTURE PROTECTION PROGRAM.

A critical infrastructure protection program may be designated as such by one of the following:

- (1) The President.
- (2) The Secretary of Homeland Security.

SEC. 214. PROTECTION OF VOLUNTARILY SHARED CRITICAL INFRASTRUCTURE INFORMATION.

(a) PROTECTION-

- (1) IN GENERAL- Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study,

recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2)--

(A) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act);

(B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official;

(C) shall not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith;

(D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this subtitle, except--

(i) in furtherance of an investigation or the prosecution of a criminal act; or

(ii) when disclosure of the information would be--

(I) to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(II) to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the General Accounting Office.

(E) shall not, if provided to a State or local government or government agency--

(i) be made available pursuant to any State or local law requiring disclosure of information or records;

(ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such information; or

(iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act; and

(F) does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.

(2) EXPRESS STATEMENT- For purposes of paragraph (1), the term 'express statement', with respect to information or records, means--

(A) in the case of written information or records, a written marking on the information or records substantially similar to the following: 'This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002.'; or

(B) in the case of oral information, a similar written statement submitted within a reasonable period following the oral communication.

(b) LIMITATION- No communication of critical infrastructure information to a covered Federal agency made pursuant to this subtitle shall be considered to be an action subject to the requirements of the Federal Advisory Committee Act (5 U.S.C. App. 2).

(c) INDEPENDENTLY OBTAINED INFORMATION- Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority, or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a), including any information lawfully and

properly disclosed generally or broadly to the public and to use such information in any manner permitted by law.

(d) TREATMENT OF VOLUNTARY SUBMITTAL OF INFORMATION- The voluntary submittal to the Government of information or records that are protected from disclosure by this subtitle shall not be construed to constitute compliance with any requirement to submit such information to a Federal agency under any other provision of law.

(e) PROCEDURES-

(1) IN GENERAL- The Secretary of the Department of Homeland Security shall, in consultation with appropriate representatives of the National Security Council and the Office of Science and Technology Policy, establish uniform procedures for the receipt, care, and storage by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government. The procedures shall be established not later than 90 days after the date of the enactment of this subtitle.

(2) ELEMENTS- The procedures established under paragraph (1) shall include mechanisms regarding--

(A) the acknowledgement of receipt by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government;

(B) the maintenance of the identification of such information as voluntarily submitted to the Government for purposes of and subject to the provisions of this subtitle;

(C) the care and storage of such information; and

(D) the protection and maintenance of the confidentiality of such information so as to permit the sharing of such information within the Federal Government and with State and local governments, and the issuance of notices and warnings related to the protection of critical infrastructure and protected systems, in such manner as to protect from public disclosure the identity of the submitting person or entity, or information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is otherwise not appropriately in the public domain.

(f) PENALTIES- Whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any critical infrastructure information protected from disclosure by this subtitle coming to him in the course of this employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18 of the United States Code, imprisoned not more than 1 year, or both, and shall be removed from office or employment.

(g) AUTHORITY TO ISSUE WARNINGS- The Federal Government may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, or the general public regarding potential threats to critical infrastructure as appropriate. In issuing a warning, the Federal Government shall take appropriate actions to protect from disclosure--

(1) the source of any voluntarily submitted critical infrastructure information that forms the basis for the warning; or

(2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

(h) AUTHORITY TO DELEGATE- The President may delegate authority to a critical infrastructure protection program, designated under section 213, to enter into a voluntary agreement to promote critical infrastructure security, including with any Information Sharing and Analysis Organization, or a plan of action as otherwise defined in section 708 of the Defense Production Act of 1950 (50 U.S.C. App. 2158).

SEC. 215. NO PRIVATE RIGHT OF ACTION.

Nothing in this subtitle may be construed to create a private right of action for enforcement of any provision of this Act.

Subtitle C--Information Security

SEC. 221. PROCEDURES FOR SHARING INFORMATION.

The Secretary shall establish procedures on the use of information shared under this title that--

- (1) limit the redissemination of such information to ensure that it is not used for an unauthorized purpose;
- (2) ensure the security and confidentiality of such information;
- (3) protect the constitutional and statutory rights of any individuals who are subjects of such information; and
- (4) provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

SEC. 222. PRIVACY OFFICER.

The Secretary shall appoint a senior official in the Department to assume primary responsibility for privacy policy, including--

- (1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;
- (2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
- (3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;
- (4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; and
- (5) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters.

SEC. 223. ENHANCEMENT OF NON-FEDERAL CYBERSECURITY.

In carrying out the responsibilities under section 201, the Under Secretary for Information Analysis and Infrastructure Protection shall--

- (1) as appropriate, provide to State and local government entities, and upon request to private entities that own or operate critical information systems--
 - (A) analysis and warnings related to threats to, and vulnerabilities of, critical information systems; and
 - (B) in coordination with the Under Secretary for Emergency Preparedness and Response, crisis management support in response to threats to, or attacks on, critical information systems; and
- (2) as appropriate, provide technical assistance, upon request, to the private sector and other government entities, in coordination with the Under Secretary for Emergency Preparedness and Response, with respect to emergency recovery plans to respond to major failures of critical information systems.

SEC. 224. NET GUARD.

The Under Secretary for Information Analysis and Infrastructure Protection may establish a national technology guard, to be known as 'NET Guard', comprised of local teams of volunteers

with expertise in relevant areas of science and technology, to assist local communities to respond and recover from attacks on information systems and communications networks.

SEC. 225. CYBER SECURITY ENHANCEMENT ACT OF 2002.

(a) SHORT TITLE- This section may be cited as the 'Cyber Security Enhancement Act of 2002'.

(b) AMENDMENT OF SENTENCING GUIDELINES RELATING TO CERTAIN COMPUTER CRIMES-

(1) DIRECTIVE TO THE UNITED STATES SENTENCING COMMISSION- Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this subsection, the United States Sentencing Commission shall review and, if appropriate, amend its guidelines and its policy statements applicable to persons convicted of an offense under section 1030 of title 18, United States Code.

(2) REQUIREMENTS- In carrying out this subsection, the Sentencing Commission shall--

(A) ensure that the sentencing guidelines and policy statements reflect the serious nature of the offenses described in paragraph (1), the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses;

(B) consider the following factors and the extent to which the guidelines may or may not account for them--

(i) the potential and actual loss resulting from the offense;

(ii) the level of sophistication and planning involved in the offense;

(iii) whether the offense was committed for purposes of commercial advantage or private financial benefit;

(iv) whether the defendant acted with malicious intent to cause harm in committing the offense;

(v) the extent to which the offense violated the privacy rights of individuals harmed;

(vi) whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice;

APPENDIX N-STATEMENT OF SENATOR ROBERT BENNETT ON CRITICAL INFRASTRUCTURE INFORMATION

Congressional Record, November 19, 2002, pp. S11562-S11563

Mr. BENNETT. Mr. President, for several years, I have been actively working to protect our Nation's critical infrastructure and promote information sharing between the government and the private sector. From my experience with Y2K, I recognized that our Nation's critical infrastructure was vulnerable and that the private sector and the government needed to cooperate. Last year I introduced S. 1456, the Critical Infrastructure Information Security Act of 2001, which sought to bolster critical infrastructure security by fostering and encouraging critical infrastructure information sharing. Both the Senate Government Affairs Committee and the Senate Energy and Natural Resource Committee held hearings on this issue. Once legislation creating the Department of Homeland Security was introduced in the Senate, I worked to ensure that some of the protections found in S. 1456, specifically protection from public disclosure pursuant to the Freedom of Information Act (FOIA), were addressed and considered in the proposed legislation.

The need for congressional attention on this issue stems from the growth of new technology and the increased reliance on computer networks created new vulnerabilities. For the past two decades, once physically distinct operations, controls and procedures have been tightly integrated with information technology. Pipelines can be controlled remotely. A vulnerability in a telecommunication systems can impact the functioning of the Department of Defense and the financial services sector. Sectors are more interconnected and more interdependent.

Eighty-five percent of the United States' critical infrastructures, the essential services that if disrupted or destroyed would impact our economic or national security such as financial services, telecommunications, transportation, energy, and emergency services, are still owned and operated by the private sector. Osama bin Laden has called on his supporters to attack the pillars of the U.S. economy the private sector.

If the private sector and the Federal Government are increasingly interconnected and are targets for those who wish us ill, it makes sense for both targets to share information with each other. We have to think differently about national security, as well as who is responsible for it. In the past, the defense of the Nation was about geography and an effective military command-and-control structure. Now prevention and protection must shift to partnerships that span private and government interests.

Yet the private sector has no access to government information about possible threats, much of which is often classified. The Federal Government, with its unique information and analytical capabilities, lacks specific information from the private sector on attacks. Both parties have a blind spot and only see parts of the problem. Government and industry would benefit from cooperating in response to threats, vulnerabilities, and actual attacks by sharing information and analysis. If the Department of Homeland Security is tasked to match threats with vulnerabilities, the private sector must be a willing partner.

Although the Senate bipartisan FOIA agreement that I negotiated is not included in the current homeland security bill, I am pleased that the final version includes a number of provisions that will foster critical infrastructure information sharing. As the government and the private sector cooperate and begin to exchange information, we will be in a better position to prevent, respond to and recover from future attacks to our country.

APPENDIX O-STATUS OF FEDERAL BUDGET REQUESTS FOR ASSISTANCE TO STATES AND LOCALITIES

This appendix provides a brief overview of Federal funds provided to State and local entities in an effort to improve their ability to respond to terrorist attacks. As mentioned in previous reports by the Advisory Panel, these funds have traditionally been funneled through the Department of Justice or FEMA as part of their law enforcement or emergency response training and equipment programs. However, after the attacks of 11 September 2001, more attention has been focused on the essential role that State and local first responders play combating terrorism. Therefore, the following table focuses specifically on funds that will likely be provided directly to State and local entities in the form of grants.

After the 11 September 2001 terrorist attacks against the World Trade Center and Pentagon, the Congress provided the President with a \$40 billion supplemental budget to respond to these attacks. Of this \$40 billion, approximately \$8.2 billion was designated as assistance to Pennsylvania, New York, and Virginia to aid in the immediate mitigation and response activities, and an additional \$2.5 billion was made available to HHS as part of its emergency fund to assist the Federal, State, and local public health system. Only approximately \$240 million of the \$40 billion was given directly to State and local entities to assist in their preparedness activities.

In the FY03 budget, recently submitted to the Congress, the President requested an additional \$3.5 billion to go directly to State and local entities to assist in their preparedness efforts, \$1.2 billion to increase hospitals' capacity to respond to bio-terrorism incidents, and \$175 million to improve interoperability in communication networks between Federal, State and local entities.

This information is provided in the following table, along with the amounts contained in the current appropriations bills in the House and Senate. The appropriations bills that include the additional amounts reflected in the table have not, at the time of this writing, been passed by the Congress and signed by the President.

Table 1. Status of Budget Requests for State and Local Preparedness

President's Budget Submissions: Summary (in Millions)	
Assistance to First Responders	\$ 3,500.00
Increase Hospitals' Capacity for Tio-Terrorism	\$ 1,200.00
Improve State and Local Communications Interoperability	\$ 175.00
Total	\$ 4,875.00

House Appropriations Bills: Summary (in Millions)	
FEMA -- Emergency Management, Planning and Assistance	\$ 367.00
FEMA -- Pre-Disaster Mitigation	\$ 236.25
FEMA -- Pre-Disaster Mitigation Grants per State per Year	\$ 13.75
FEMA -- Citizen Corps	\$ 30.00
FEMA -- Communications Interoperability	\$ 78.00
FEMA -- Firefighter Assistance Grants	\$ 450.00
Total	\$ 1,175.00

Senate Appropriations Bills: Summary (in Millions)	
DOJ -- Equipment Grants	\$ 1,047.00
DOJ -- Exercise Grants	\$ 20.50
DOJ -- Technical Assistance Grants	\$ 5.00
HHS -- Public Health Improvement	\$ 117.70
FEMA -- Fire Grant Program	\$ 900.00
FEMA -- First Response Interoperable Communications	\$ 180.00
FEMA -- S&L Emergency Planning Grants	\$ 75.00
FEMA -- State Emergency Operations Centers	\$ 180.00
FEMA -- Emergency Responder Training	\$ 60.00
FEMA -- Community Emergency Responder Teams	\$ 15.00
Total	\$ 2,600.20

APPENDIX P—DEPARTMENT OF DEFENSE CBRNE RESPONSE ASSETS

Chemical Biological Rapid Response Team (CB-RRT): The CB-RRT is the DoD joint national response asset mandated by Public Law 104-201. The CB-RRT deploys in support of the lead federal agency and assists in the detection, neutralization, containment, dismantlement, and disposal of WMD articles containing (or suspected of containing) chemical and/or biological or related hazardous materials and assists first responders in dealing with potential WMD consequences. Coordinates and synchronizes DoD's technical assistance (medical and non-medical) to respond to a WMD incident, terrorist attack, or designated National Security Special Event. Focused on domestic, but responsive worldwide.

Defense Threat Reduction Agency's (DTRA) Consequence Management Advisory Team (CMAT): CMAT contains military and civilian experts trained in emergency response, command and control, communications, public affairs, law, health physics, radiation medicine, site remediation, emergency planners, and chemical/biological experts according to the specific mission needs. CMAT assists the On-Scene Commander through the DoD Lead Commander in the management of WMD related issues. The CMAT can advise on the DoD assets best suited to meet the requirements of the incident. The team is on-call 24 hours a day and can deploy within 4 hours of notification.

Joint Task Force Civil Support (JTF-CS): A standing joint task force assigned to U.S. Northern Command, that provides command and control over DoD forces in support of a Lead Federal Agency, for managing the consequences of weapons of mass destruction incident in the United States, its territories, and possessions. When directed, for a WMD incident, the Defense Coordinating Office and Defense Coordinating Element serve as a special staff augmenting the JTF-CS. Located in Norfolk, VA

Radiological Assessment Medical Team (RAMT): Specially trained in radiological health matters, this team can provide assistance and guidance to the on-scene Crisis Response Task Force (CRTF) and local medical authorities. The RAMT assists and furnishes radiological health hazard guidance to the on-scene commander or other responsible officials at an accident site, and the installation medical authority.

Army Materiel Command (AMC) Treaty Laboratory: The AMC Treaty Laboratory provides an on-site analytical laboratory capability. The lab is capable of analyzing chemical surety materials, foreign chemical warfare agents, and all precursors and degradation by-products.

U.S. Army Medical Command (MEDCOM): MEDCOM provides support to the C/B-RRT in the form of Medical Chemical and Biological Advisory Teams (MCBAT).

Medical Chemical-Biological Advisory Teams (MCBATS) (USAMRICD): USAMRICD and USAMRIID regularly contribute members to which in turn become parts of larger teams, which are run by other organizations. These teams are force-tailored and threat-driven. That is, the organization which puts the teams together decide whether or not to ask USAMRICD and/or USAMRIID to participate depending on the nature of the threat or the actual event. This structure not only for real events but also regularly for participation in exercises. USAMRICD personnel supporting MCBATs come from the Chemical Casualty Care Division and are ordinarily either physicians or nurses.

52nd Ordnance Group: This group provides Explosive Ordnance Disposal (EOD) support to incidents involving nuclear, chemical, biological, or high technology devices and is the primary agency for access and disablement operations. The 52nd Ordnance Group (EOD) jointly develops, with the Department of Energy (DOE), the disablement plan and subsequently implements the approved disablement option. The group is deployable on short-notice.

US Army Reserve Chemical Companies (Dual Purpose): Twenty-five US Army Reserve company sized units that have been specially trained and equipped to conduct nuclear, biological, and chemical personnel and casualty decontamination in support of the incident commander or lead federal agency. Units are spread throughout the nation.

US Army Reserve Chemical Companies (Reconnaissance): 3 US Army Reserve company sized units that have been specially trained and equipped to conduct nuclear, biological, and chemical reconnaissance support to include contamination surveys, agent/material sampling, and assistance with casualty search and extraction in support of the incident commander or lead federal agency. Units are located in Little Rock, AR, Arden Hills, MN, and Richmond, VA.

Aero Medical Isolation Team (AIT), USAMRIID: Maintains personnel, skills and equipment necessary to provide aero medical isolation and transport of patients infected with extremely dangerous organisms. The AIT is a rapid response unit that can deploy to any area of the world to transport and provide patient care under high containment.

Joint Task Force Consequence Management (JTF-CM): 1st and 5th US Armies. JTF-CMs deploy in support of the Lead Federal Agencies providing operational control over all committed DoD elements (less Joint Special Operations Forces Task Force and the Army Corps Of Engineers. Establishes a fully functional JTF command post in the vicinity of the incident within 24 hours of notification. Conducts 24 hour operations and provides liaison officers to appropriate civil agencies.

US Army, Technical Escort Unit (TEU): Subordinate element of the U.S. Army Soldier and Biological Chemical Command (SBCCOM). Capable of responding to a threat of or an actual incident involving chemical or biological agents or materials. Maintains a 24-hour, on-call, worldwide deployable alert team consisting of chemical, biological, and explosive ordnance disposal specialists. Capability includes render safe procedures, damage limitation, reconnaissance, recovery, sampling, mitigation, decontamination, transportation, and performance of, or recommendation of final disposition of weaponized and non-weaponized C/B materials and hazards encountered. Headquartered at Aberdeen Proving Grounds (Edgewood area), with detachments at Pine Bluff Arsenal, AR, and Dugway Proving Grounds, UT.

US Army Medical Research Institute of Infectious Diseases (USAMRIID): Conducts research to develop strategies, products, information, procedures and training programs for medical defense against biological warfare threats and infectious diseases. Develop products, such as vaccines, drugs, diagnostic tests, and medical management procedures, to protect military personnel against biological attack or against endemic infectious diseases. Serve as the DoD reference center for identification of biological agents from clinical specimens and other sources. USAMRIID has many capabilities, which can be employed for assessing and evaluating a biological terrorist incident, from initial communication of the threat through incident resolution.

Weapons of Mass Destruction Civil Support Teams (WMD CST): The National Guard WMD CST will deploy to an area of operations to perform three primary missions: assess a suspected chemical, biological, radiological, or nuclear (CBRN) event in support of a local Incident Commander, advise civilian responders regarding appropriate action, and facilitate requests for assistance to expedite arrival of additional state assets. WMD CSTs are normally part of the state response and operate under the control of the state governor; however they can be federalized, if required, and would then operate under the control of the JTF-CS.

US Army Radiological Control (RADCON) Team: Provides expert health physics (radiation control and safety) assistance to the Crisis Response Task Force (CRTF). The Team can provide support to site characterization (ground and air monitoring) and maintains a mobile radiological analysis capability.

Air Force Radiation Assessment Team (AFRAT): A deployable team of health physicists, technicians and equipment, AFRAT provides radioisotope analysis, radiation protection, and consulting support. AFRAT provides assistance worldwide for on-site detection, identification, and quantification of any ionizing radiation hazard.

Air Force Technical Application Center (AFTAC): Sole DOD agency operating and maintaining a global network of nuclear event detection sensors, the US Atomic Energy Detection System (USAEDS). Once the USAEDS senses a disturbing event underground, underwater, in space, or in the atmosphere, AFTAC's experts analyze the event for nuclear identification and report the findings to the national command authorities through Headquarters, Air Force. AFTAC provides post-detonation plume trajectory prediction, meteorological modeling, complete plume analysis/characterization, and leading edge technology dealing with chemical/ biological counter proliferation.

Navy Environmental and Preventive Medicine Units (NEPMU): The NEPMU provides chemical, biological, radiological, and environmental defense response teams (CBRED) to advise CB-RRT medical assets.

U.S. Marine Forces Atlantic (MARFORLANT) Chemical-Biological Incident Response Force (CBIRF): Subordinate element of the U.S. Joint Forces Command (USJFCOM). Capable of responding to a threat of or an actual accident or incident involving chemical or biological agents or materials. Capabilities include agent detection/identification, C/B sampling, hazard area identification, downwind hazard area identification, personnel/equipment decontamination, triage and emergency medical treatment, epidemiological investigation, site security, and evacuation/rescue. The Naval Medical Research Center augments the CBIRF. Headquartered at Indian Head, MD. CBIRF is a 350 personnel unit consisting of headquarters, C/B, medical, security, and service support elements.

Defense Technical Response Group (DTRG): Part of the Naval EOD Technical Division (NAVEODTECHDIV), is a joint-service manager for explosive ordnance disposal. DTRG provides on-site operational and technical support, personnel, equipment, and technology (R&D) to DOE and DOD units. DTRG also provides support to military EOD technicians in the field at all command levels. Primary duties include providing safe access routes to suspected weapons of mass destruction, training, and liaison support to other agencies.

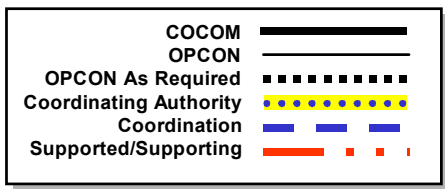
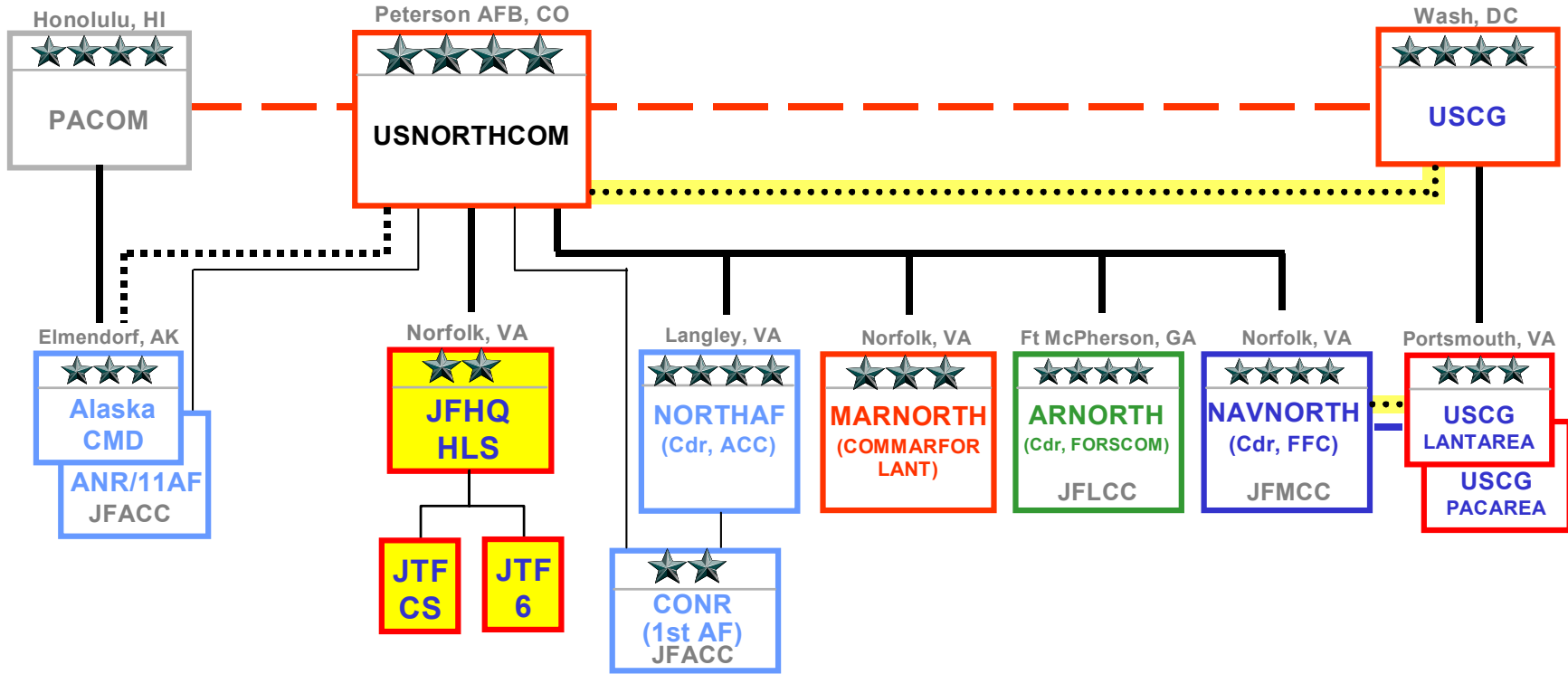
Radiological Control Team (RADCON) : The Navy's RADCON Team serves as a technical support center for radiological incidents involving nuclear weapons incidents/accidents and provides expert health physics (radiation control and safety) assistance. The Radiological Affairs Support Office (RASO) serves as the Navy's Technical Support Center for radiation sources involving industrial gamma radiography, low- and mid-level radioactive waste, base closure and site remediation, radiological surveys, and training of Navy Radiation Safety Officers. The staff is composed of highly skilled physicists (Ph.D. level) capable of providing reach-back technical assistance or the ability to field very limited number (2 or 3) of physicists to serve as advisors, supervisors, or trainers. RASO also possess a wide array of state-of-the-art gamma ray spectroscopy with sodium iodide and high purity germanium detectors and survey instruments for laboratory and field utilization.

Naval Medical Research Center (NMRC): Conducts a Biological Defense Research Program (BDRP) for research and development of agents and field deployable handheld screening assays and complementary confirmatory identification assays for the detection of biological warfare agents in clinical

and environmental samples. The Biological Defense Research Directorate (BDRD) has formed a scientific research program for the development and production of a forward deployable laboratory, which provides a rapid biological threat detection capability. The field lab can be ready to deploy within four hours of notification. The Field lab components are located at NMRC, Silver Spring, MD.

APPENDIX Q—NORTHCOM COMMAND RELATIONSHIPS

Execution Construct at IOC



- Cdr, FORSCOM designated as the Army Service Component Commander (ASCC) to NORTHCOM as ARNORTH
- Cdr, ACC designated as the AFSCC to NORTHCOM as NORTHAF
- Cdr, FFC designated as the NSCC to NORTHCOM as NAVNORTH
- Cdr, MARFORLANT assigned to NORTHCOM as COMMARFORNORTH

SOURCE: U.S. Northern Command, from the presentation "United States Northern Command," to the Joint Collaborative Analysis Conference, October 16-18, 2002

APPENDIX R—LIST OF ABBREVIATIONS

2-PAM (Pralidoxime chloride)
AAR (After Action Review)
ACE (Academy of Counter-Terrorist Education)
ACLU (American Civil Liberties Union)
AFIP (Armed Forces Institute of Pathology)
AG (U.S. Attorney General)
AHA (American Hospital Association)
AHRQ (Agency for Healthcare Research and Quality)
AMA (American Medical Association)
ANA (American Nurses Association)
APHIS (Animal Plant Health Inspection Services)
APHL (Association of Public Health Laboratories)
APPLE (Area Police Private Sector Liaison)
AQI (Agricultural Quarantine Inspection)
ARNORTH (Army North)
ASD (Assistant Secretary of Defense)
ASG (Abu Sayyef Group)
ASTHO (Association of State and Territorial Health Officials)
ATF (Bureau of Alcohol, Tobacco, and Firearms)
ATTF (U.S. Attorneys Anti-Terrorism Task Forces)
AVMA (American Veterinary Medical Association)
AVMF (American Veterinary Medical Foundation)
BLS (Bureau of Labor Statistics)
BSL (Bio-Safety Level)
BW (Biological Weapons)
CATIC (California Terrorism Information Center)
CBRN (Chemical, Biological, Radiological, Nuclear)
CBRNE (Chemical, Biological, Radiological, Nuclear, and high Explosive)
CDC (Centers for Disease Control and Prevention)
CDP (Center for Domestic Preparedness)
CERT (Community Emergency Response Teams)
CIA (Central Intelligence Agency)
CIAO (Critical Infrastructure Assurance Office)

CIIP (Critical Information Infrastructure Protection)
CIP (Critical Infrastructure Protection)
CNN (Cable News Network)
COCOM (Combatant Command)
CWAN (Cyber Warning and Alert Network)
DCI (Director of Central Intelligence)
DHHS (U.S. Department of Health and Human Services)
DHS (U.S. Department of Homeland Security)
DIA (Defense Intelligence Agency)
DMAT (Disaster Medical Assistance Teams)
DoC (Department of Commerce)
DoD (Department of Defense)
DOE (Department of Energy)
DOJ (Department of Justice)
DoL (Department of Labor)
DOMS (Director of Military Support)
DOT (Department of Transportation)
EMAC (Emergency Management Assistance Compact)
EMERS (Emergency Management Exercise Reporting System)
EMI (Emergency Management Institute)
EMRTC (Energetic Materials Research and Testing Center)
EMS (Emergency Medical Services)
EMT (Emergency Medical Technician)
EOC (Emergency Operations Center)
EPA (Environmental Protection Agency)
EPCRA (Emergency Planning and Community Right-to-Know Act)
Epi-X (Epidemic Information Exchange)
ESA (Emergency Supplemental Appropriations)
ESF (Emergency Support Function)
ETA (Basque Fatherland and Freedom)
FAA (Federal Aviation Administration)
FAD (Foreign Animal Disease)
FAO (Food and Agricultural Organization)
FBI (Federal Bureau of Investigation)

FCC (Federal Communications Commission)
FDA (Food and Drug Administration)
FEMA (Federal Emergency Management Agency)
FFRDC (Federally Funded Research and Development Center)
FISA (Foreign Intelligence Surveillance Act)
FISC (Foreign Intelligence Surveillance Court)
FMD (Foot and Mouth Disease)
FOIA (Freedom of Information Act)
FSIS (Food Safety and Inspection Service)
FTE (Full Time Equivalent)
FWMDPPS (Federal Weapons of Mass Destruction Preparedness Programs)
GAO (U. S. General Accounting Office)
GDP (Gross Domestic Product)
HACCP (Hazard Analysis and Critical Control Points)
HAN (Health Alert Network)
HAZMAT (Hazardous Material)
HEICS (Health Emergency Incident Command System)
HIPAA (Health Insurance Portability and Accountability Act)
HRSA (Health Resources and Services Administration)
HSTF (Homeland Security Task Force)
HUM (Harakat ul-Mujahedin)
HUM-A (Harakat ul-Mujahedin al-Alami)
I3C (Institute for Information Infrastructure Protection)
IC (Intelligence Community)
ICS (Incident Command System)
IMU (Islamic Movement of Uzbekistan)
INS (U.S. Immigration and Naturalization Service)
ISP (Internet Service Providers)
JCAHO (Joint Committee on Accreditation of Healthcare Organizations)
JFCOM (Joint Forces Command)
JFHQ-HLS (Joint Force Headquarters Homeland Security)
JI (Jemaah Islamiya)
JTF-6 (Joint Task Force 6)
JTF-CS (Joint Task Force Civil Support)

JTTF (Joint Terrorism Task Forces)
KMM (Kumpulan Mujahidin Malaysia)
LFA (Lead Federal Agency)
LRN (Laboratory Response Network)
MARFOR NORTH (Marine Forces North)
MASINT (Measurement and Signature Intelligence)
MILF (Moro Islamic Liberation Front)
MMRS (Metropolitan Medical Response System)
MOU (Memorandum of Understanding)
MRC (Medical Reserve Corps)
NACCHO (National Association of City and County Health Officials)
NASA (National Aeronautics and Space Administration)
NAVNORTH (Navy North)
NBC (Nuclear, Biological, Chemical)
NCTC (National Counter Terrorism Center)
NDMS (National Disaster Medical System)
NDPC (National Domestic Preparedness Consortium)
NEDSS (National Electronic Data Surveillance System)
NFA (National Fire Academy)
NIAID (National Institute of Allergy and Infectious Diseases)
NIH (National Institute of Health)
NIOSH (National Institute for Occupational Safety and Health)
NIPC (National Infrastructure Protection Center)
NISAC (National Infrastructure Simulation and Analysis Center)
NIST (National Institute for Standards and Technology)
NNRT (National Nurses Response Teams)
NOAA (National Oceanic and Atmospheric Administration)
NORAD (North American Aerospace Defense Command)
NORTHAF (North Air Force)
NORTHCOM (U.S. Northern Command)
NPRT (National Pharmacy Emergency Response Teams)
NPS (National Pharmaceutical Stockpile)
NRC (Nuclear Regulatory Commission)
NSA (National Security Agency)

NSC (National Security Council)
NTS (Nevada Test Site)
NTSB (National Transportation Safety Board)
NYCDOH (New York City Department of Health)
OCPM (Office of Crisis Planning and Management)
ODP (Office of Domestic Preparedness)
OEM (Office of Emergency Management)
OEP (Office of Emergency Preparedness)
OHS (White House Office of Homeland Security)
OIPR (Office of Intelligence Policy and Review)
OJP (Office of Justice Programs)
OMB (Office of Management and Budget)
ONP (Office of National Preparedness)
OPHEP (Office of Public Health Emergency Preparedness)
OSHA (Occupational Safety and Health Administration)
PAPR (Powered Air-Purifying Respirator)
PCIPB (President's Critical Infrastructure Protection Board)
PDD (Presidential Decision Directive)
PIJ (Palestinian Islamic Jihad)
PIRA (Provisional Irish Republic Army)
PLO (Palestine Liberation Organization)
POC (Point of Contact)
PPE (Personal Protective Equipment)
RDT&E (Research, Development, Test, and Evaluation)
RSA (Republic of South Africa)
SAD (State Active Duty)
SAMHSA (Substance Abuse and Mental Health Services Administration)
SARA (Superfund Amendments and Reauthorization Act)
SCADA (Supervisory Control And Data Acquisition)
SCBA (Self Contained Breathing Apparatus)
SME (Subject Matter Expertise)
SOLIC (Special Operations/Low Intensity Conflict)
SRG (Survey Research Group)
TEEX (Texas Engineering Extension Service)

TIPS (Terrorism Information and Prevention System)
TSA (U.S. Transportation Security Administration)
USAHA (United States Animal Health Association)
USC (United States Code)
USCG (U.S. Coast Guard)
USCS (U.S. Customs Service)
USDA (United States Department of Agriculture)
USFS (U.S. Forest Service)
USPHs (U.S. Public Health Service)
VMAT (Veterinary Medical Assistance Teams)
WHO (World Health Organization)
WMD (Weapons of Mass Destruction)
WMDCST (Weapons of Mass Destruction Civil Support Team)
WTC (World Trade Center)

APPENDIX S—PANEL ACTIVITIES—CALENDAR YEAR 2002

During the past year, the panel held five formal meetings:

April 11-12, 2002, U.S. Capitol, Washington, DC
June 17-18, 2002, Indiana State Office Complex, Indianapolis
September 12-13, 2002, RAND Washington Office, Arlington, VA
September 30, 2002, The Pentagon, Washington, DC
November 7-8, 2002, RAND Washington Office, Arlington, VA

During the course of those meetings, panel members received presentations or engaged in categorical discussions as follows:

Congressman Curt Weldon - Congressional activities and priorities for homeland security

Chuck Ludlam, Staff of Senator Joseph Lieberman's – Potential legislative proposals for medical response

Brendan Shields, House Republican Conference Staff – On the new Homeland Security Coordination Group of the Conference

Congressman Saxbe Chambliss - Update on House Permanent Select Committee on Intelligence subcommittee on combating terrorism, and other Congressional issues

Congresswoman Jane Harman - Update on House Permanent Select Committee on Intelligence subcommittee on combating terrorism, and other Congressional issues

Dale Watson, Federal Bureau of Investigation – FBI organizational and mission restructuring (Classified)

Will Chapleau, National Association of Emergency Medical Technicians - On the need for financial support for emergency medical responders

John Buchman, President, International Association of Fire Chiefs - On the need for financial support for local responders

Peter Beering, City of Indianapolis - On the lack of communication between the government and the private sector

Trina Hembree, National Emergency Management Association - On the need for a formal process of intelligence sharing and a common incident command center

Steven Charvat, International Association of Emergency Managers - On the need for local, state, regional and federal levels to use the incident command system

Patrick Sullivan, National Sheriffs Association - On the need to improve information sharing

Stephanie Osborn, National Association of Counties - On the role counties play in health preparedness and the need for additional resources

Tom Hanify, President, International Association of Fire Fighters - On the need for more personnel, training, and equipment to fight potential terror attacks

Ron Olin, International Association of Chiefs of Police - On the general lack of communication and information sharing and the lack of funding

Bill Webb, Congressional Fire Services Institute – On the proposal to expand the fire grant program instead of creating new ones

John Parachini, RAND Support Staff – Threat Update Briefing

Linda S. Millis, Business Executives for National Security - “New Tools, New Teams for New Threats” - On the lack of information available to the private sector to protect themselves and their facilities.

Steve Jordan, U.S. Chamber of Commerce - On the need for better private sector awareness, adoption of secure practices, reconciliation of economic and security issues, information sharing, technology change, and human behavior

Sam Bozzette, RAND Support Staff - On medical responses including vaccination and isolation techniques of protecting against a bio-terrorist incident

Lieutenant Colonel Jerry Walsh – Office of the Secretary of Defense - On the roles and missions of U.S. Northern Command

Tom Kuster – Office of the Secretary of Defense - On the use of special forces inside the United States (partially classified)

Robert Mueller, Director, Federal Bureau of Investigation - Classified discussion on FBI intelligence activities

Ted Macklin and Corey Gruber, Office of Domestic Preparedness, Department of Justice – Briefing on TOPOFF II

Under the provisions of the Federal Advisory Committee Act, meetings of the panel are generally open to the public, except when national security classified information is being presented or discussed, or for one of the other exceptions stated in the Act. Notices of meetings are published in the Federal Register and posted on the panel’s web page on the RAND web site, <http://www.rand.org>. Unclassified minutes of the panel meetings are posted to the same web page as soon as the panel has approved them.

Panel members and support staff also attended and participated directly in numerous conferences, workshops, and symposia on the subject of terrorism. In addition, panel members and staff attended numerous Congressional hearings on terrorism and presented testimony when requested and appropriate.

APPENDIX T—RAND STAFF PROVIDING SUPPORT TO THE ADVISORY PANEL

Executive Project Director

Michael Wermuth

Co-Project Director

Jennifer Brower

Research Staff for the Report

Donna Barbisch	Can Du	Renee Labor	Negeen Pegahi
Gabrielle Bloom	David Eisenman	Michael Lostumbo	William Rosenau
David Brannan	Ron Fricker	Nicole Lurie	Kevin Jack Riley
Robert Button	Barbara Genovese	Scott McMahan	Paul Steinberg
Gary Cecchine	Bruce Hoffman	Charles Meade	Suzanne Spaulding
Peter Chalk	Gerald Jacobsen	Roger Molander	Michael Stoto
Kim Cragin	Brian Jenkins	Sarah Myers	Terri Tanielian
Lois Davis	Seth Jones	Sarah Cotton Nelson	Jeffrey Wasserman
Linda Demaine	David Kassing	Jennifer Pace	Barbara Wynn
Bruce Don	Terrence Kelly	John Parachini	

Administrative Support

Nancy Rizor	Michael DuVal	Sandra Hanson	Christel Chichester
-------------	---------------	---------------	---------------------

Other RAND Staff Providing Support

Kimberly Alldredge	Tamara Hemphill	Phillip Mazzocco	Diana Thornton
Dorothy Chen	Risha Henneman	Kathy Mills	Sandra Wade-Grusky
Molly Coleman	Candace Hoffman	Hillary Peck	Deanna Webber
Karen Echeverri	Peter Hoffman	Carolyn Rogers	Elwood Whitaker
David Feliciano	Emily King	Amy Rudibaugh	Patricia Williams
Leanna Ferguson	Jessica Kmiec	Toya Russell	Ralda Williams
Hunter Granger	Barbara Lacy	Jane Ryan	Angie Wyatt
Tyrone Greene	Lee Meyer	Dan Sheehan	Natalie Ziegler

RAND Corporate Leadership for the Project

Jeffrey Isaacson, Vice President, National Security Research Division, and Director, National Defense Research Institute (NDRI)

Susan Everingham, Director, Forces and Resources Policy Center (NDRI)

James Dobbins, Director, International Security and Defense Policy Center (NDRI)

LIST OF KEY RECOMMENDATIONS

Organizing the National Effort

- Establish a National Counter Terrorism Center (NCTC)
- Transfer the collection of intelligence inside the United States to the NCTC
- Concentrate oversight of the NCTC in the intelligence committee in each House
- Produce continuing, comprehensive “strategic” assessments of threats inside the United States
- Ensure DHS authority to levy direct intelligence requirements, and robust DHS capability for combining threat and vulnerability information
- Clearly define DHS and other Federal agency responsibilities before, during, and after an attack
- Designate DHS as lead, and DHHS as principal supporting agency, for bioterrorism attack
- Perform a comprehensive National Intelligence Estimate on the threats to infrastructure
- Restructure interagency mechanisms for better coordination
- Thoroughly review applicable law and regulations; propose legislative changes
- Establish separate Congressional authorizing committee and appropriation subcommittee for homeland security

Improving Health and Medical Capabilities

- Strengthen the public health system with support on the order of \$1 billion per year for 5 years
- Coordinate and centralize funding information from various agencies and simplify the application process
- Implement a formal process for evaluating the effectiveness of investments in preparedness
- Funds studies on health care and public health workforce requirements
- Assess the resources required by the nation’s hospital system to respond to terrorism
- Strengthen the Health Alert Network and other secure and rapid communications systems
- Increase resources for public health and medical emergencies
- Articulate and integrate the roles, missions, capabilities and limitations of, and effectively train special response teams
- Improve system for providing required technical assistance to States and localities
- Develop an electronic, continuously updated handbook on best terrorism response practices
- Strengthen and prioritize basic medical and applied public health research
- Adopt the Model Health Powers Emergency Act or develop adopt alternative
- Clarify the special conditions under which HIPAA information can be shared;and require State plans for enhanced cooperation between law enforcement and public health, EMS and hospital officials
- Education the public on health and medical information before, during and after an event
- Enhance research into the short and long-term psychological consequences of terrorist attacks
- Improve capacity in the Intelligence Community for health and medical analysis
- Enhance technical assistance to states to develop plans and procedures for distributing the NPS
- Establish a national strategy for vaccine development
- Implement the smallpox vaccination plan incrementally; and raise the priority on research for a safer smallpox vaccine

Defending Against Agricultural Terrorism

- Perform a National Intelligence Estimate on the threat to agriculture and food
- Include an Emergency Support Function for Agriculture and Food in the Federal Response Plan and the National Incident Response Plan
- Allow specially designated laboratories to perform tests for foreign agricultural diseases
- Institute a standard system for fair compensation for agriculture and food losses
- Improve and provide incentives for veterinary medicine education in foreign animal diseases; and improve education, training, and exercises between government and the agricultural private sector

LIST OF KEY RECOMMENDATIONS (CONTINUED)

Improving the Protection of Our Critical Infrastructure

- Establish an Independent Commission to suggest strategies for critical infrastructure protection
- Conduct a National Intelligence Estimate on threats to critical infrastructure
- Elevate the priority of measures for baggage and cargo screening on passenger aircraft
- Develop comprehensive guidelines for improving the security of general aviation
- Establish regulations for more effective security of dam facilities
- Merge physical and cyber security policy development into a single entity in the White House
- Use NISAC's capabilities to develop metrics for describing infrastructure security

Use of the Military

- Clarify the NORTHCOM mission to ensure plans across a full spectrum of activities
- Ensure NORTHCOM commander has operational control of all Federal military forces in AOR
- Review and amend statutes so that authorities and safeguards exist for use of the military domestically; and prepare a legal "handbook" on use of the military domestically for civilian and military leaders
- Develop a comprehensive requirements identification process for use of the military for civil support
- Direct that all military personnel who may serve under NORTHCOM receive special training for domestic missions
- Clarify NORTHCOM to ensure pre-incident planning, training, and for civil support missions
- Establish NORTHCOM dedicated, rapid-reaction units with a wide range of response capabilities
- Provide funds for National Guard civil support planning, training, exercising and operations
- Establish a collaborative process for deploying National Guard forces in Title 32 duty status; provide new authority under Title 32 to employ the National Guard on a multi-State basis; and support a system for National Guard civil support missions regionally
- Assign and train certain National Guard units exclusively for homeland security missions

