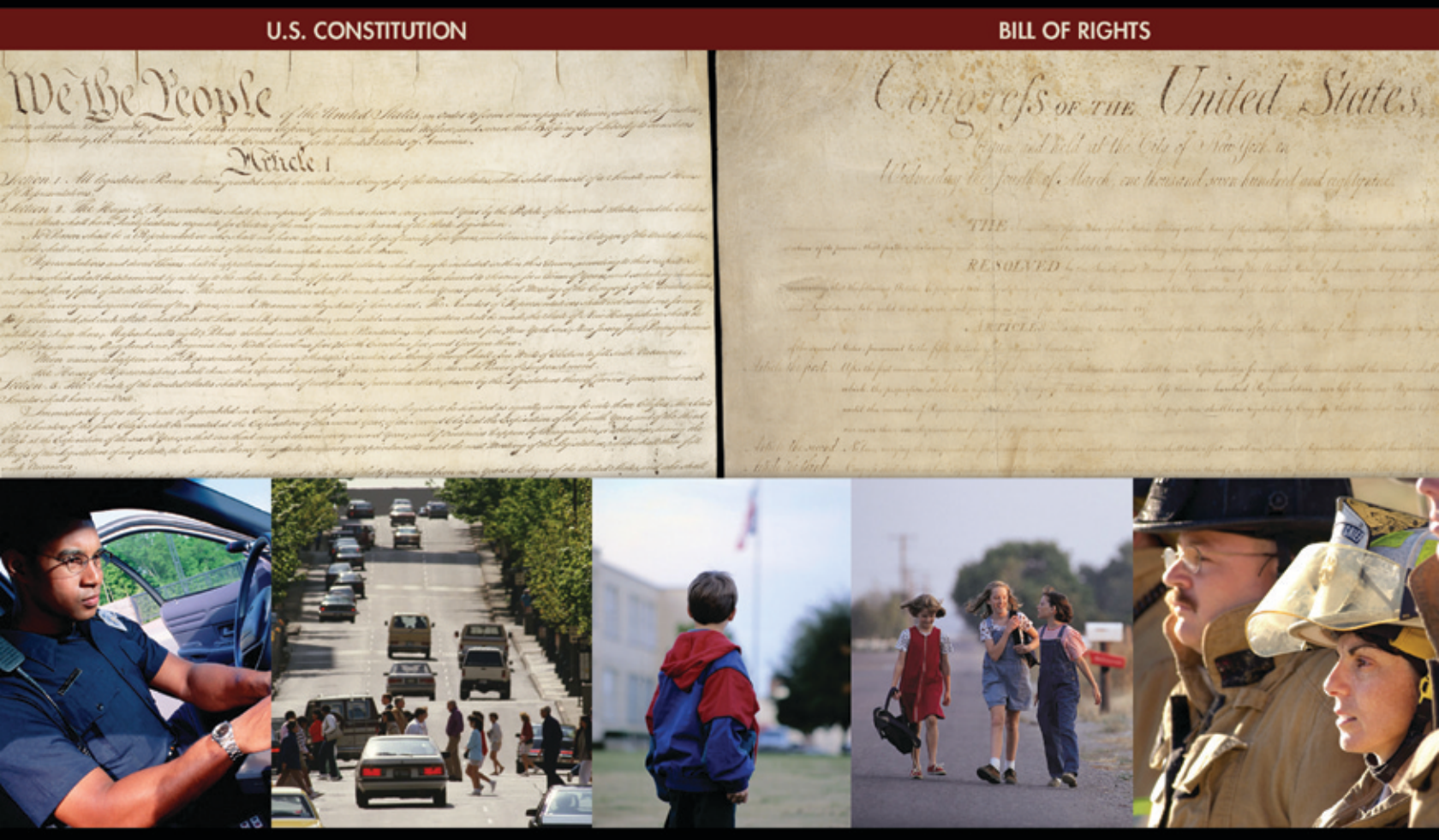
★ 15 December 2003 ★

V. Forging America's New Normalcy



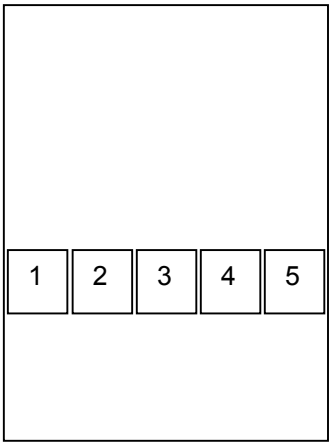
Securing Our Homeland, Protecting Our Liberty

The Fifth 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 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), as amended. 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 Fifth 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

PHOTO CREDITS FROM FRONT COVER



1—Policeman entering data into an enhanced communications terminal. Photo from Thinkstock
2—A typical American street scene. Photo from Photodisc
3—Admiring our national colors. Photo by David Buffington
4—Walking home from the school bus stop with friends. Photo by Mark Andersen
5—Firefighters, always vigilant. Photo from Thinkstock

Images of the U.S. Constitution and the Bill of Rights from the U.S. Archives

Cover design by Stephen Bloodsworth

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

December 15, 2003

To Our Readers:

We deliver this *Annual Report*, our fifth and final, impelled by the urgency that America succeed in its efforts to secure the homeland and sustain our national values. In households and communities, State capitols and our nation's capitol, in the workrooms and boardrooms of businesses, and on the battlefield, America seeks its destiny in the post 9-11 era.

A little over 27 months ago, our nation was viciously attacked. Our enemies sought to undermine the resolve and indomitable spirit that have been the cornerstone of the United States since its founding. They failed. Today, we remain a nation united in a common purpose. We are committed to a global effort to defeat terrorism. We are committed to a national effort to make America safer and more secure.

For 227 years the United States has followed the path established by our founding fathers. They provided us the roadmap. Generations since have navigated the journey, always mindful of where and why it began. It has not been easy—requiring sweat, intellect, and sacrifice. Americans have consistently met the challenges to fulfill, and not change, the vision of those who gave birth to our nation.

America must not waver from the guiding principles established at its birth while simultaneously crafting and executing a national approach that counters the threats posed by terrorists. Progress is being made. *The Panel wishes to be clear, however, that it believes there is more to be done and soon.* Homeland security strategies—whether developed by individuals, governments, or the private sector—are a beginning. But general strategies must be turned into specific roadmaps to direct local, State, Federal, and private sector actions. Turning vision into reality will require sustained commitment of human and financial capital over the longer term. It will require disciplined and consistent approaches balanced against mid-course adjustments when necessitated by real versus perceived shortcomings.

The nation faces tangible dangers that demand our attention, and our response must rise above anyone's or any group's agenda. In our five years of service, panel members have observed the ebb and flow of national efforts. We have watched since September 11th the overwhelming desire for the nation to achieve some level of normalcy. It is our opinion, buoyed by fact and instinct, that we can forge a new normalcy that sustains the principles set forth by our founding fathers, while mindful that the threat requires some level of adjustment in our lives. We are convinced that, in forging America's new normalcy, our nation will be better and stronger.

Please address comments or questions to:
The RAND Corporation
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

In this final year of service, our members have attempted to look beyond the crisis of the moment with a view toward the future. The Panel has offered 144 recommendations since its inception; 125 have been adopted and are being implemented in whole or part. Many of these recommendations were made prior to the 2001 attacks. We remain resolute in our belief that securing the homeland and preserving our national values requires a two-pronged effort. Action must be taken to achieve the goals already set forth. Equally important is deliberately looking at the entire national enterprise of readiness to determine what work remains. All of this must be done in strict observance of our national values *of individual freedom.*

There will never be an end point in America's readiness. Enemies will change tactics, citizen's attitudes about what adjustments in their lives they are willing to accept will evolve, and leaders will be confronted with legitimate competing priorities that will demand attention. These are simply characteristics of our society that must be factored into our national efforts. In the end, America's response to the threat of terrorism will be measured in how we manage the risk. There will never be a 100% guarantee of security for our people, the economy, and our society. We must resist the urge to seek total security—it is not achievable and drains our attention from those things that can be accomplished.

Managing the risk requires a continuum not subject to the ebb and flow that characterizes many of our national priorities. Assessing threats and applying an acceptable level of resources to minimize vulnerabilities cannot occur *only* in the aftermath of an attack. It must become the steady state. This does not imply that America will have to remain at a heightened threat level. Rather the goal is to create an environment where current fears of terrorism are ameliorated by a future confidence derived from knowing that the nation is better prepared to counter the terrorist threat. This confidence, engendered through informed awareness for our citizens, will give the nation the tools necessary to adjust to the full range of 21st Century risks.

Our new normalcy will involve better management of risks, ahead of time, of terrorism, naturally occurring diseases, and natural or technological disasters. All levels of government, the private sector, and our citizens must each do their part. Better managing our risks will lead to a safer and more secure America. It will allow us to return to a level of normalcy, albeit one somewhat different than prior to the 2001attacks. Our enemies want us to be controlled by fear. Our panel members are confident the nation can instead control the fear and rob the enemy of their key strategy for undermining our national values.

Together with others, we believe our work has contributed to the national debate and has been instrumental in advancing the homeland security dialogue beyond the Washington Beltway. We have accomplished the goals set forth nearly five years ago through the dedicated efforts of a group of Americans representing all levels of government and the private sector. Over five years we were able to *look ahead*, unconstrained by the crisis of the moment, at what was needed to advance the safety and security of the nation. Our findings have been reflected in our work and in the measurable advances of the United States in the aftermath of the evil and tragic attacks of 2001. We also believe that these attributes—a

national approach, forward-looking, and based on measurable results—must be the cornerstones to our continuing efforts to secure our hometowns and the homeland.

I am particularly appreciative of the exceptional Americans who have served on this panel during the past five years. None was more important than another and each has brought an unsurpassed level of commitment and dedication to our work. Throughout this project the RAND Corporation has provided invaluable support to the panel, especially the co-project directors Michael Wermuth and Jennifer Brower. I am honored to have had the opportunity to work with my fellow panel members, the RAND staff, and the many other fine Americans who have worked tirelessly to help us complete our tasks. Their efforts have made America stronger and more secure.

We complete our work with a great sense of pride. Most important, we thank the many individuals who have informed our work during the past five years. We have produced a series of reports that are not the work of a few, but rather the commitment of many. In this work is the hope and desire of every American for a more secure homeland that preserves our liberty for all time.

Sincerely,

James S. Gilmore, III
Chairman

CONTENTS

PREFACE

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 1999, Public Law 105-261 (H.R. 3616, 105th Congress, 2nd Section, October 17, 1998). The panel was directed to submit, beginning in December 1999, three annual reports to the President and the Congress assessing how well the Federal government was supporting State and local efforts to combat catastrophic terrorism. The panel was also charged to recommend strategies for ensuring fully effective local response capabilities. As a result of the attacks on September 11, 2001, the Congress extended the panel's charter with the requirement to submit two additional annual reports on December 15 of 2002 and 2003, respectively.

Because of the inextricable relationships between all components of the nation's efforts to counter the risks of terrorism—awareness, prevention, preparedness, response, and recovery—the panel felt it was critically important to look more broadly at all Federal support for combating terrorism. Thus, its work has reflected comprehensive analyses and recommendations across the full spectrum of efforts to combat terrorism.

This document represents the fifth and final report of the panel. The strategic vision, themes, and recommendations of the *Fifth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* were motivated by the unanimous view of the panel that this report should attempt to define a future state of security against terrorism—one that the panel has chosen to call "America's New Normalcy."

In developing this year's report, panel members all agreed at the outset that it could not postulate, as part of its vision, a return to a pre-September 11 "normal." The threats from terrorism are now recognized to be a condition that we must face far into the future. It is our firm intention to articulate a vision of the future that subjects terrorism to a logical place in the array of threats from other sources that the American people face every day— from natural diseases and other illnesses, to crime, and traffic and other accidents, to mention a few. The panel firmly believes that terrorism must be put in the context of the other risks that we face, and that resources should be prioritized and allocated to that variety of risks in logical fashion.

To accomplish that purpose, this report integrates and synthesizes both the earlier work of the panel, continuing extensive supporting research and analysis from RAND, and the experience and efforts of the country as a whole in the period before and since September 11—within governments at the local, State, and Federal level, in the private sector, and for the public at large. This report attempts to project a future—five year—equilibrium state of well-established and sustained measures to combat terrorism. It focuses on conceptualizing a *strategic vision* for the Nation that, in the future, has achieved in both appearance and reality an acceptable level of awareness, prevention, preparedness, response and recovery capabilities to cope with the uncertain and ambiguous threat of terrorism as part of dealing with all hazards. The report also makes specific findings and recommendations on process and structure that must be addressed to move from general strategies into specific accomplishments.

This report builds on almost five years of work by the panel. Initially the panel looked closely at the terrorist threat facing the nation, reflecting the view that it is impossible to know if we are prepared without understanding what we are preparing for. In the first report, the panel recommended a comprehensive national strategy for combating terrorism. That recommendation remains a cornerstone of the panel's philosophy and is underscored by the belief that a national strategy is not a simply a Federal strategy but rather one that integrates and synchronizes local, State, and Federal government and privates sector efforts in a true nationwide effort. In the second report, the panel recommended specific actions to improve governmental structures and processes and to develop a national strategy in a number of areas including border control and health and medical issues. In the third year, the panel made additional specific recommendations for strategies and programs for combating terrorism in several functional areas. Last year the panel readdressed the overall terrorist threat, responded with a critique of the *National Strategy for Homeland Security*, and focused additional recommendations on key areas requiring specific improvements.

At this writing, 125 of the 144 substantive recommendations made by the panel in its first four reports have been adopted in whole or in major part, in legislation, executive action, or other processes. In prior years, we have catalogued those recommendations cumulatively in the introductory material of each succeeding report. For this last report, we are providing a matrix (at Appendix K) that provides additional detail on the status of each recommendation and highlights those that have not been implemented that continue to require urgent attention.

As we have clearly stated in prior reports, this panel cannot offer all the answers or necessarily the best answers for many of the difficult challenges ahead. Nevertheless, as we bring to a close this five-year undertaking—spanning more than two years on each side of September 2001—we are confident that we have fulfilled our Congressional mandate by contributing materially and significantly to this vital national effort by helping to shape and accelerate both the national debate and improvements in capabilities.

EXECUTIVE SUMMARY

The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons on Mass Destruction was created by the Congress in 1999 to assess Federal efforts to assist State and local responders in combating terrorism. The inextricable relationships between all components of the nation's efforts—local, State, and Federal governments, the private sector, and the public at large—to counter terrorist threats caused the panel to look broadly at the issues.

In our first four annual reports to the Congress and the President, the Panel has, among its 144 recommendations, offered foundational perspectives on:

- The nature of the threat
- The need for and components of a successful national strategy
- Attributes of effective structures to guide and empower the implementation of preparedness at the local, state and federal levels, in the private sector and across all key disciplines – especially local and State responders
- America's efforts to respond to the tragic attacks of 2001 in a deliberative manner to ensure they establish a solid foundation for future efforts to build a safer and more secure America – one that will allow us to control and manage our risks more effectively
- Finally, and most importantly, the need to sustain the principles set forth by our founding fathers that preserve national values, among them important personal freedoms

The panel completes its work by establishing a benchmark to fuel future debate and action and to regain the nation's momentum to secure the homeland and preserve our liberty.

We underscore in this report that America has made advances, especially since September 11th, on many fronts. The level of awareness and initiatives already undertaken by all levels of government, the private sector, and the general population constitute an important beginning. They offer a sound foundation for the future actions that we believe we must achieve—the New Normalcy—a condition that this report describes.

Paramount to the panel's work is the vitally important need for America to secure the homeland in a manner that is consistent with and further empowers the values set forth at the birth of our nation. We believe that the current debate, characterized by a suggestion of competing values between liberty and security, is misplaced. Rather, the panel is firmly committed to the precept that they are values that—just as the founding fathers intended—must be mutually reinforcing.

The panel also notes that our readiness cannot be subject to the ebb and flow of other events or limited simply to the terrorist threat. To make additional, measurable advances built on sustained commitment of human and financial capital, intellect and sacrifice, further changes are needed. Organizational changes that have occurred represent a first step. But these cannot be viewed as the end goal. There is a compelling need for additional institutional changes that bring balance to the requirement to implement those programs and policies already identified against the need to maintain a forward-looking approach that continuously anticipates future risks and develops national strategies and approaches continuously to mitigate our vulnerabilities. Recent history has reminded the United States that the threats we face are broad—from natural disasters

to terrorism, from inside and outside our borders, and affecting not only our physical safety but our economic well being and societal stability.

The panel has proffered a view of the future—five years hence—that we believe offers a reasonable, measurable, and attainable benchmark. We believe that in the current absence of longer-term measurable goals, this benchmark can provide government at all levels, the private sector, and our citizens a future set of objectives for readiness and preparedness. We do not claim that the objectives presented in this future view are all encompassing nor necessarily reflect the full continuum of advances that America may accomplish or the successes that its enemies may realize in the next five years. It is, however, a snapshot in time for the purpose of guiding the actions of today and a roadmap for the future.

America's new normalcy in January of 2009 should reflect:

- Both the sustainment and further **empowerment of individual freedoms** in the context of measurable advances that secure the homeland.
- Consistent **commitment of resources** that improve the ability of all levels of government, the private sector and our citizens to prevent terrorist attacks and, if warranted, to respond and recover effectively to the full range of threats faced by the nation.
- A standardized and effective process for **sharing information and intelligence** among all stakeholders—one that is built on moving actionable information to the broadest possible audience rapidly, and that allows for heightened security with minimal undesirable economic and societal consequences.
- Strong **preparedness and readiness across State and local government and the private sector** with corresponding processes that provide an enterprise wide national capacity to plan, equip, train, and exercise against measurable standards.
- Clear definition about the roles, responsibilities, and **acceptable uses of the military domestically**—that strengthens the role of the National Guard and Federal Reserve Components for any domestic mission, and ensures that America's leaders will never be confronted with competing choices of using the military to respond to a domestic emergency versus the need to project our strength globally to defeat those who would seek to do us harm.
- Clear processes for engaging academia, business, all levels of government, and others in rapidly developing and implementing **research, development and standards** across technology, public policy, and other areas needed to secure the homeland—a process that focuses efforts on real versus perceived needs.
- Well-understood and shared process, plans, and incentives for **protecting the nation's critical infrastructures** of government and in the private sector—a unified approach to managing our risks.

Forging a New Normalcy will require additional changes in the way the nation develops strategy and policy, and how it focuses on moving from concept to accomplishment. These are not major structural changes. They represent changes in attitude and culture as well as processes. These are formidable changes without any doubt. But they remain critically necessary if we are going to remain one step ahead of our enemies and achieve duality of purpose in this great American investment to secure the homeland.

INTRODUCTION

Although the nation better understands the threats it faces and many of the measures necessary to counter them, the panel is concerned that the momentum, which accelerated full force following the September 11 attacks, may have been interrupted, that scarce resources may not be prioritized and applied most effectively, that fragmentation continues to hamper efforts for better coordination across all levels of government and with the private sector. Terrorist attacks worldwide are increasing in both number and lethality.[1] It is from those concerns and out of an abundance of caution that we suggest a reinvigoration and refinement of certain efforts. To do this, we suggest a strategic vision for the future and the steps necessary to move us toward that steady state.

In seeking to develop a strategic vision of the future of homeland security, the Advisory Panel has been guided by the recognition that the threat of terrorism can never be completely eliminated and that no level of resources can prevent the United States from being attacked in the future. At the same time, the panel believes that the Nation is achieving an important, critical understanding of the risks posed to America by terrorism, an understanding that derives from America's inherent strengths—the strength in our Constitutional form of government and particularly the strength of our people.

As a group of American citizens with broad experience in government at all levels and in the private sector, the panel members see in those national strengths an ability to respond to the threat of terrorism with firm resolve and through concrete actions across the full spectrum of awareness, prevention, preparedness, response, and recovery—areas already familiar to a society that has successfully responded to a wide array of natural and manmade disasters. Our goal is to articulate a strategy to achieve a "steady state" in the next five years—a vision shaped by a broad and well-grounded American perspective on the threat of terrorism and supported by a profound increase and sustainment of our preparedness *especially at the State and local levels*. Our collective actions must be focused and forward thinking to deal effectively with this ambiguous and evolving threat.

Critical to this uniquely American perspective on the threat posed by terrorism is the recognition that important civil liberties issues must be considered when evaluating measures for combating terrorism. As the President said recently when speaking about the war in Iraq, "stability cannot be purchased at the expense of liberty." That same idea is firmly rooted in the American ethos and is reflected in one of the panel's favorite quotes from Benjamin Franklin:

> They that would give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.

In times of crisis, when the pressure for dramatic change is most intense, it is helpful to return to these fundamental principles that have guided this nation since its inception. As Thomas Jefferson advised in his first inaugural address:

[1] For an overview of terrorism trends, see Appendix J.

> The essential principles of our Government form the bright constellation which has gone before us and guided our steps through an age of revolution and reformation....[S]hould we wander from them in moments of error or of alarm, let us hasten to retrace our steps and to regain the road which alone leads to peace, liberty and safety.

Because of our national tendency to react—perhaps overreact—in times of crisis, it is crucial to have a well-defined vision of homeland security and a roadmap to achieve that goal. Nevertheless, because it is human nature to relax and refocus in the absence of an obvious threat we must use the roadmap to prevent us from letting our guard down too far, regardless of the timing or characteristics of the next terrorist attack.

Imperatives for this report

As recommended in the *First and Second Annual Reports of the Advisory Panel*, the President developed and published a *National Strategy for Homeland Security*—an important first step in leading the nation forward. The Department of Homeland Security and other governmental agencies at all levels are working diligently to prevent future terrorist attacks; analyze threats and vulnerabilities; guard borders and transportation; protect critical infrastructure; and coordinate response to and recovery from such attacks when they occur. Much is still required in order to achieve an effective, comprehensive, unified national strategy and to translate vision into action. Notably absent is a clear prioritization for the use of scarce resources against a diffuse, unclear threat as part of the spectrum of threats—some significantly more common than terrorism. The panel has serious concern about the current state of homeland security efforts along the full spectrum from awareness to recovery, worried that efforts by the government may provide the perception of enhanced security that causes the nation to become complacent about the many critical actions still required.

In its previous report, the panel was hopeful that the momentum created by the attacks of 2001 would result in the comprehensive articulation and timely implementation of a national strategy. Despite an encouraging start, the momentum appears to have waned as people, businesses, and governments react to the uncertainties in combating terrorism and to the challenge of creating a unified enterprise architecture for awareness, prevention, preparedness, response, and recovery among all of the differing components. While recognizing the inherent difficulty of such a complex undertaking, we suggest that adapting to these existing obstacles between the various levels of government and the private sector requires our attention and more comprehensive forward thinking.

It is time to move beyond our traditional reactive behavior to a comprehensive process for constant forward thinking and strategic planning, one that continuously engages all stakeholders in defining and implementing the future vision. One part of our national effort must be dedicated to accomplishing what has already been defined; a second must be dedicated to defining and refining what has yet to be done. Otherwise the current efforts to enhance preparedness will be tenuous at best and subject to change after the next threat emerges or key Administration officials or Congressional leaders change.

Moreover, the fragmentation of responsibilities and capabilities within the Federal structure, among governments at all levels, and with the private sector requires our urgent attention.

Continuing fragmentation is especially dangerous when our enemies are becoming more coordinated and sophisticated in their communications and tactics. Our approach must be the development of comprehensive, collaborative approach—an *enterprise architecture*—that can handle both the actions of the moment and planning for the future.

Consistent with Congressional direction and our previous work, the panel's vision of a steady state five years in the future focuses on measures to combat terrorism as a key component of homeland security and also one that is fully consistent with an all-hazards approach. As our experience with SARS, West Nile Virus, monkeypox, the recent fires in California, and the current influenza epidemic have demonstrated vividly, we must be able to handle a wide variety of threats.

Guiding Principles

The strategic vision presented in this report reflects the firm and unanimous view of the Advisory Panel, and emerged only after deliberate, focused, often pointed debate. The panel recognizes that the United States is still in the early stages of a truly comprehensive national approach to the threat of terrorism and that there are difficult choices to be made at all levels of society, choices complicated by substantial uncertainty with respect to threats, vulnerabilities, and the future effectiveness of initiatives already undertaken. Facing these uncertainties, the concept of a strategic vision for a future state and an associated action plan seemed appropriate to these circumstances—and appropriately American. With this in mind, the strategic vision of the panel applies to all parts and all levels of society. It reflects both an assessment of what the panel believes America is capable of achieving *over the next five years* and the clear challenge to the nation to take the necessary and appropriate steps to accomplish that goal. This approach will provide a baseline from which to debate—within our governments and among the American public—difficult decisions on approaches and priorities.

The strategic vision offered here reflects the guiding principles that Panel has enumerated in its past four reports as well as those reflected in this report:

- It must be truly national in scope, not just Federal
- It should build on the existing emergency response system within an all-hazards framework
- It should be fully resourced with priorities based on risk
- It should be based on measurable performance
- It should be truly comprehensive, encompassing the full spectrum of awareness, prevention, preparedness, response, and recovery against domestic and international threats against our physical, economic and societal well being
- It should include psychological preparedness
- It should be institutionalized and sustained
- It should be responsive to requirements from and fully coordinated with State and local officials and the private sector as partners throughout the development, implementation, and sustainment process
- It should include a clear process for strategic communications and community involvement
- It must preserve civil liberties

This proffered vision presents a carefully balanced approach to the difficult question of whether to place more or less emphasis on *reducing the terrorist threat* versus *lessening American vulnerabilities* to terrorist attacks. The challenge in effective strategic planning is stark at all government levels and in the private sector. On the one hand, we face a situation where it is extremely difficult to assess the absolute magnitude and character of the present and potential terrorism threat. It is likewise difficult to develop measures of effectiveness that reflect whether the threat is genuinely being reduced in a strategically meaningful way. Due to the very nature of American society, we live in a potentially target-rich environment—our vulnerabilities are virtually limitless. Establishing strategic defensive priorities in such an environment poses formidable problems. In addition, the natural tendency of decisionmakers to fill specific needs in their own communities as opposed to national security needs makes allocating resources even more difficult, especially in the absence of clearly articulated requirements and measures for evaluating effectiveness.

In spite of these challenges and uncertainties, the need for strategic planning and risk assessment is inescapable. For that reason, the panel will describe a future state that attempts to chart a course for managing the risks of terrorism balanced against other threats and through acceptable measures of public policy.

As this report goes to press, the panel recognizes that the level of awareness and initiatives already taken by government at all levels and increasingly by the private sector and the general population constitute an important beginning. As such, they offer the country a sound basis for building a solid foundation for those future conditions—the New Normalcy that we will describe—in which there is a level of acceptance of the actions to combat terrorism akin to the eternal vigilance that characterizes the national posture on other more traditional threats to American values and national well-being.

Protecting Civil Liberties

The attacks of September 11 and the subsequent anthrax attacks in the fall of 2001, led to new laws, policies, and practices designed to enhance the nation's security against the terrorist threat. These security measures have prompted a debate about their effect on civil liberties, especially privacy. The panel believes that the debate should be reframed. Rather than the traditional portrayal of security and civil liberties as competing values that must be weighed on opposite ends of a balance, these values should be recognized as mutually reinforcing. Under this framework, counterterrorism initiatives would be evaluated in terms of how well they preserve all of the unalienable rights that are essential to the strength and security of our nation: life, liberty, and the pursuit of happiness. While these fundamental rights are guaranteed by our Constitution they should not be confused with privileges, which may be imposed upon to protect national security. However, even privileges should not be imposed upon lightly; they are fundamental to our quality of life. For example, the opportunity to fly may be viewed as a privilege rather than a right, but overly stringent and arbitrary security measures can not only have an economic impact but could also increase public skepticism about security measures generally.

As more terrorist attacks occur, the pressure will rise to lessen civil liberties, albeit perhaps with different labels. Governments must look ahead at the unintended consequences of policies in the quiet of the day instead of the crisis of the moment. One thing we have learned from Al Qaeda is

that they pick the time and day that they will strike. They are ideologically patient. We are not. There is probably nothing more strategic that our nation must to do than ensure our civil liberties.

Shortcomings in State and Local Empowerment

Every State and most localities in America have taken steps for combating terrorism, but it is time to ask ourselves: *If local responders are in fact our first line of defense, have we succeeded in effectively empowering and enhancing State and local capabilities?*

The overall picture that emerged from the RAND survey is that State organizations tend to feel that the Federal government is giving them some of the support they need, although there are areas for improvement. By contrast, local organizations tend to feel less positive about Federal empowerment. This may reflect the fact that the State governments have more experience in working with Federal grant programs and understand the wide gap between "an announcement" and the reality of the time frame for funding to actually flow, once it has been appropriated by the Congress. Local organizations sound a consistent theme of the need for direct Federal support, and this may indicate that States need to do a better job of managing expectations and providing better education on grant-making processes. For example, more than 80% of "First Responder" funding has been dedicated to local governments, a much higher percentage than that available to States.

A continuing problem is a lack of clear strategic guidance from the Federal level about the definition and objectives of preparedness and how States and localities will be evaluated in meeting those objectives. While some progress is being made, it is not happening at a pace commensurate with the flow of Federal funding to communities and States. By the time clear definition and objectives are provided, many communities and States may have embarked on paths that are measurably different from those adjacent to them and potentially inconsistent with a national approach. Moreover, deadlines should not be allowed to overtake deliberative approaches. Such actions further weaken our ability to establish the foundation for a unified national enterprise approach.

A second problem is the deficit in intelligence and information sharing. The creation of the Terrorist Threat Integration Center may have increased intelligence and information sharing at the Federal level. Some increases have also occurred in actionable, sensitive (but unclassified) information shared with State and local decision makers, but it remains ad-hoc and diffuse among various Federal agencies.

Further, to the lack of security clearances at the State and local levels continues to inhibit the widespread dissemination of more general strategic intelligence beyond a very limited number of individuals.

The lack of a well defined process for two-way information sharing means that State and local officials are both not receiving the information they need to make strategic decisions and are not consistently providing Federal authorities with critical intelligence and information developed at the local and State level that may have measurable implications for national security.

Finally the lack of a clear process for translating requirements at the State and local level into research and development at the Federal level means that the products being developed may not be tailored to meet the needs at all levels of government. To be fair, the Federal government has succeeded in providing some resources to localities, States and to a lesser degree the private sector, and also in providing a somewhat more unified point of contact for certain purposes within the Federal government. But those processes require further improvement.

Effects of Other Events

The political cycle of the United States results in cyclical responses, while national and world events often motivate us to respond reactively. In addition to the battles in Iraq and Afghanistan, in recent months we have had several major events: we have had a widespread blackout across the northeast; we have had a hurricane on the Atlantic Coast; we have had historic fires in California; and we have had a number of health and medical events such as the large outbreak of Hepatitis A and a current virulent flu strain. These events have affected the American psyche and may dilute the focus on domestic preparedness for terrorism. While other events such as the car and suicide bombings over the last several weeks in Turkey and Iraq remind the world of the potential for terrorism around the globe. There needs to be a sustained effort that is not subject to the ebb and flow of the national and international events or national debates. Based on our political history, this will be difficult to do, especially in an election year.

The Criticality of Forward Planning

The political cycle in the United States tends to focus decisionmakers on the near term. As the President has stated, the war on terrorism is going to be long and hard, and it is the view of the panel that efforts at combating terrorism must be institutionalized. The Department of Homeland Security is still hiring and moving personnel, organizing itself structurally, defining its mission more clearly, and often responding to the crisis of the day. This problem is not unique to DHS. In many ways, governments at all levels are still "fighting the last war," reacting to September11.

Although we must learn from history, terrorists and terrorism are dynamic, and we must consider the future as well as the past with regards to threats and countering those threats. We must be careful not to focus too heavily on the tactics and techniques September 11. We should consider collectively the changing nature of terrorism and other risks faced by the United States as a means to prioritize resource allocation.

The panel attempts, in this its final report, to provide a future vision for homeland security to serve as a catalyst for debate about the direction for our long-term thinking and planning. Recognizing that a DHS-like entity would only be equal in position to each of the other cabinet agencies and would be focused on day-to-day operations, the panel recommended previously that an office in the White House coordinate the country's efforts. DHS does not have overarching authority for directing all aspects of the homeland security mission. As examples, the Department of Justice, the Department of Health and Human Services, and the Department of Defense are still major players. Our firm opinion is that an entity in the White House, currently the Homeland Security Council and its supporting staff, needs to provide the strategic vision and interagency policy coordination within the Federal Executive Branch. This process will also require direct and continuing integration of local, State and private sector players—not just with DHS as the go-between—in the HSC on-going efforts. Moreover, we repeat our strong view that

an entity in the White House, to be truly effective, must have some clear authority over the homeland security budgets and programs throughout the Federal government.

Focus Remains Federal-Centric

The panel recognized initially that while there is a need for a national strategy, in almost every case the response to any attack is first and foremost by local and State authorities. The focus on a solution at the Federal level is too narrow and in some ways the easy part. There are 55 States and territories; with the lack of clear articulated vision from the Federal level, each has been moving to combat terrorism in its own way. In many ways, the fight now is at the State and local levels, and so the panel has refocused its vision to some extent on the State and local portion of how well the Federal government is supporting State and local efforts.

The Federal government (the Executive and Legislative Branches) has initiated many types of programs, processes, systems, training, proficiency tests, grants, and other activities, without sufficient mechanisms in place at the State, and especially at the local level, to accomplish these tasks and to obtain meaningful input on their efficacy. The Federal government is moving forward in many areas and simply expects States and localities to catch up. This process cannot be effective without a coordinated system for the development, delivery, and administration of various program tasks that engages a broad range of stakeholders. Until a mechanism is in place—one that is more than a few meetings of advisory groups—to articulate requirements and develop priorities from the local level up to the national level, there will be continuing fragmentation and potential misapplication of resources.

An Enterprise Architecture for the Future

To achieve a truly national strategy, the Federal government must empower States and locals by providing a clear definition of preparedness and a strategic plan and process to implement the objectives of a longer-term vision across the entire spectrum from awareness through recovery. While the vision will specify the strategic objectives, the Federal policies must allow the States' flexibility in implementation to reflect the individual resources and communities within States. The Federal government should provide resources to States through a single source, based on risk and with measurable goals that encourage regional actions and integration. Let us be clear: Risk-based allocation of finite resources makes good practical sense. But the challenges of an uncertain threat environment first requires the development of a comprehensive national risk assessment that provides "apple to apple" comparisons among communities and States, and certain aspects of the private sector. Such a process does not currently exist. Officials at the Federal level should lead the development of *an enterprise architecture* to institutionalize intelligence and information sharing, risk assessments, better integrated planning and training, and effective requirements generation in close coordination with State and local governments and the private sector. Only through true cooperation will we achieve some sustainable measure of preparedness for the uncertain threat of terrorism.

Attempting to Define Preparedness

The panel has noted time and again that preparedness cannot progress until it is defined. While many aspects of preparedness have been defined, there is not one accepted strategic definition. The panel offers its definition below.

> Preparedness for combating terrorism requires measurable demonstrated capacity by communities, States, and private sector entities throughout the United States to respond to acute threats with well-planned, well-coordinated, and effective efforts by all of the essential participants, including elected officials, police, fire, medical, public health, emergency managers, intelligence, community organizations, the media, and the public at large. At times, this may require support from the military, active and reserve. Such preparedness requires effective and well-coordinated preventative efforts by the components of the Intelligence Community, law enforcement entities, and a well-educated and informed public. These efforts must be sustainable over the foreseeable future while maintaining a free civil society.

DEVELOPING A FUTURE VISION

In deciding on its strategic vision, the panel assessed four alternatives—detailed later in this chapter—each of which has validity in its own right. They represent a future toward which the country could deliberately navigate or to which it could drift without a committed effort toward a particular end state. The goals that the panel sets forth are challenging, but we have specifically chosen objectives that can be addressed with varying levels of effort over time.

In the material that follows, we will first describe the process of conceptualizing and fashioning a strategic vision of the character described above and then summarize and discuss the four alternative visions we evaluated. We then address in much greater detail a preferred strategic vision for the future.

Conceptualizing a Specific Strategic Vision for Combating Terrorism

In seeking to cast a useful strategic vision of the conditions that would characterize a sustainable level of national preparedness vis-à-vis the threat of terrorism, it was incumbent on the panel that such a vision be given a structure that is both comprehensive—not too simple considering the problem—and comprehendible—logical but not too complex considering the likely variety of audiences.

It is also imperative that such a conceptualization of the future confront the difficult issue of priorities in the national plan of action to reduce the risk of terrorism *vis-à-vis* other risks. There is a particularly difficult challenge in assessing the potential return on investment of resources in the context of combating terrorism, a context characterized by such wide-ranging uncertainties. This is especially true in the balancing of efforts – and associated expectations – between the two components of risk mitigation, namely threat reduction and vulnerability reduction.

The Time Frame for a Strategic Vision for Combating Terrorism

Recognizing that the threat of terrorism is relatively new to the United States and that many dimensions of the initial response to this threat are only now being implemented – with accompanying uncertainties as to their acceptance and effectiveness – just how far in the future is it reasonable to anticipate achieving the favorable conditions worthy of a strategic vision with some measure of temporal stability? Five years? Ten years? Twenty years? For the purposes of this report, and in consideration of the nature of the terrorism problem and the still early state of development of the U.S. and the larger global response, the Advisory Panel concluded that casting a strategic vision roughly five years into the future was a reasonable objective.

The Threat Assessment Dilemma

It is now well recognized that it is in the nature of global and national affairs that a wide variety of terrorism threats already exist, that others will assuredly emerge and develop, and that the United States homeland will be among the targets of such threats for the foreseeable future. While ameliorating the political, social, and economic conditions that give rise to terrorism is a challenging undertaking that is clearly worthy of the expenditure of national and international time and treasure, it is an effort that is not likely to pay major dividends in the short term—the

typical expectation of our citizens that we will immediately solve any problem. However, it is extremely difficult to assess the magnitude and character of the current threat, much less do a genuinely useful, specific, or actionable threat projection. This clearly will hamper any efforts to develop even crude metrics or measures of performance that reflect whether the threat is being reduced to a strategically meaningful degree. Fortunately, we have to this point, had few attacks against which to measure certain performance. It is likely that future attacks will provide the only meaningful measure of certain aspects of our preparedness. It can be argued, however, that the *absence* of attacks is one appropriate measure of how well we are doing in deterring and preventing attacks.

With this perspective in mind, this report addresses the challenge in postulating a strategic vision with a healthy respect for the uncertainties in both the current and potential future terrorism threat spectrum. These uncertainties include the prospect that the source of such threats might be not only independent or quasi-independent terrorist organizations—either international or of a "home-grown" variety—but also possibly state-sponsored terrorism. In this latter case, terrorist actions might be carried out anonymously without attribution, and possibly even without strong suspicion as to their source. In such state-sponsored terrorism circumstances, the magnitude of the potential terrorist threat would move well beyond (in both character and magnitude) the levels usually associated with independent terrorist organizations.

In casting a strategic vision for U.S. efforts to combat terrorism, there are inevitable issues of priorities in setting goals and in the allocation of scarce resources to achieve those goals. In an environment where you can't do it all, where will the nation get the greatest return on investment in its efforts to reduce the risk of terrorism? In threat reduction efforts? In improved hardening or other methods of reducing traditional vulnerabilities? In improved warning and associated planning to permit adequate time to take (presumed temporary) measures to reduce vulnerabilities?

This dilemma is portrayed graphically in Figure 1, which emphasizes the three main areas of competition for resources in the effort to reduce the risk from terrorism:

(1) Threat reduction through direct action to destroy or dismantle terrorist groups ("draining the swamp") and deny such groups chemical, biological, radiological, and nuclear weapons and other instruments of terror;
(2) Vulnerability reduction through a wide variety of pre-attack terrorism-specific actions that would be effective independent of near-term strategic or tactical warning (a "fortress against terrorism"); and
(3) Vulnerability reduction through terrorism-specific actions that would be implemented upon tactical warning of an imminent attack or that an attack is on the way but has not yet arrived.

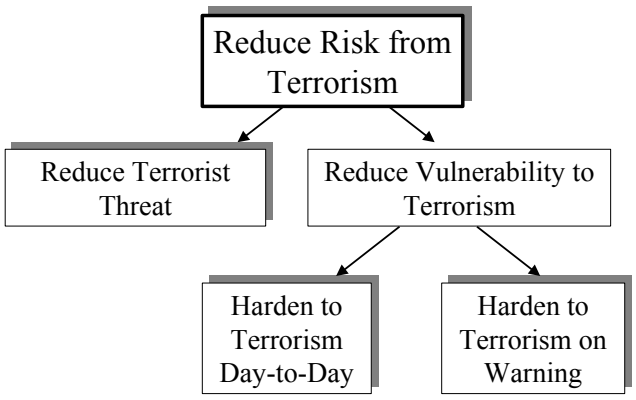


Figure 1. Terrorism Risk Reduction Components

It can be inferred from Figure 1 that more than one legitimate strategic vision – i.e., a vision fully defensible in the light of terrorism-related uncertainties – is possible in this context through a mixing of priorities between the three main areas of competition for resources. In the simplest terms, any of the three main areas of risk reduction cited above could dominate a strategic vision. (A fourth simple and extreme alternative would be not to take any counter-terrorism actions and rely wholly on existing plans and programs for natural disasters and other hazards.) At the same time any evaluation of alternative constellations of priorities requires a careful look at the individual domains of associated counter-terrorism activity – as discussed below. The challenge presented by this kind of prioritization process will be seen more clearly in the detailed consideration of alternative strategic visions.

Careful consideration of the domains also makes clear that, at least in principle, there are potential responsibilities in each of the domains at virtually all levels of government and society. At the same time for some domains and activities it is clearly unrealistic to expect State and local governments to accept the same level of responsibility as the Federal government or for individual citizens and the private sector to take on the same level of responsibility as government.

With this perspective in mind, and looking to fashion a strategic vision some five years in the future that is realistic in terms of the likely commitment of scarce resources to the terrorist threat versus other threats and problems faced by governments, the private sector, and individuals, the sections that follow—after consideration of the difficult terrorism threat assessment and projection problem—sequentially address each of the above domains with a particular eye to providing the building blocks for fashioning such a strategic vision.

Constructing Alternative Strategic Visions

As noted, there are inevitable issues of priority and emphasis in:

- Identifying a finite set of key characteristics or dimensions by which to describe a meaningful strategic vision of the character contemplated here;

- For these key characteristics, setting meaningful goals or objectives against which progress and achievement can be measured in some qualitative or even quantitative fashion; and

- The allocation of scarce resources to achieve such goals.

With this perspective in mind, the panel believes that consideration of the following key dimensions can provide the basis for characterizing and drawing distinctions between alternative strategic futures for combating terrorism.

Four Specific Alternative Visions

Terrorism is and will remain vague, ambiguous, unpredictable, and largely episodic. It will continue to require an approach unlike any other enemy with which we have had to deal. In considering alternative visions, we have postulated three somewhat different threat scenarios over the next five years, recognizing that reality may prove to be some combination or permutation of them.

> Very Infrequent Attacks. This scenario is characterized by the absence of significant terrorist attacks in the United States. It assumes an eventual success in the Iraqi war and a reduction in Israeli- Palestinian tensions over the next five years. In retrospect, 9/11 is seen as a unique event, highly unlikely ever to be repeated particularly as time goes by. It is also characterized by the absence of successful terrorist attacks on U.S. assets and bases overseas (akin to the African Embassy bombing or the attack on U.S.S. *Cole*.
>
> A Continuation of Post-9/11 Threats Levels. The country continues on basically the course it is on today, anticipating a long-term, slow motion, highly episodic strategic threat. The episodic incidents of terrorism might include some major incidents, albeit most likely not with the impact of 9/11.
>
> A Rise in Terrorist Attacks and Lethality. In spite of a U.S.-led international effort to combat terrorism, the overall terrorist threat stays ahead of national and international preparedness. Independent terrorist groups are increasingly in league with nations hostile to the United States. In this scenario, attacks continue be successful worldwide, and Americans are killed or injured in attacks at home and abroad.

With that background and having considered the dimensions of the challenge, the four illustrative strategic visions considered by the panel were:

- **Complacence**. The push for committing resources to combat terrorism is significantly diminished with increased political pressure from those who want resources in other areas, and the country returns to a state of pre-9/11 focus on preparedness. But the terrorists' interests in attacking the United States have not diminished and the country, in effect because of decreased vigilance, is potentially vulnerable to an attack with strategic impact akin to 9/11.

- **Reactive**. There would be steady funding but be no major increases in the level of assets (time, money, coordination, training, exercises, etc.) committed to homeland security and other dimensions of the terrorism problem. Organizational and other efforts that have been launched since 9/11 would be continued with some consolidation. The country will react strongly in the short term, but not fundamentally change its resource allocation priorities over the longer term.

- **Fortress America**. Most observers express skepticism about the prospects of significantly curtailing the terrorist threat without draconian measures. The prospect of unforeseen severe terrorism-related financial and personal losses is acknowledged and addressed via insurance and government programs that compensate victims under procedures akin to the aid provided to victims of natural disasters. An ever-increasing level of resources is committed to combating terrorism with a focus on improved prevention and response, as well as hardening and reducing vulnerabilities in critical infrastructures. Significant resources are devoted to the "fortress" at the expense of other programs and initiatives and civil liberties are actually or perceived to be eroded.

- **The New Normalcy**. The country navigates toward a new normalcy in its posture and approach to terrorism. The threat of terrorism is not eliminated but the threat is viewed in light of an aggressive and coordinated international effort to combat the threat. The destructive risks associated with terrorism are normalized at the personal, State, and local level vis-à-vis other destructive acts against U.S. society and interests both natural and manmade ("Take the terror out of terrorism"). Efforts to combat terrorism are substantial as compared to the period before 9-11 but prioritized, institutionalized, and sustained. Terrorism is essentially treated as criminal action of a hybrid intranational/international character, with attendant clear roles and responsibilities at the Federal, State, and local level and in the private sector, as well as among citizens. This approach provides duality of purpose so that we are better prepared for all emergencies and disasters, including terrorism. It is broad and considers not only the physical impact but economic and societal as well.

Based on the panel's conception of what is both possible and desirable, the first three of the above strategic visions are treated in summary fashion. The fourth, "Forging the New Normalcy," is the panel's conception of the strategic vision that it believes should guide U.S. decision-making and strategic planning for the foreseeable future. In taking the steps to ensure the New Normalcy, the country will likely avoid many of the pitfalls inherent in the first three potential futures. The New Normalcy is, therefore, treated subsequently in greater detail. (For a side-by-side comparison of components of each of the visions, see Appendix L.)

AMERICA'S NEW NORMALCY

January 20, 2009—Washington, DC

It is the morning of January 20, 2009. In a few hours the President will give his Inaugural Address, which will cover, among other things, the significant progress that has been made in combating terrorism both worldwide and in the homeland. The President will describe major improvements across the entire spectrum of capabilities to combat terrorism from awareness activities (intelligence and information sharing), to prevention, to preparedness, through response and recovery.

The news has not all been good in the five years prior to New Year's Day 2009. American interests have continued to be attacked around the world by those who hate freedom and the country that most epitomizes liberty and equality. Overseas, scores of Americans have died and many more have been injured. At home, while nothing on the scale of September 11 has recurred, the remnants of al Qaeda and others trying to imitate it have attacked a few soft targets with "conventional" type devices, and killed 21 more Americans on our own soil.

Nevertheless, with vastly improved intelligence and cooperation from our allies—some very nontraditional—several attempts by terrorist groups to acquire a variety of chemical and biological weapons, and low yield radiological devices, have all seemingly been thwarted.

On the home front, coordination at all levels of government and with the private sector has improved significantly and has been institutionalized and regularized. The public at large understands the nature of the terrorist threats, and has increasing confidence in government to be able to deals with those threats appropriately. There is a stronger sense among our citizens of physical and economic security as well as societal stability, as a result of visible successes among governments and the private sector in developing and implementing strategies and plans that address the threats.

Future Vision 2009—State, Local, and Private Sector Empowerment

States, localities, and appropriate entities in the private sector are fully and consistently integrated into planning and decisionmaking processes. The DHS regional structure and an integrated communications and information network provides for real time, day-to-day coordination across a broad spectrum of prevention, preparedness, response and recovery issues at all levels. The Homeland Security Council is engaged in continuous, sustained, and well-organized dialogue with all levels of government, the private sector, and academia to develop a forward looking vision of readiness efforts.

The Federal government has developed and implemented a consistent program of financial support for State and local government efforts to combat terrorism, a program that has played a major role in sustaining State and local investment to combat terrorism and coordination in Federal, State, and local preparedness planning. Of particular significance has been the sustained funding to strengthen preparedness and coordination within the public health system. Information on Federal support is available through a central clearinghouse managed by DHS.

The Federal government, in coordination with the States, has developed grants and other forms of Federal assistance to fund programs that are based on continuing risk assessments where population is only one measure of vulnerability. Federal assistance is based on a fully developed system of priorities and requirements generation that flows up from the local level, is consolidated and coordinated at the State and territorial level, and then is rationalized against available Federal funding.

DHS, in cooperation with other Federal agencies and State and local governments, has coordinated the development and implementation of a comprehensive process for State and localities, and appropriate entities in the private sector, to assess and articulate potential requirements for all-hazards Federal support. That process has vastly improved the allocation of Federal resources based on a prioritization of capabilities for potential support.

Most important, the Federal government has incentivized through funding a nationwide system and has provided significant support to States for the implementation of a comprehensive, integrated, overlapping network of mutual aid for all-hazards response—a "matrix" of intrastate multijurisdictional and interstate supporting capabilities that has helped to ensure responsiveness anywhere in the country. Federal assistance in this system is based on various considerations, including localities and areas of higher threat, the efficiency of consolidating resources in highly trained and well equipped government response entities, and close coordination among all levels of government and the private sector.

State and local responders have been adequately funded, equipped and trained to meet nationally defined and accepted terrorism preparedness standards. Risk assessments have been developed and updated in line with national guidelines. There is a National Incident Management System (NIMS) adopted and used by all levels of government and the private sector. Significant progress has been made in communications interoperability for all response disciplines. Regular exercises are held to refine and practice in the effective response to potential terrorist attacks and other hazards.

Future Vision 2009—Intelligence

The relationship between DHS, the intelligence community, the Department of Justice and the FBI, and the other Federal agencies involved in collection, analysis, and dissemination of terrorist threat information is increasingly mature with strong and effective coordination responding to DHS leadership and DHS-levied intelligence requirements.

The Terrorist Threat Integration Center (TTIC) is seen as increasingly successful in integrating overseas and domestic intelligence, including information from State, local and private sector sources, to provide a well-reasoned comprehensive strategic terrorism threat assessment covering potential perpetrators, capabilities, and objectives. The overseas and domestic intelligence assessments that are emerging acknowledge continued uncertainties in the current and projected terrorism threat, while at the same time placing bounds in a manner useful for planning purposes on the magnitude and character of that threat. All appropriate elements of other Federal agencies have been fully integrated into the TTIC, and it has significant staff elements representing State and local government entities and the private sector. Executive Branch and Congressional oversight mechanisms have proven to be highly effective in preventing any abuses.

The emphasis on combating terrorism within the intelligence community over the years has led to an unprecedented level of expertise and cooperation, including matters related to health and medical factors.

The broad national commitment to combating terrorism has led to vastly improved vulnerability assessments across the different elements of society (including in particular in the area of critical infrastructures) and a commensurate ongoing effort to reduce existing vulnerabilities and limit the emergence of new vulnerability problems.

The improvements in both threat and vulnerability assessments have enabled DHS to produce overall national risk assessments for critical target sets (such as infrastructures and national icons) and to aid State and local governments in high-risk target areas in performing site- and community-specific risk assessments, including real-time risk assessments that respond to new actionable intelligence. These data are being used to guide the allocation of preparedness funding but not to the exclusion of those low threat areas. The national warning system has been refined to provide more geographic specific information based on the actual or potential threats.

While the availability of actionable warning cannot be guaranteed, there have been instances in which such warning has been available and has contributed substantially to reducing the impact of terrorist attacks. For planning purposes, however, it is still assumed that in many cases of terrorist attack, such warning will not be available.

Future Vision 2009—Information Sharing

In addition to the information sharing within the Federal government that has enabled improved threat assessments, terrorism-related cooperation on sharing information on every aspect of combating terrorism—from risk assessments to best practices for responding to specific threats—within the Federal government, between the Federal government and State and local entities, and between governments and the private sector, has vastly improved.

The Intelligence Community, in cooperation with other Federal agencies, with State and local governments, and with the private sector, has developed a new classification system and a series of products that are unclassified but limited in distribution to allow dissemination to those responsible for public and private sector preparedness. Specific products with actionable guidance are designed to meet the needs of and available daily to public health officials, State and local law enforcement, and other responders.

Most noteworthy is the improvement in information sharing between the government and among the owners and operators of critical infrastructures, made possible by major changes in previously existing laws and regulations regarding freedom of information and restraint of trade.

The Federal government has led the development of a comprehensive risk communications strategy for educating the public on the threats from and consequences of terrorist attacks. The strategy covers both pre-event communications and protocols for communications when an event occurs and during recovery.

The Health Alert Network and other health-related secure communications systems that generate all-hazard surveillance, epidemiological, and laboratory information have been substantially improved and strengthened and are now being utilized with high reliability by all entities of the medical and health communities—public and private.

In the border control arena, there is now a well-established, comprehensive database and information technology systems internal to the border agencies under DHS and those of other Federal agencies, State and local entities, private sector operators, and cooperating foreign governments, who conduct activities related to people or things moving across U.S. borders or are involved in border-related intelligence collection, analysis, and dissemination.

Future Vision 2009—Training, Exercising, Equipping, and Standards

Grant programs in DHS have been consolidated into a single entity that reports directly to the Secretary. In addition, the President has established a Federal interagency coordinating entity for homeland security grants, headed by the Secretary of Homeland Security. Allocation criteria have been developed for all Federal grants that considers risk/threat, capabilities, progress towards achieving national standards in various disciplines, population and regional cooperative efforts. That entity has also streamlined the grant application and decision process throughout the government, and has been instrumental in eliminating unnecessary redundancies in programs.

The insurance industry is basing rates on the level of preparedness of communities, States and businesses based on established nationwide standards, providing incentives for enhanced risk management.

DHS has implemented a program that has established training standards for first responders that outlines the tasks, conditions, and standards of performance for individuals and units.

In addition, a broad program of all-hazards exercises, with specific standards for conducting and evaluating them, and funded in part by DHS, continues to expand at the State and local level and with substantial private sector participation. Training specifically for responding to terrorist attacks is given a high priority.

A joint combating terrorism exercise program for potential major terrorists involving CBRN has been institutionalized and implemented nationwide for Federal, State, and local officials and the private sector participants. It has steadily improved the ability of government and private entities to work together effectively.

The sustained level of government funding for terrorism preparedness has facilitated the establishment of standards and proficiency tests associated.

A successful national effort to improve communications interoperability (particularly at the local level) through the promulgating of national equipment standards, facilitated by substantial Federal and private sector investment in RDT&E, has been a hallmark of progress in combating terrorism as a component of all hazards preparedness.

Best practices in all aspects of combating terrorism, informed by lessons learned from exercises and actual events, is available through a significantly improved national database. This best practices database is seen as particularly useful in assisting States in meeting surge capacity requirements and dealing with associated resource allocation issues.

Future Vision 2009—Enhanced Critical Infrastructure Protection

There are major improvements in protective and defensive measures, especially for critical infrastructures. As appropriate, many programs have been implemented as old infrastructures and supporting systems are replaced.

Improvements in the aviation industry include measures mandating the screening of all baggage and cargo for passenger and commercial aircraft and the implementation of a new set of comprehensive security guidelines for general aviation. In the shipping industry, U.S. seaports and many international air and seaports are now equipped with extensive suites of detection and monitoring equipment. In the energy, chemical, and telecommunications sectors, there are now well-established models and metrics for evaluating the vulnerability existing systems and facilities and additional protective measures. In the process of reducing vulnerability to natural disasters and providing redundancy in response to lessons learned from the power outages of 2003, the vulnerability of the energy supply sector has been reduced.

For U.S. border crossings, there are stiff pre-entry identification requirements for people, and pre-shipping reporting requirements and other regulations for commercial shipments that have dramatically improved the prospects of detecting people or materials that terrorists might attempt to move into the United States. Technology has helped the private sector to adjust to new requirements at minimal economic impact.

The country has a vigorous, comprehensive public health system infrastructure, with the capacity to respond around the clock to acute threats, while maintaining the capability to simultaneously respond to chronic public health issues. Public health officials institutionalized relationships with the public and private medical community and other response entities to deal with the full range of potential challenges. Other major improvements include an emphasis on an all hazards/dual use capabilities, and well defined health care requirements for bioterrorism. The national system of special response teams for medical/health contingencies has been unified and modernized with a special emphasis on preparedness for a broad range of bioterrorism attacks, as well as chemical, radiological, and nuclear health effects. The Congress authorized several programs to encourage nursing, epidemiological, large animal veterinarian, environmental health, and pharmaceutical education and training; and workforce issues are fading. After the development of a strategic communications plan, a cooperative effort of Federal, State and local public health officials, the nation is in the middle a five-year campaign to improve the psychological readiness and resilience of the U.S. population.

Cyber and physical threats to critical infrastructures have been addressed through a strategy that recognizes interdependencies and potential cascading effects. Programs to ensure that the latest in protective tools and practices are implemented have been increasingly successful in building confidence throughout the networked systems that are vulnerable to attack.

The potential threat to the agriculture and food industries is continually being assessed in a cooperative effort between the intelligence community, DHS, DHHS, and the Department of Agriculture (USDA) that includes joint education and training programs. As a consequence of this continuing assessment, specific actions to protect the agriculture and food industries have been undertaken, to include specially designated laboratories to perform tests on foreign agricultural diseases. In addition, Federal support has substantially increased the level of research and funding for veterinary medicine education. USDA has an integrated network of Federal and State BSL-3 and BSL-4 laboratories for the detection and diagnosis for foreign animal and plant diseases. Through an integrated, voluntary effort, all food production, processing and transport and distribution facilities have achieved basic security guidelines described in Federal guidance. The inspection force is fully trained. Response to an outbreak is clearly defined within a national strategy and a fair system of indemnity to compensate those affected by agricultural losses is available along the spectrum of food production and dissemination (which has helped to encourage rather than discourage the rapid disclosure of outbreaks). Aggressive R&D has produced vaccines for high-risk pathogens such as Foot and Mouth and the USDA research portfolio has been prioritized according to a comprehensive risk assessment matrix for both deliberate and natural outbreaks. In addition, the Federal Government has continued to expand its cooperation and surveillance presence overseas to prevent introduction of pathogens into the United States.

Future Vision 2009—Research and Development, and Related Standards

The Federal government is providing sustained funding for a wide-ranging R&D program that is seeking major improvements in the ability to detect and analyze terrorism-related materials or devices both at the borders and in transit within the country. The Federal R&D agenda is coordinated and prioritized through a comprehensive interagency and intergovernmental process led by the Secretary of Homeland Security.

The National Institute for Mental health has undertaken a long-term research program examining the most effective ways to both prepare people mentally for possible terrorist attacks and to treat people with mental and emotional problems following such attacks.

The Congress has expanded incentives under Bioshield to encourage industrial production and development of biological and chemical defense pharmaceuticals. NIAID, in collaboration with industry, has launched a major research effort in the area of vaccine development in anticipation of possibly facing threats from natural and genetically modified biological agents, and is building on its successes of rapid and reliable diagnostic tests for the full spectrum of biological agents.

New approaches in epidemiologic surveillance are yielding dramatic results, and State and local public health departments are implementing the findings to reduce time in detection of disease outbreaks.

.

The challenge of improving cybersecurity is being addressed through a comprehensive government-industry R&D partnership that has developed not only improved defensive tools and procedures but also industry standards for ensuring that improved protective techniques and tools are implemented on a continual basis.

Future Vision 2009—Role of the Military

Statutory authority and implementing regulations for use of the military inside the homeland—for both homeland defense and civil support missions—have been clarified. Extensive public education—for State and local governments, for the private sector (especially critical infrastructure operators) and for the populace at large, has greatly improved the understanding about legal authority for using the military as well as its capabilities and limitations. Specific attention has been focused on defining the parameters of homeland defense and its distinctions from civil support.

Clearly articulated Rules for the Use of Force exist to govern the military's actions inside the United States in situations where it is unclear if the foe is a combatant or a criminal

In recent years, the role of USNORTHCOM and USPACOM in enhanced civil-military integration for homeland security has been clarified and institutionalized within the Department of Defense. A critically important part of this process has been, as noted, the development of a comprehensive requirements identification process by DHS, and tested through extensive exercises involving USNORTHCOM and State and local emergency response officials.

The potential role and responsibilities of the military in supporting civilian authorities in the event of a terrorist attack has been refined largely through a continued program of training and exercises involving USNORTHCOM, other military entities, and State and local partners with preparedness responsibilities.

USNORTHCOM now maintains dedicated rapid-reaction units with a wide range of response capabilities relating to attack assessment, emergency medical support, isolation and quarantine, and communications support. Capabilities are intended for military homeland defense missions but have been implemented in a way to be applicable to civil support missions as well.

The National Guard has been given new homeland security mission with a comparable increase in funds for civil support planning, training, exercises, and operations. Some Guard units are trained for and assigned homeland security missions as their primary or exclusive missions. With authorizing legislation, the Department of Defense has established a collaborative process for deploying National Guard units including authority to employ the Guard on a multi-state basis for homeland security missions. The National Guard remains a strong component of the military for the war-fighting mission, but enhanced resources are maintained for military assistance to States and communities for all types of emergencies. Use of Reserve Component forces for extended homeland security missions has been structured in a manner that does not detract from recruiting and retention efforts.

Military missions in the homeland are consistent with traditional military missions. Specialized State and local responder capabilities have been enhanced through a sharing of military technology and realignment of funding. State and local responders have more effectively funded, trained, and equipped to address the impacts of a terrorist attack and the military (including the National Guard) have funded and trained for missions distinctively different than those of State and local responders. With this substantial empowerment of State and local civilian response organizations, the potential reliance on any part of the military—active forces and the reserve components (including the National Guard in its non-Federal status)—for military support to civil authorities has diminished.

A ROADMAP TO THE FUTURE

We have outlined an ambitious vision for the near future not only to counter the threat of terrorism but to advance America's ability to prepare more effectively for the full range of threats to our nation. We stress that the vision is not likely to become reality without a firm commitment and sustained effort among all levels of government and in the private sector. Nor are we suggesting that we should accept taking five years to reach all or most of the components of the vision. Even with current programs and resource, the nation must achieve real and measurable improvements soon. Clearly, however, additional steps are needed to bring the United States from its current state of preparedness to the panel's view of America's New Normalcy. Below, we describe where we are and what, in the opinion of the panel, are some of the key steps to achieving the vision. Some recommendations have been made before; they are worth repeating until they have been implemented. The panel does not suggest that these are the only actions required to achieve an acceptable future state of security, nor that implementing all of these steps exactly as we recommend will ensure attainment of the future state. They are, nevertheless, the best judgment of individual panel members within their own discipline and the collective view of the full panel as an opportunity for translating resolve and policy into action and accomplishment.

Civil Liberties at the Foundation

There is an on-going debate in the United States about the tradeoffs between security and civil liberties. History teaches that the debate about finding the right "balance" between security and civil liberties is misleading. This traditional debate implies that security and liberty are competing values and are mutually exclusive. It assumes that our liberties make us vulnerable and if we will give up some of these liberties, at least temporarily, we will be more secure. Yet, consider the context in which civil liberties were first firmly established. The framers of the Constitution had just survived a truly existential threat and were acutely aware of the fragility of their nascent nation. In this uncertain and insecure environment, the framers chose not to consolidate power and restrict freedoms but to devolve power to the people and protect civil liberties from encroachment. They recognized that civil liberties and security are mutually reinforcing.

The Declaration of Independence has at its core the premise that there are certain "unalienable rights, that among these are Life, Liberty and the pursuit of Happiness." What terrorists seek to destroy requires a comprehensive strategy to defeat their objectives, while seeking to preserve not just life, but also liberty and our uniquely American way of life.

We must, therefore, evaluate each initiative as well as the combined effect of all initiatives to combat terrorism in terms of how well they preserve all of the "unalienable rights" that the founders believed were essential to the strength and security of our nation—rights that have no become so imbedded in our society and ingrained in our psyche that we must make special precautions, take extra steps, to ensure that we do not cross the line. It is more than the clearly defined protections in the Constitution—protections against unreasonable search and seizure; and against self-incrimination. It is that less well-defined but nevertheless exceptionally important "right to privacy" that we have come to expect, and that our judicial system has come increasingly to recognize.

As an example, we should not move away from the traditional requirement for a criminal predicate to justify law enforcement activity. As a Nation, our most significant concerns with broadening law enforcement powers should be

- the potential chilling effect of allowing the monitoring of First Amendment activities, such as freedom to peaceably assemble, the free exercise of religion, and freedom of speech, to the point where it discourages the exercise of or directly impinges upon such fundamental rights; and

- the increasing reliance on more sophisticated technology that has vast potential for invading our privacy.

Military intelligence gathering as an aid to law enforcement or as part of military "homeland defense" missions was not fully anticipated by our existing system of laws and safeguards. It now becomes essential for the Congress to legislate and for the Department of Defense to implement through clear procedures the limitations on the use of satellite imagery and other advanced technology monitoring inside the United States. Such limitations, we suggest, should be similar to those governing electronic surveillance for intelligence purposes inside the United States under the Foreign Intelligence Surveillance Act in 1978.[2]

To enhance both our security and our liberty, **we recommend that the President establish an independent, bipartisan civil liberties oversight board to provide advice on any change to statutory or regulatory authority or implementing procedures for combating terrorism that has or may have civil liberties implications (even from unintended consequences).**

Strategy and Structure

The process of creating the Department of Homeland Security (DHS) has been one of the most significant and challenging United States government restructuring efforts since World War II. The aim of establishing DHS and integrating a wide range of agencies and offices has been to increase the security of the U.S. homeland and to improve the governments' ability to prevent and prepare for terrorist attacks and other major disasters. Indeed, the challenge of integrating 22 separate agencies into a single, effective department has been substantial. Anecdotal evidence suggests that many of the agencies and employees subsumed by the integration continue to have no identity with or "buy-in" to their parent organization. Overcoming these factors is critical to the success not only of DHS but to the national effort.

Clearly, there has been a strong focus on ensuring that the structure of DHS is right to achieve programmatic and operational level coordination and execution. The fact remains that the homeland security dilemma facing the United States is broader and more complex than a single agency. The Department of Homeland Security, as a Secretariat within the Federal government, now competes with other Federal entities for funding and policy attention. Its primary focus is that of "physical" protection, which leaves the broader issue of economic and societal security potentially lacking for attention.

[2] 50 USC 1801 et seq.

There remains, especially at the policy level, the continuing need for Federal cross department and agency coordination, and regular continuing dialogue with local and State elected leaders. In addition, the need for forward thinking, strategy development, and planning can best be accomplished in a forum free from the day-to-day crisis and reactive environment that has characterized DHS—an understandable situation, given its mission. Internal DHS strategy and planning can and will occur, but there remains a compelling need for higher-level policy coordination at the White House that rises above the inevitable turf wars among Federal agencies. Ostensibly, the Homeland Security Council will accomplish this task, but that entity has little structure for engagement of local and State elected leaders now that the Homeland Security Advisory Council and its advisory groups have been transferred to DHS.

State and local officials across all responder organization expect a lot from DHS. For example, 70-80 percent of State and local organizations expected DHS to improve coordination, information-sharing, and communication among governments at all levels, according to the RAND survey. Where there were differences in views, the pattern reflected a particular organization's mission or primary Federal agency partner. For example, fewer State public health departments (33 percent) expected DHS to streamline the grant application process as compared to 60-70 percent of other organizations. This difference makes sense, given that DHHS (not DHS) is the primary Federal agency providing support to public health departments. State OEMs were in agreement with other organizations, but in several cases expressed the opinion more strongly. Overall, 50-60% of organizations expect DHS to standardize the grant application process across Federal agencies and consolidate multiple grant application requirements; however, 80 percent of State OEMs expressed this view.

The stronger desire by State OEMs for DHS support in these areas is consistent with the mission of the State OEMs and their role in helping to distribute Federal preparedness funding and support to local entities. Table 1 lists other areas where responders expect empowerment from DHS.

Table 1. In What Ways Do Local/State Responders Expect the DHS to Impact Them?

	Activities
70-80% expect DHS to…	▪ Improve coordination, information-sharing, and communication between Federal/State/local levels
60-70% expect DHS to…	▪ Streamline grant application process across Federal grant programs
50-60% expect DHS to…	▪ Standardize the grant application process across Federal agencies and consolidate multiple grant application requirements
40-60% expect DHS to…	▪ Establish single point of contact at Federal level for information on available programs ▪ Provide primary contact at Federal level instead of many on training, equipment, planning and other critical needs *[Health organizations not asked this question]*
45-60% expect DHS to…	▪ Provide intelligence information and more detailed guidance on terrorist threat
40-60% expect DHS to…	▪ Consolidate numerous training courses/ programs and numerous equipment programs *[Health organizations not asked about equipment programs]*
40-60% expect DHS to…	▪ Provide better/standardized templates and/or guidance to help with planning
30-40% expect DHS to…	▪ Improve integration between public/private sectors' efforts to improve terrorism and protect critical infrastructure

DHS is still relatively new; time will be required for it to be come fully effective and operational. Yet, there are apparent areas for concern, including intelligence analysis and dissemination; duplication of efforts; lack of standards; and the continuing ability of DHS component agencies to fulfill traditional—and important—day-to-day missions. DHS has largely been sidelined in

the evolving process of terrorist-related intelligence. Despite legislative mandates, it has developed little analytical capacity and has insufficiently developed capabilities to disseminate information to State, local, and private actors. Numerous reports have pointed out that cooperation between departments of the Federal government, State and local government agencies, and private sector entities has clearly been inadequate.[3] Interviews with State and local officials (conducted by RAND for the panel) have indicated that DHS has not yet effectively shared threat information with appropriate State and local entities. Indeed, DHS has had significant competition from other Federal agencies in disseminating information to State and local authorities, and the private sector despite President Bush's July 2003 Executive Order giving the Secretary of Homeland Security primary authority for sharing homeland security information.[4]

DHS is an operational entity. As such it *executes* policy. It does not own all of the Federal capability for combating terrorism and cannot, therefore, be expected to develop even a Federal government-wide policy, much less a national one, for addressing all aspects of awareness, prevention, preparedness, response, and recovery. On the other hand, entities in the Executive Office of the President do have that broad mandate to develop policy applicable to those affected entities of the Executive Branch. In this case, the entity is the Homeland Security Council (HSC) and its supporting staff (the HSC staff—the successor to the Office of Homeland Security). That entity should have the responsibility for developing the longer-range vision and the strategic policies for implementation. It should not be involved in planning or conducting operations, except as observers to help inform future policy development.

Current DHS structure suffers from a duplication of emergency preparedness and response efforts. In particular, the location of the Directorate of Emergency Preparedness and Response (EP&R) and the Office for Domestic Preparedness (ODP) in separate directorates has created internal and external problems. In the April 2003 *Semiannual Report to the Congress on the Department of Homeland Security*, the Office of Inspector General argued that placing planning, training, and equipment purchases for emergency management personnel in different DHS directorates creates problems with interdepartmental coordination, performance accountability, and fiscal accountability.[5] It also leads to confusion among State and local officials for identifying available Federal preparedness resources.

Since September 11, 2001, State organizations have participated more than local organizations in federally-sponsored training, equipment, and funding programs.[6] In addition, while State organizations tended to participate across a variety of programs, local organizations participated

---

[3] *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001* (Washington, DC: U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, December 2002); Ivo H. Daalder et al, *Assessing the Department of Homeland Security* (Washington, DC: The Brookings Institution, July 2002), pp. 17-21; Gary Hart and Warren B. Rudman, *America – Still Unprepared, Still in Danger* (New York: Council on Foreign Relations, 2002), pp. 1-5; *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force* (New York: The Markle Foundation, October 2002), pp. 69-78.

[4] George W. Bush, *Executive Order: Homeland Security Information Sharing* (Washington: White House Office of the Press Secretary, July 29, 2003).

[5] Department of Homeland Security: *Semiannual Report to the Congress* (Washington, DC: Office of Inspector General, April 2003), pp. 3-4.

[6] For a detailed summary of the survey results regarding organizations participation in federally-sponsored programs, see Tab 3 to Appendix D.

in a more limited number of programs specific to their professional community. Further, State organizations tended to have much higher participation rates than local organizations. In general, State organizations that had participated in federally-sponsored programs since the 9/11 attacks also shared those resources with other organizations within their State (commensurate with their mission and role as a pass-through for Federal support to local communities and response organizations). In addition, those local organizations that had received Federal support also tended to share it with other organizations within their jurisdiction.

State and local organizations differed in their views about whether Federal funding was reaching the right communities and organizations. State OEMs and State public health departments (those organizations responsible for distributing Federal funding and/or resources within their State for emergency and bioterrorism preparedness) tended to believe that Federal support was reaching those communities and organizations with the greatest need. Local organizations, on the other hand, were more likely to believe that Federal funding was *not* reaching the communities and organizations with the greatest need, regardless of whether the funding was distributed through the State governments or directly to local communities and response organizations. (For more detailed survey information, see Appendix D.) This highlights the need for Governors to drive comprehensive state-wide strategies (that reflect composites of local, interjurisdictional, and State agency needs within each State) that address the full range of readiness and cross the continuum of State and Federal funding programs as a precursor to managing national expectations. In the absence of a measurable end-goal, everyone—States and localities—will likely believe and insist that their agency should get everything.

State and local governments should have a one-stop clearinghouse for grants, training programs, and other types of terrorist and disaster preparedness assistance. Perhaps more seriously, the absence of coordinated preparedness efforts makes it difficult to develop training and exercised standards that are agreed upon and utilized by all relevant training centers. Some current funding processes have DHS and other agencies awarding preparedness grants directly to public and private recipient organizations with no pre-award coordination with the States. Recognizing that there inevitably will be some of the current programs that do not "flow through" the States, there should, at a minimum, be vertical coordination requirements among Federal agencies and local governments with States on all funding allocations, to ensure consistency with statewide strategies. DHS and other Federal agencies may be required to make some awards directly, but that does not negate the need and appropriateness of engaging States in the process.

In addition, there are at least six Federal departments and a number of interagency and independent organizations that are involved in developing standards for communication systems and equipment. This situation makes it difficult for States and local entities to know what to buy, and increases the possibility of incompatible equipment.

Finally, current DHS efforts have diminished and compromised important "traditional" day-to-day missions of some component agencies. For example, the Coast Guard has put substantial resources into patrolling ports and assisting in U.S. military operations in Afghanistan and Iraq, but it has seen decreased resources for important missions such as drug interdiction. Recent disasters across the nation have identified issues between the DHS parent organization and FEMA in terms of roles and responsibilities. While these types of challenges are not unexpected with a reorganization of this magnitude they, nonetheless raise the concern that momentum across a broad spectrum of activities is being interrupted.

Based on the foregoing, **we recommend that DHS combine all departmental grant making programs into a single entity in DHS.** Currently, grant programs are scattered through several departmental units. One alternative is an expansion of ODP (renamed) with that office reporting directly to the Secretary. **We also recommend that the President establish an interagency mechanism for homeland security grants, led by the Secretary of DHS, to streamline and consolidate the grant application and decision process throughout the Federal government.** The creation of such a process will reduce confusion among grant applicants, and relieve them of some of the burden of multiple—and different—application processes.

We further recommend (again) that DHS develop a comprehensive process for establishing training and exercise standards for responders. That process must be involved in the development of training and exercise curricula and materials. It must include State and local response organization representation on a continuous, full-time basis.

The Homeland Security Advisory System has become largely marginalized. This may be attributed to a lack of understanding of its intended use as well as the absence of a well-orchestrated plan to guide its implementation at all levels of government. The Governor of Hawaii chose to maintain a blue level in February 2003 when the Federal government raised the level to orange, and the Governor of Arizona announced that his State might do the same based on the particular threat or lack thereof to Arizona.[7] Organizations surveyed by RAND for the panel had a number of suggestions for improving the Homeland Advisory System. Between 60-70 percent of State and local organizations suggested providing additional information about the threat (type of incident likely to occur, where the threat is likely to occur, and during what time period) to help guide them in responding to changes in the threat level.

We recommend that DHS revise the Homeland Advisory System to include (1) using a regional alert system to notify emergency responders about threats specific to their jurisdiction/State; (2) providing training to emergency responders about what preventive actions are necessary at different threat levels; and (3) a process for providing specific guidance to potentially affected regions when threat levels are changed.

Prehospital care—emergency medical services (EMS)—plays a crucial role in the response to and recovery natural and manmade disasters, including terrorism. The Emergency Medical Technicians and Paramedics who comprise EMS in the United States, unlike there fellow responders in fire services and law enforcement, have no designated "EMS" Federal funds and no one single Federal agency for coordination on State and local EMS operational matters. As was cited in earlier panel reports, the lack of any fiscal assistance to enhance EMS response capacity, especially for combating terrorism, must be addressed. In order to reduce mortality and morbidity, especially in the aftermath of a CBRNE terrorist attack, investment in the response component that is tasked with turning victims into patients is critical. Concurrent with the lack of specific funding is the continuing absence a Federal entity that provides guidance and assistance on a daily basis to EMS responders nationwide.

[7] http://www.bizjournals.com/pacific/stories/2003/02/24/story4.html, February 7, 2003; http://www.azcentral.com/arizonarepublic/news/articles/0601homeland01.html

We recommend:

- **That the Congress establish sustained funding to enhance EMS response capacity for acts of terrorism.** Such funding must address personal protective equipment, training, antidotes, technology transfer, EMS interoperability issues, threat assessments, and other operational and training doctrine issues.
- **That Congress reestablish a Federal office specifically to support EMS operational and systems issues.**

State and Local Empowerment

There continues to be a lack of understanding about the roles of State and local government in a national strategy. As discussed in more detail, the Terrorist Threat Integration Center (TTIC) is a pointed example. It is essentially an entity created by and for the Federal government, not (yet) for State and local government. National strategy and concomitant resources need to be designed and executed in a way most likely to empower State and local governments to maintain awareness, and to deter, prevent, respond to, and recover from terrorist events.

Conversely, State and particularly local organizations and officials may not be fully aware of the "big picture," and simply do not have the resources to equip and train every locality to perform every mission across the spectrum of preparedness. Moreover, as salutary as many efforts by States and localities have been, absent a standard system and processes for activities nationwide, the potential for significant incompatibility and lack of interoperability looms large.

Therefore, **we recommend the development of a system of a:**

"Matrix" of Mutual Aid. In coordination with local, State, and other Federal agencies, DHS must develop a plan for a nationwide system of mutually supporting capabilities to respond to and recover from the full spectrum of hazards. Unlike the suggestion of other entities that have addressed the issue, the system does not have to be built on the premise that every community in America must have the same type and same level, based almost exclusively on population considerations, of response capabilities. The panel firmly believes that one size does *not* fit all. The panel envisions a much more comprehensive system of mutual aid than that which generally exists. This expanded system would catalog and display, at any point in time, the capabilities resident anywhere in the country to respond to various types of emergency. It would be built, at its foundations, on capabilities that already exist. Capabilities would constantly be mapped geographically in order to identify gaps in coverage. The goal is not to know the location of every piece of equipment or trained personnel but rather the types and scope of actions that can be undertaken. Every level of government would be required, as a condition of Federal assistance, to participate in the system. Mutual aid would run in multiple directions—from large cities to small towns in the same State and vice versa; from small towns to other small towns in the same State, and from large cities to other large cities in the same State and in other States; from State to State; from the Federal level to States and localities. Such a system would significantly enhance capabilities while making the most of limited resources.

Private Sector Engagement

The important role of the private sector in homeland security has not been fully recognized and articulated. As noted by the panel in its 2002 report to Congress:[8]

> 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.

Enhancing coordination with the private sector is obviously critical for ensuring the preparedness of States and localities and for protecting vital physical and economic infrastructure. In the third wave of the survey, we asked State and local organizations about their coordination activities with the private sector.

Following the 9/11 attacks, nearly all the State organizations and between a third to three-quarters of the local organizations created new organizational structures to address preparedness for terrorism-related incidents. Of those that created new structures, about half (except for public health) indicated that the duties of these new positions or units included liaison with the private sector. For virtually all local and State public health departments, this probably refers to coordination activities with hospitals, managed care organizations, or other individual healthcare providers, many of which belong to the private sector.[9] However, when we compare these results to whether organizations say they have any formal agreements in place with the private sector about emergency planning or response, many fewer organizations indicated this to be the case. Only about one out of three local and State OEMs and one out of five of the other organizations said they had formal agreements with private companies, businesses, or labor unions to share information or resources in the event of an emergency or disaster. Further, few local organizations and only about twenty percent of State organizations and local OEMs indicated that they would contact the private sector if they had any threat information to pass on about suspected terrorist activities within their jurisdiction or region.

State organizations, in particular, recognize there is room for improvement in strengthening coordination with the private sector. Between half to two-thirds of State organizations expect DHS to help improve integration between the public/private sectors' efforts to improve terrorism preparedness and to protect critical infrastructure. The primary linkage for private sector engagement must occur at the local and State levels; that is where the interaction is going to be most effective in preventing or responding to an event.

The business community believes that it has an obligation and wants to be better integrated into planning and preparedness activities than it has been. (See testimony of C. Michael Armstrong,

---

[8] 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, December 16, 2001, pp. 30-31. www.rand.org/nsrd/terrpanel/

[9] The CDC cooperative agreements for public health preparedness encourage establishing public/private partnerships, with one of the enhanced capacities calling for the strengthening of relationships between the health department and emergency responders, the business community, and other key individuals or organizations involved in healthcare, public health, or law enforcement. Source: CDC Continuation Guidance for Cooperative Agreement on Public Health Preparedness and Response for Bioterrorism--Budget Year Four Program Announcement 99051, May 2, 2003.

The Business Roundtable, at Appendix N.) **We recommend the adoption and full implementation of the security component of the Business Roundtable's Principles of Corporate Governance.** An executive summary of those principles is included at Appendix N.[10]

Intelligence and Information Sharing

In the two years following the September 2001 terrorist strikes, governmental bodies, journalists, and policy analysts have advocated a variety of measures intended to improve domestic counterterrorism intelligence. Most of these critics focused on shortfalls within the FBI. This panel and others have recommended the establishment of a new domestic security service that some have likened to the United Kingdom's MI-5. Such an organization, according to its supporters, would focus on prevention, rather than simply investigating terrorist acts once they occur.[11] Critics of the concept charge that it would add needless complexity to the system, slow down rather than promote information flows among agencies, and threaten civil liberties.[12] Ultimately, the Bush administration rejected calls for the creation of an "American MI-5," choosing instead to press for reforms within the FBI and new bureaucratic arrangements within other parts of the Federal government. The FBI's leadership has outlined a comprehensive program of internal changes that are intended to make the prevention of terrorism the bureau's paramount mission.

In some ways, these steps will provide the country with a more robust, comprehensive, and rationalized structure for the analysis and dissemination of terrorism information. Steps have been taken to overhaul the intelligence function of the FBI, including a common analysis of business practices regarding how information is gathered, shared, analyzed, and distributed. This is a potentially useful business-process approach that DHS could adopt in bringing together all of the Federal agencies and State and local government entities to develop of an overarching national plan for the sharing of information and intelligence among all levels of government and with the private sector. Principal elements of this realignment effort should include: (1) investments in communications and information management technology and integration; (2) emphasis on developing rigorous, discretely focused analytical capabilities; (3) establishing a cadre of specifically assigned, professional counterterrorism specialists; (4) increased coordination of dispersed field office operations within the context of a singularly developed (and enforced) national strategy; and (5) a clear set rules that establishes product dissemination to specific entities and the communication links for moving intelligence and other information.

This being said, several facets of the reform process either remain questionable or raise additional issues of concern. These variously relate to: (1) the efficacy of changes enacted within the FBI; (2) the development of viable structures of accountability and oversight to balance more intrusive domestic information gathering; (3) the incorporation of local law enforcement in

[10] The entire document is available at http://www.businessroundtable.org/pdf/984.pdf.
[11] See for example the panel's *Fourth Annual Report to the President and the Congress*, pp. 41-44; and "Senator Edwards Proposes Homeland Intelligence Agency," accessed at http://www.cdt.org/security/usapatriot/030213edwards_pr.html.
[12] See for example David Johnston, "F.B.I. Director Rejects Agency for Intelligence in the United States," Washington Post, 20 December 2002, p. A22; Larry M. Wortzel, "Americans Do Not Need a New Domestic Spy Agency to Improve Intelligence and Homeland Security," Heritage Foundation Executive Memorandum no. 848, 10 January 2003; and Ronald Kessler, "No to an American MI5," Washington Post, 5 January 2003, p. B07.

Federal efforts to combat terrorism; (4) the coordination of national intelligence structures; and (5) the unintended consequence that much of the enforcement for certain types of criminal activity—for example, bank robberies and organized crime enterprises—has been shifted from the FBI back to State and local law enforcement.

As a partial solution to several of these problems, the panel repeats its support for an independent agency with certain domestic collection responsibilities. A separate domestic intelligence collection agency might allow the FBI to return to a context in which a criminal predicate is once again a pre-requisite for law enforcement activity. It could also provide a clearer context in which to evaluate and address concerns that relate specifically to the collection of intelligence inside the Unites States, separate and apart from the issues related to what enforcement actions the government can take based on that information. Clarifying the distinction between intelligence collection authority and law enforcement power could also clarify oversight responsibility. Despite arguments to the contrary,[13] the panel continues to believe—as it articulated in 4th Report—that 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 "sanction" authority of law enforcement agencies—the threat of prosecution and incarceration—could prevent people who have important intelligence information from coming forward and speaking freely. The panel has suggested that this collection entity 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. Nor should it have 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. This independent entity could 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 independent body needs 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 an independent agency would have to operate under significant judicial, policy, and administrative restraints. It will be subject to the requirements of the Foreign Intelligence Surveillance Act (FISA)[14] 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. 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.

Further, to address several of the challenges discussed above, **we recommend that the Congress establish the Terrorist Threat Integration Center as an independent agency and**

[13] At a recent meeting of the Advisory Panel, the Attorney General of the United States made a strong and well-reasoned argument why, from his perspective, the FBI should be allowed to continue domestic intelligence collection. Among other points he raised were the extensive experience that the FBI has, and the network of contacts that it has established with State and local law enforcement, which he (correctly) suggests also collect law enforcement intelligence.

[14] 50 U.S. Code, Chapter 36 (50 USC Sections 1801-1863) (PL 105-511, October 25, 1978)

that the TTIC be required to have permanent staff from representative State and local entities.

Finally to address these challenges, the Attorney General should modify the AG guidelines. The potential chilling effect of broadened surveillance authority could be reduced if, in addition to barring the collection or storage of information *solely* for monitoring protected activity, a more rigorous standard was imposed for any targeting that involved protected activity. The key would be to ensure that the higher threshold was not interpreted in the field as effectively a prohibition against such collection or storage, as has happened in the past.

Organizations want more intelligence information about the terrorist threat, but security clearances are lagging

The RAND survey confirmed that State and local organizations are looking to DHS for dissemination of intelligence information and information about the terrorist threat within their jurisdiction or State, in part to help them in conducting their own risk assessments. Since September 11, 2001, about half of law enforcement and half of local and State OEMs have received guidance from the FBI about what type of information about suspected terrorist activity should be collected and passed to FBI field offices. In comparison, only a quarter of paid/combination fire departments and hospitals and only a few volunteer fire departments indicated they have received such guidance.

Despite a desire for more detailed intelligence information since the 9/11 terrorist attacks, State OEMs and State public health departments are primarily the only organizations that have sought security clearances for their personnel. (For more information, see Appendix D). This finding is likely related to recent requests by DHS and the Department of Health and Human Services (DHHS) for States to apply for such clearances for their senior officials. To date, only about half of State OEMs and a third of State public health departments that applied for security clearances have received them for at least some of their personnel.[15]

Recently, DHS announced that, in addition to State governors, five senior State officials would be issued security clearances to receive about specific threats or targets. (These clearances are in addition to the security clearances to be issued to public health officials.[16]) However, there is concern among State officials that the number of security clearances allocated may still be too few to account for all their needs.

Based on the foregoing, **we recommend**

- **That the Federal government develop and disseminate continuing comprehensive strategic threat assessments on the character, magnitude, and objectives of terrorists and their organizations**. As we have said consistently in previous reports,

[15] Because the survey did not ask when organizations had applied for government security clearances, RAND cannot distinguish between those who may have applied only recently versus those that have been waiting for a longer period of time to receive their security clearances.

[16] DHS Office of the Press Secretary, Press Release August 18, 2003. "Secretary Ridge Addresses National Governors Association."

these assessments must be more than current, actionable information in order to be helpful in longer-term planning and prioritization of resources.

- **That the President designate one or more security clearance-granting authorities, which can grant clearances Federal government wide that are recognized by all Federal agencies.** It is incomprehensible that the security clearances of one Federal agency are not recognized by other Federal agencies. Agency-specific requirements may indicate who can have access to certain information (the "need to know"), and certain information will logically fall into the special categories (e.g., Special Access Programs and Special Compartmented Information). Nevertheless, basic clearances—once granted by a competent authority—should be "portable" to the maximum extent possible.

- **That the President direct the development of a new regime of clearances and classification of intelligence and other information for dissemination to States, localities, and the private sector.** This new regime would remove some of the specific elements that raise the data to a traditional "national security" classification (e.g., sources and methods information) to provide the widest possible distribution to local and State responders and in a form that it conveys meaningful and useful information. Such a process could also prove to be less expensive and less time consuming for background investigations and the grant of clearances, as well as more effective in disseminating valuable intelligence. Furthermore, States could be empowered as managing partners by being "certified" to conduct background investigations. During his recent appearance before the panel, we asked the Attorney General if any thought had been given to such a new regime. He answered candidly that he did not know. With the urgent requirement to get information into the right hands in the most timely and effective way, we strongly believe that it is time for such a new system.

- **That DHS develop a training program for State and local officials and elements of the private sector for interpreting intelligence products.** Many State, local, and private sector officials have had limited if any practical experience in how to best use intelligence information. Most of these same officials, while not meteorologists, understand how to make operational decisions based on weather forecasts because they understand the inherent variables in the data. The same needs to be true with shared intelligence. How best to utilize important intelligence product is just as important as the product itself for sound decisionmaking.

In the information sharing arena, **we recommend that DHS establish comprehensive procedures, with definitive standards for the equipment and software vehicles, for sharing information with relevant State and local officials.** There is no central repository and clearinghouse for information related to combating terrorism. There are legacy systems that should be integrated and new ones that should be established.

Research and Development and Related Standards

The Department of Homeland Security has a substantial research and development role. In its second year of funding, it has a research and development budget request of 1.0 billion dollars, giving it the eighth largest research and development budget among Federal departments and

independent Federal research agencies. Research and development should not be limited to technology. There is a host of policy, organizational, and legal issues that need urgent attention.

The sudden and large commitment of resources to a new mission carries with it some important challenges. Chief among these challenges is for the Department of Homeland Security to organize and coordinate an effective research and development program amidst great uncertainty and across numerous operational needs. Moreover, DHS will have to contend with the challenges of implementing and coordinating research in an arena in which the organizations conducting research are almost entirely unrelated to the organizations that must implement the results of that research. Finally, Department of Homeland Security's research and development efforts will have to be developed mindful of the fact that substantial fractions of both the research and user communities largely are outside of the department.

Although DHS is given some R&D coordinating authority under the Homeland Security Act of 2002, that coordinating mechanism needs to be specified. **We recommend the formal establishment, by Executive Order of Presidential Decision Directive, of a Federal Interagency Homeland Security Research and Development Council, chaired by the Secretary of Homeland Security (or his designee) and with representatives of Federal R&D entities as well as end users.** Within that process, R&D should be categorized and prioritized across the entire Federal government, for internal (Federal laboratory) and external (contract and grant) programs. That process must also include input from end users at the State and local levels, and from the private sector, both on requirements and on the utility of developed and emerging technologies. Moreover, that process must include procedures for establishing national standards for equipment and technology, with government and private sector involvement.

Funding and Resources

Billions of Federal dollars are now flowing to State and localities. While these dollars will undoubtedly improve preparedness in many areas, the lack of a national implementation plan, standards, prioritization and clear guidance on objectives may be leading to ineffective application of these monies. We are poised to make measurable improvement in the nations readiness but only if we pursue a disciplined and deliberate approach that ensures at the end of the day that we have spent limited resources wisely and to the best ends.

The RAND survey found a positive relationship between receipt of funding and other resources since 9/11 and the assignment of a higher priority to spending departmental resources on terrorism preparedness. In particular, differences in priority between State and local organizations may reflect differences in the distribution and receipt of funding from the Federal government (as well as from other sources) following the 9/11 attacks. The initial influx of Federal funds focused on State governments (since in many cases they provide or fund public health services at the local level) and on bioterrorism preparedness. Differences in priority assigned to terrorism preparedness may partly reflect differences in organizational mission. For example, State organizations that have an overall emergency preparedness mission versus first-responder organizations, such as law enforcement or fire services, which have a broader public safety mission.

A recurring theme from State and local organizations was that they needed funding support for such activities as training and equipping, as well as for conducting risk assessments.

Organizations cited limited training and equipment procurement budgets, as well as competing or higher departmental budget priorities, as factors limiting their ability to purchase specialized equipment for terrorism preparedness and to participate in Federally sponsored training or equipment programs. Primarily, State and local organizations were looking toward DHS for financial support in these areas. (For more detailed survey information, see Appendix D.)

Prognostication about the amount of funding that the Federal government should provide in the near future is premature at best. Recent calls for the funding upward of $100 billion is, in our view, not the wisest approach. Federal funds have started to flow. Absent a more clear articulation of an end state, and the levels of preparedness sought to be achieved—with some reasonable way to measure our efforts—any attempt to establish an overall price tag is mere speculation and could be politically unwise. Moreover, we have consistently said that "one size doesn't fit all;" we should develop and implement a more logical process for improving capacity that just pushing increasingly more money into the system. We should evaluate efforts underway, continue to develop a better system of requirements generation, and refine priorities for funding along the way.

To ensure improving and continued preparedness the Federal Government should continue to provide sustained, assured levels of Federal funding, so that States and localities can plan and implement programs with both Federal and their own funding with more certainty about the funding available. One process could be multi-year funding that will allow States and communities to plan more effectively over time.[17] A finite time frame may be subject to adjustment because of another series of attacks. That being said, States and communities should also recognize that they should not expect a multi-year funding program to be extended as it nears it end and should resist the temptation to lobby accordingly unless there is a significantly compelling reason.

This funding should be provided through formula or other types of grants based on risk—threat *and* vulnerability considerations (where population is only one measure of vulnerability). Funding should not be based on consideration of vulnerability (or fear) alone. Performance measures must be established and evaluations conducted to ensure that funds are actually used wisely and are effectively improving or maintaining preparedness. As previously noted, risk based funding makes good practical sense but current threat and vulnerability data is not sufficient to implement such a process in the near term.

Psychological Preparedness

Preparing the nation for the psychological and behavioral consequences associated with terrorism involves more than just a strategic communication plan. Individuals not only need information and resources to help them understand and interpret the risks associated with terrorism, they need tools to help them prepare for and cope with the potential physical, psychological, and behavioral consequences associated with threatened and real acts of terrorism. This requires a broad, public health and education based model not only to inform and educate, but also to create community based resources for support or treatment. Such a community-based approach should involve not only public health officials and agencies, but

[17] The COPS program provides a useful example of States and communities ability to plan on sustained assistance over a five-year period.

must involve the private health care providers and other non-traditional health care and psychological support providers, including schools, local civic organizations, and the faith based community as active partners.

This community-based model will facilitate trust, enable better communication, and promote greater adherence to public health recommendations, while at the same time help in alleviating the psychological distress and potential negative behavioral consequences. Preparedness and response mechanisms must recognize that psychological distress and behavioral reactions are normal and will likely be common following a threatened or real event; yet not everyone will require a formalized mental health intervention. While not minimizing the importance of an evidence-based mental health response for those most in need, we must also recognize the need to address acute and long term psychological distress and behavioral reactions. For example, the nation's ability to respond effectively to a terrorist event will depend upon public cooperation. Yet, we know that following terrorist events, psychological distress and heightened anxiety can result in behavioral actions that will impede the response effort, including when individuals take unwarranted response actions (such as spontaneous evacuation or taking unnecessary medications). It also has significant economic implications, manifested in absenteeism and decreased productivity. The Panel heard compelling testimony on potential approaches to "shielding" the population during biological incidents. This concept recognizes that educating and informing citizens ahead of incidents could achieve higher compliance of protective measures while minimizing overall disruption to community life.

To address these issues and create comprehensive preparedness and response plans at all levels, Federal leadership is needed to indicate the importance of the psychological and behavioral readiness component by creating the funding opportunities for resiliency building and requiring accountability for State and local public health agencies to design and implement programs based on evidence. In a recent report, an Institute of Medicine committee established specifically to consider these issues made several cogent recommendations for limiting the psychological consequences of terrorism during all phases of a terrorism event, including before an event occurs.[18] First, they recommended that DHHS (including NIH, SAMHSA, and CDC) develop evidence based techniques, training and education in psychological first aid to address all hazards and all members of society and that the same develop public health surveillance and methods for applying the findings of this surveillance through appropriate interventions for groups of special interest. Further they recommended that academic healthcare centers, professional associations and societies for mental health professionals, and state board of education, in collaboration with DHHS (including SAMHSA, NIH, and CDC), ensure the education and training of mental health care providers, including community- and school-based mental health care providers, relevant professionals in health fields, including primary care providers, school-based health care providers, public health officials, and the public safety sector, and a range of relevant community leaders and ancillary providers. In addition, the Committee recommended that NIOSH, the Department of Labor, and the Department of Education ensure the existence of appropriate guidelines to protect workers in a variety of work environments; that Federal agencies should coordinate research agendas, cooperate in establishing funding mechanisms, and award timely and sufficient funding on best practices for

[18] National Academy of Sciences, Institute of Medicine (2003) Preparing for the Psychological Consequences of Terrorism: A Public Health Strategy. Butler, Panzer, and Goldfrank, Editors. National Academies Press, Washington, DC

interventions; and that DHHS and DHS analyze terrorism preparedness to ensure that the public health infrastructure is prepared to respond. Finally, the Committee suggested that Federal, state, and local disaster planners should address psychological consequences in their planning and preparedness and resources.

We recommend:

1. **Implementation of the IOM Committee's recommendations**
2. **That Congress provide increased funding to DHS and DHHS for States and local agencies, and that DHS and DHHS require and monitor State and local compliance of incorporating in plans an appropriate focus on psychological and behavioral consequence preparedness and management**
3. **That DHS and DHHS create a Federal joint task force on these issues**

Agroterrorism

To date, terrorists have not yet successfully carried out or even attempted (as far as we know) a large-scale agricultural attack. Yet, attacks against agriculture could emerge as a favored form of secondary aggression. A major terrorist attack on the U.S. agricultural sector would have serious economic impact and could undermine the public's confidence in government. Further, if the disease were transmissible to humans, there could be significant adverse public health consequences. The agricultural sector is vulnerable to deliberate and natural introductions of disease for several reasons,[19] all the more threatening because the capabilities required for exploiting them are not significant.

If an attack were perpetrated, emergency assistance funds for crop and livestock disease outbreaks are nearly non-existent. The Terrorism Risk Insurance Act of 2002 specifically excludes crop and livestock from Federal compensation programs from insured losses. The USDA simply advises producers to purchase private insurance as their primary risk management strategy. Emergency compensation for livestock established under the 21 U.S. Code Chapter 4 (on seizure, quarantine, and disposal of livestock or poultry to guard against introduction or dissemination of communicable disease) requires the USDA to compensate owners of any animal, carcass, product, or article destroyed within a quarantine zone at the fair market value of the destroyed asset but does not account for the significant losses caused by decontamination, lost income, and reduced production capacity. On the crop side, the Agriculture Risk Protection Act of 2000 gives the Secretary of Agriculture the "ability to prohibit or restrict the importation, exportation, and the interstate movement of plants, plant products, certain biological control organisms, noxious weeds, and plant pests." If implemented, the Act only provides the Secretary with the *option* to provide compensation for economic losses.

USDA is, nevertheless making changes to meet these challenges,[20] including:

- The formation of a Homeland Security Council,

[19]The vulnerabilities are taken directly from *Hitting America's Soft Underbelly: The Potential Threat of Deliberate Biological Attacks Against the U.S. Agricultural and Food Industry*, Peter Chalk, MG-135-OSD (Santa Monica, CA: RAND, 2004).

[20]This information is taken from Secretary of Agriculture Ann Veneman's Statement to Panel September 9, 2003 at Appendix M.

- The institution of a dedicated Homeland Security Staff,
- The implementation of the "Select Agents Rule,"[21] and
- A pilot program for the National Animal Health Laboratory Network (NAHLN).[22]

USDA has also developed guidance on communications for State and local partners; upgraded security systems in the field offices; and enhanced training. For food supply protection, USDA has participated in drills to enhance government response coordination; conducted threat and vulnerability assessments; moved to develop an integrated food security plan; increased bio-security testing and surveillance measures; enhanced physical security and diagnostic capacities at laboratories; and implemented Consumer Complaint Monitoring. USDA has also addressed USDA Laboratory security including pathogen control and cyber security. It is implementing a USDA National Incident Management System in conjunction with DHS.

USDA plans to expand laboratory networks, increase lab security, improve diagnostic, prevention, and treatment capabilities; expand the plant lab network through standard operating procedures and inter-regional communication and by creating a national monitoring database. In addition, USDA plans to hire 80 additional field inspectors; increase on-site farm checks; improve communication with the private sector; and coordinate efforts with DHHS and DHS.

Although these efforts represent a first step, several areas require increased attention. Measures need to be undertaken to create a partnership of Federal, State, local and private sector entities to secure the industry from deliberate disruption and sabotage. These initiatives would also have the dual-use benefit of strengthening overall prevention and response efforts in relation to naturally-occurring disease outbreaks. While USDA is increasing personnel, a 1% increase in inspectors is unlikely to make a significant difference given the thousands of agricultural facilities in the United States. Other issues include insufficient personnel and laboratory capacity, such as appropriately secured disease research laboratories (the USDA still lacks any BSL-4 facilities),[23] and too few veterinarians trained to diagnose and treat foreign/exotic animal pathogens. Coordination and standardization with State, local, and private participants in the agricultural sector is still lacking and forensic and information collaboration with relevant members of the intelligence and criminal justice communities remains inadequate. Added to these problems is inconsistent food surveillance and inspections at processing and packing plants and an emergency response program that is limited by an unreliable passive disease-reporting system and a lack of trust between regulators and producers.

To address these shortcomings, **we recommend that the President designate DHS as the lead and USDA as the technical advisor on all homeland security issues regarding food safety and agriculture and emergency preparedness across the full spectrum of activities from awareness through response and recovery.**

Both DHS and USDA must foster better cooperation among states and producers. USDA should work to prioritize R&D and security resources; further increase the number and capabilities of

[21] 7 CFR part 331 and 9 CFR part 121, Possession, Use, and Transfer of Biological Agents and Toxins, mandated by the Agricultural Bioterrorism Protection Act of 2002.
[22] The NAHLN designates the National Veterinary Services Laboratory as the lead animal health laboratory and allows selected State and academic laboratories to work in foreign animal disease surveillance and related services.
[23] In the panel's *Fourth Report*, Plum Island was mistakenly identified as a BSL-4 facility; it is BSL-3.

Federal, State, and local personnel with the skills to identify/treat exotic foreign animal diseases; foster more coordinated and standardized links with the intelligence and law enforcement communities; review the effectiveness of the passive disease reporting system through Federal and State outreach, information, and indemnity programs; and evaluate the short-term cost versus long-term benefit of upgrading biosecurity at food processing and packing plants. Over the longer-term, a national strategy must include processes to standardize and integrate food supply and agricultural safety measures within Federal, State, and local agencies and the private sector.[24]

Role of the Military

The potential for serious infringement of liberties stemming from the domestic deployment of troops could be significantly reduced by the development of Rules for the Use of Force for activities inside the United States and its territories; rigorous training; and publicly articulated standards and procedures for determining when the military is conducting a military operation in its homeland defense role and when it is conducting law enforcement activities. These issues need to be fully discussed in the public arena so that the American people understand and are prepared for the military's intervention, should that become necessary.

Furthermore, there should be a well coordinated, clearly defined set of roles and missions for the military, including the National Guard, where the military is expected to support State and local government in response to terrorism, as well as other hazards. Ideally, civilian response capabilities will be improved to such an extent that there will be minimal requirements for the military to provide support to civil authorities. As a result, both the active and reserve components can concentrate on traditional military missions. In the meantime, in the broader scheme of Federal funding for support to States and localities, near-term military roles and missions should not detract from enhanced funding, training, and equipping for State and local responders.

Congress should consider working with the Administration to develop, in statute as supplemented by Executive Order, new guidelines and procedures for domestic intelligence collection by the military. Definitions may need to be revisited, or additional safeguards added, in order to address the challenges of this unconventional war.

[24] In part from *Hitting America's Soft Underbelly: The Potential Threat of Deliberate Biological Attacks Against the U.S. Agricultural and Food Industry*, Peter Chalk, MG-135-OSD, 2004.

CONCLUSION

This panel firmly believes that it has contributed materially to the national debate and has been instrumental in advancing homeland security dialogue and action across the nation. Over the five years of its tenure, we were able to consider the fundamental challenges of combating terrorism, making comprehensive findings and recommendations both prior and subsequent to September 11. Our work is reflected in many of the advances the nation has made in recent years.

We complete our work with a great sense of pride. We thank all of those who have contributed to our efforts. We believe our work reflects the hope and desire of every American for a more secure homeland—one that also preserves our essential liberty in the process.

The panel recognizes that its responsibility transcends the completion of this effort and should empower other similar entities to take significant steps to make the shared goal of a safer and more secure America a reality. Accordingly, we are providing a copy of this report and our four previous reports to the National Commission on Terrorist Attacks Upon the United States (also known as the "9-11 Commission") with the hope that it will measurably assist and inform their efforts.

Our duties now completed, the panel members, individually and collectively, recognize that we must remain resolute in our efforts to achieve a more secure homeland. The tragedy of September 11th remains a vivid image, especially the loss of our friend and fellow panel member Chief Ray Downey and the thousands of others who died that day—a compelling reminder of the importance of our work. We are reminded of the ancient Athenian saying: "The true statesman is one who plants a tree knowing he will never personally enjoy its shade."

We now entrust our work to the thousands of dedicated Americans in and out of government who are working tirelessly every day to attain these laudable and noble goals.

TABLE OF APPENDICES

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

Current Members	Expertise
James S. Gilmore, III, Attorney at Law, and former Governor of the Commonwealth of Virginia, Chairman	State government
George Foresman, Deputy Director, Office of Commonwealth Preparedness, Commonwealth of Virginia, Vice Chairman	Emergency response—State
L. Paul Bremer, Presidential Envoy and Administrator of the Coalition Provisional Authority in Iraq; Former Ambassador-at-Large for Counter-Terrorism, U.S. Department of State *(Member until May 5, 2003)*	Counterterrorism
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, University Assistant Professor, 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

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

John Lombardi, U.S. Department of Defense Alternative 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), former panel Vice Chairman; Director, National Imagery and Mapping Administration; former Director, Defense Intelligence Agency

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 ***(Killed in the Line of Duty, New York City, September 11, 2001)***

John Gannon, Staff Director, Select Committee on Homeland Security, U.S. House of Representatives; former Deputy Director of Central Intelligence; and former Chairman, National Intelligence Council

Joseph Samuels, Jr., Chief of Police, Richmond, California, and Immediate Past President, International Association of Chief of Police

JAMES S. GILMORE III—CHAIRMAN

Jim Gilmore is a former Governor of Virginia (1998-2002) and a partner at the law firm of Kelley Drye and Warren, where he practices corporate and technology law, and counsels clients on homeland security matters. He received his undergraduate degree from the University of Virginia and attended the University of Virginia Law School, from which he graduated in 1977. Gilmore worked for over a decade as a lawyer in a private practice. In 1993, Mr. Gilmore was elected Virginia Attorney General, a post that he held until his election as Governor in 1997. Gilmore has been the Chairman of the Congressional Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction since its inception in 1999. He also chaired the national Advisory Commission on Electronic Commerce, which was charged with making recommendations to Congress on Internet taxation. He was appointed by President Bush to serve on the Board of Visitors of the United States Air Force Academy, and was elected President of the Board by the members. He is a Distinguished Fellow at the Heritage Foundation.

GEORGE WILLIAMSON FORESMAN—VICE CHAIRMAN

George Foresman currently holds the Cabinet rank post of Deputy Assistant to the Governor for Commonwealth Preparedness for the Commonwealth of Virginia, appointed by Governor Mark Warner in January 2002, and is responsible for ensuring Virginia's preparedness for emergencies and disasters of all kinds, including terrorism. He is also responsible for Continuity of Operations and Continuity of Government activities and serves as special liaison for the Governor with Virginia's military installations and commands. Previously, Foresman was appointed by former Governor James S. Gilmore to the post of Deputy State Coordinator of Emergency Management. In 1985, he joined the Virginia Department of Emergency Management where he did work with disaster grants management, local and state planning, risk and hazard reduction, special projects, intergovernmental relations and operations. Together, Foresman has nearly twenty years of local and state level public safety response and executive leadership experience. He is nationally recognized as an expert on emergency preparedness, homeland security and government management issues and active with numerous national and state associations. He is a graduate of the Virginia Military Institute.

L. PAUL BREMER, III

Jerry Bremer was named Presidential Envoy to Iraq on May 6, 2003 and in this capacity is the Administrator of the Coalition Provisional Authority. Until that appointment, he had been a member of the Advisory Panel since its inception in 1999. Bremer served as Chairman and Chief Executive Officer of the Marsh Crisis Consulting Company until May 2003. From 1989 to 2000, he was Managing Director of Kissinger Associates, headed by former Secretary of State Henry Kissinger. Bremer spent 23 years in the U.S. State Department, serving in embassies in Afghanistan, Malawi, Norway and the Netherlands. President Reagan named him Ambassador to the Netherlands in 1983 where he served for three years. Ambassador Bremer also served as President Reagan's Ambassador-at-Large for Counter Terrorism. In 1999, Ambassador Bremer was appointed Chairman of the National Commission on Terrorism. Ambassador Bremer was also appointed to the President's Homeland Security Advisory Council in June 2002.

P. MICHAEL FREEMAN

Michael Freeman is the Fire Chief of the Los Angeles County Fire Department, a position he has held since February of 1989. The Department provides fire protection and emergency medical services to more than 3 million residents in 2,200 square miles and 57 cities within the County of Los Angeles. Chief Freeman has successfully led the Department through numerous large-scale emergencies, including the 1993 brush fires and the 1994 Northridge Earthquake, and most recently, the 2003 Fire Siege. Under his leadership, the Department has grown with the addition of specialized services including Urban Search and Rescue, Swiftwater Response Teams, and state-of-the-art Firehawk helicopters. Chief Freeman majored in Business and Personnel Management at Southern Methodist University in Dallas, Texas. He is the Chairman of the FIRESCOPE Board of Directors; a member of the Federal Emergency Management Agency's National Urban Search and Rescue (USAR) Advisory Committee; Chairman of the International Association of Fire Chiefs Terrorism Committee; and mutual aid coordinator for a five-county area in Southern California. Chief Freeman also serves on the Department of Homeland Security Emergency Response Senior Advisory Committee.

MAJOR GENERAL (RET) WILLIAM F. GARRISON

Bill Garrison, a retired U.S. Army Major General, has over thirty years of direct experience involving terrorism, intelligence, security management, emergency response training, and tactical operations. Garrison was a member of the U.S. Army's Special Forces and commanded the Delta Force. Currently, Garrison supports the U.S. State Department's Antiterrorism Training Assistant Program (ATAP), the Department of Justice International Criminal Investigation Training and Assistance Program (ICITAP), and the Department of Energy Defense Program's for Emergency Response. He has extensive experience in conduction intelligence assessments and managing intelligence operations, combined with training management and tactical responses to threat scenarios.

ELLEN M. GORDON

Ellen Gordon, who has held the position of Administrator of Iowa Emergency Management Division since July 1986, was additionally appointed as Iowa Homeland Security Advisor in October 2001. In this post, she has led the State of Iowa through numerous State disasters, including the United Airlines 232 Crash in Sioux City, the most costly and widespread flooding disaster in the State's history, severe ice storms, tornadoes and the State's largest chemical release incident. Prior to her appointment at the State level, Gordon had eight years of local government emergency management experience. Ms. Gordon is a Past-President of the National Emergency Management Association after serving several years as a NEMA Regional Vice President. She now sits as the head of the NEMA Homeland Security Committee. Gordon is also a former member of the Harvard University Kennedy School of Government Executive Session on Domestic Preparedness and a member of the Iowa Emergency Response Commission.

JAMES W. GREENLEAF

For more than twenty-six years, James Greenleaf served the FBI in positions in Virginia, Minnesota, Washington, DC, Illinois, Massachusetts and London, England. After completing his training at Quantico, Virginia he served in Minneapolis, Norfolk, Virginia, and Washington, DC. Greenleaf then held the position of Assistant Special Agent in Charge in Chicago. In 1981, he was placed in charge of the FBI's Inspection Division. From 1982 to 1986, Greenleaf was the Special Agent in Charge of the Boston Field Office. After this post, Greenleaf was named FBI Assistant Director in Charge of Training and Director of the FBI Academy. In 1989, the Director of the Central Intelligence Agency appointed Greenleaf CIA Director of Public Affairs. He returned to the FBI in 1990, as Associate Deputy Director for Administration. In 1992, Greenleaf was assigned as the Legal Attaché in London where he remained until his retirement in July 1994. Since his retirement, Greenleaf has worked as a consultant to NBC Television and to the Laborers' International Union of North America, assisting the Union in its efforts to rid itself of organized crime influences.

DR. WILLIAM F. JENAWAY

Dr. William Jenaway has spent over thirty years as a field specialist in the area of insurance risk control and risk management. Currently, Jenaway holds the position of Executive Vice President of VFIS, the country's largest insurer of emergency service organizations. Jenaway holds AS, BS, MA and PhD Degrees, and has authored seven books and published over 200 magazine articles. Jenaway has been a member of the volunteer fire services in his hometown of King of Prussia, Pennsylvania for almost thirty years, including holding the position of Chief of Fire and Rescue Services. He is an expert in Fire Service Risk Management and Disaster and Emergency Planning, and has served as the Chairman of the Risk Management Committee of the National Fire Protection Association, and as President of the Congressional Fire Services Institute. Jenaway is also an adjunct professor of Risk Analysis and Disaster Management in the graduate school of St. Joseph's University in Philadelphia.

WILLIAM DALLAS JONES

For the past five years, Dallas Jones has been the Director of the California Governor's Office of Emergency Services (OES). He has directed state emergency response and recovery operations for numerous disasters, including a severe freeze, two serious earthquakes, and several wildfires, including the recent 2003 South California Fire Siege. Since the September 11th attacks, Mr. Jones has directed California's anti-terrorism planning, preparedness, and response operations. He is also Chairman of the California Emergency Council and the Governor's School Violence Prevention and Response Task Force. Additionally, Jones serves as the Vice President for the National Emergency Management Association (NEMA)'s Region IX, as well as the Director of the Western States Seismic Policy Council (WSSPC). Prior to his position at the State level, Jones served for 32 years with the Los Angeles County Fire Department, 16 years of which he was the President of the Los Angeles County Fire Fighters. Jones also served as Vice President of both the California Labor Federation and the Los Angeles County Federation of Labor.

PAUL M. MANISCALCO

Paul M. Maniscalco (MPA, EMT/P) is an Assistant Professor with The George Washington University School of Medicine and Health Sciences. Maniscalco is an active member of the National Association of Emergency Medical Technicians (NAEMT), a current member of its Board of Directors and a NAEMT Past President. Maniscalco is also Chairman of the NAEMT National EMS Administrators Division. For over twenty-nine years, Maniscalco has been working in the areas of public safety emergency response, planning, training, supervision and management. During this tenure he rose through the ranks of the City of New York EMS & FDNY to Deputy Chief /Paramedic. As an academic, Maniscalco has many published works on the Emergency Medical Service, fire service, management, special operations, terrorism, public safety, and national security issues.

JOHN O. MARSH, JR.

Jack Marsh is a native of Virginia. He enlisted in the United States Army in WWII and received a commission at age 19 by graduation from Infantry Officer Candidate School. A graduate in Law from Washington and Lee University, he practiced in Strasburg, Virginia until elected to the 88th Congress in 1962, where he served four terms. He was a member of the House Appropriations Committee. Choosing not to seek a fifth term, he resumed the practice of law. In 1973 he returned to Federal service holding the positions of Assistant Secretary of Defense (Legislative Affairs), Assistant for National Security Affairs to Vice-President Ford, and later Counsellor, with Cabinet Rank, to President Ford. He chaired for President Ford the special cabinet level panel that recommended to the President measures for the reorganization and reform of U. S. intelligence community. In 1981, Marsh was sworn in as Secretary of the Army, a position he held for over eight years, to become the longest serving military Secretary in U. S. history. After WWII service, he joined the Virginia National Guard, retiring after twenty-three years of Guard service. Marsh is currently a Distinguished Professor of Law at George Mason University where he teaches in the field of Cyber issues and National Security Law.

KATHLEEN O'BRIEN

As vice president for University Services at the University of Minnesota, Kathleen O'Brien serves as an innovative executive who provides strategic direction and strong execution. Under her leadership, nearly 3,000 employees have undergone a reorganization that has brought a new level of accountability, more effective management systems, and a renewed emphasis on customer service to the organization. University Services, with a $300 million annual operating budget includes units and departments such as: Facilities Management, Capital Planning and Project Management, Auxiliary Services, Public Safety, Environmental Health and the Building Code Officials. Currently, O'Brien leads several University committees, including the President's Initiative on Sustainability, the Capital Oversight Group, and University Master Plan Update. From 1994 to 2002, O'Brien served as City Coordinator for the City of Minneapolis, Minnesota, where she oversaw a $75 million annual budget and 800 full-time employees. O'Brien was instrumental in the success of several major projects including the Convention Center Expansion, the Empowerment Zone and the new Central Library. O'Brien served as Chief of Staff for University of Minnesota President Nils Hasselmo from 1989 to 1994. Elected to the Minneapolis City Council in 1982, O'Brien represented the city's Second Ward and University community for seven and a half years. Kathleen O'Brien is a 1967 graduate of the College of St. Catherine in St. Paul, received a Masters of Arts Degree from Marquette University in Milwaukee and completed coursework toward a PhD in history at the University of Minnesota.

DR. PATRICIA QUINLISK

Dr. Quinlisk is a medical epidemiologist practicing at the Iowa Department of Public Health where she also holds the position of Medical Director and the State Epidemiologist. Her background includes training as a clinical microbiologist, training microbiologists while a Peace Corps Volunteer in Nepal, a Masters of Public Health from Johns Hopkins with an emphasis in infectious disease epidemiology, medical school at the University of Wisconsin, and training as a field epidemiologist in the Centers for Disease Control and Prevention's Epidemic Intelligence Service. Yearly, for the last ten years, she has conducted weeklong epidemiologic training courses in Europe and teaches regularly at the University of Iowa, Des Moines University, Iowa State University and other educational institutes throughout the Midwest. Dr. Quinlisk serves or has served on a number of national advisory committees including the National Vaccine Advisory Committee, the U.S. Marine Corps Chemical/Biological Incident Response Force, the DOD's Gilmore Commission, on various Institute of Medicine committees and as President of the Council of State and Territorial Epidemiologists (CSTE). Recently, she was named to the Board of Scientific Counselors for the National Center for Infectious Diseases, Centers for Disease Control and Prevention.

PATRICK RALSTON

Since 1997, Pat Ralston has served the State of Indiana as the Executive Director of State Emergency Management Agency (SEMA), State Fire Marshal, State Building Commissioner and Chairman of the Board of the Public Safety Training Institute. In addition to his duties as Executive Director, Ralston serves as Chairman of the Indiana Emergency Response Commission, sits on the Governor's Council for Impaired Driving, acts as Secretary for the Emergency Medical Commission, is a member of the Board of Fire Fighters Personnel Standards and Education and serves as Chairman of the Board of the Central United States Earthquake Consortium. Prior to his work with SEMA, Ralston served as Director of the Indiana Department of Natural Resources from 1989-1997. He was recently appointed by the National Emergency Management Association to represent State emergency management directors on the board of the National Memorial Institute for the Prevention of Terrorism in Oklahoma City.

WILLIAM H. RENO

Bill Reno is the Chief Executive Officer of the Wexford Group International, an international consulting company (www.thewexfordgroup.com). The company specializes in high impact consulting in program management, contract management, human resources, and applications of high technology to military problem solving. It works extensively in former Warsaw Pact countries to transform their Armed Forces into Western Models. Before his work with this group, Reno was the Senior Vice-President of National Operations for the American Red Cross, a position that he held from 1992-1997. In this post, Mr. Reno was responsible for all financial management, human resources, contract management, audit and coordination of programs across the departments within the institution. From 1990-1992, Reno held the post of Deputy Chief of Staff for Personnel for the United States Army, responsible for plans, policies and programs for the management of all military and civilian personnel of U.S. Army Active and Reserve Component forces.

KENNETH I. SHINE

Ken Shine, the former President of the Institute of Medicine (IOM) and the founding Director of the RAND Center for Domestic and International Health Security, was named the Executive Vice Chancellor for Health Affairs at the University of Texas in November of 2003. At RAND, Dr. Shine led the Center's efforts to make health a central component of U.S. foreign policy and guide the Center's evolving research agenda. Under Dr. Shine's leadership, the IOM played an important and visible role in addressing key issues in medicine and healthcare. Prior to his work at the IOM, Dr. Shine was Chairman of the Council of Deans of the Association of American Medical Colleges from 1991-1992 and was President of the American Heart Association from 1985-1986.

ALAN DENNIS (A.D.) VICKERY

A.D. Vickery, a 38-year veteran of the Seattle Fire Department, currently holds the rank of Deputy Chief of Safety and Homeland Security. During his tenure with the Department, he has worked on both combat and administrative positions, covering the entire spectrum of fire service responsibilities. In 1992, the Seattle Fire Department became a participant in the national FEMA Urban Search and Rescue program and Vickery was appointed a Rescue Team Manager, where he worked to improve regional and local capability to respond to catastrophic events. In 1994, Vickery became a Task Force Leader of the Washington State Team, a position that he retains to this day. Chief Vickery has been deployed to numerous national emergencies including the terrorist attacks in Oklahoma City and the 9-11 World Trade Center attack. He is Chairman of the Puget Sound Marine Fire Fighting Commission, Co-Chair of the State of Washington Committee on Terrorism Equipment Workgroup and active nationally on Fire, HazMat, EMS as well as law enforcement first responder issues. Chief Vickery is currently the elected Chair of the national InterAgency Board for Equipment Standardization and Interoperability (IAB).

HUBERT WILLIAMS

Hubert Williams, a thirty-year veteran of policing, is the president of the Police Foundation, a nonpartisan, nonprofit organization dedicated to supporting innovation and improvement in policing. He has been a leading advocate for professional standards and uniform practices in policing, and has presided over the design and implementation of scientific field experiments that are on the leading edge of the development of modern police policy and procedure. From 1974-1985, Mr. Williams was the police director in Newark, New Jersey, the largest police department in the state during a time in which inner-city deterioration, civil unrest, and drug-related crime plagued most of the nation's urban areas. His experience in the civil disorders in Newark and his leadership as president of the Police Foundation prompted the City of Los Angeles to appoint him as deputy special advisor to the Los Angeles Police Commission in the evaluation of the police response to the civil disorder in that city during 1992. Williams has also published various texts on the subject of policing.

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.

Major General (Ret) Richard Alexander
National Guard Association of the United States

Lt. Col. Mark G. Allen
National Guard Bureau

Graham Allison, Ph.D.
Harvard University

Tom Antush
Transportation Security Administration

Ann Beauchesne
National Governors Association

Richard Behrenhausen
McCormick Tribune Foundation

Peter Beering
US Filter

Eugene Bowman, J.D., LL.M.
Federal Bureau of Investigation

Paul Boyd
Terrorist Threat Integration Center

Captain Rodney Bullard
U.S. Air Force

Sam Brinkley
Department of State

Michael Byrne
Department of Homeland Security

F. Marion Cain III
Office for Domestic Preparedness

Stephen L. Caldwell
General Accounting Office

Richard Callis
Emergency Management Institute

Frank Cilluffo
Executive Office of the President

Rudy Cohen
Office of the Secretary of Defense

Brian Cowan
Federal Emergency Management Agency

Hank Christian
Unconventional Concepts

Willie Curtis
U.S. Naval Academy

Darrell Darnell
Office for Domestic Preparedness

Raymond Decker
General Accounting Office

Scott Deitchman, M.D.
American Medical Association

Rebecca Denlinger
Cobb County Georgia Fire Department

Captain Daniel Donovan
U.S. Navy

William W. Ellis
Congressional Research Service

Eugene Fidell
National Institute of Military Justice

Glenn Fiedelholtz
SAIC

Jack Fenimore
Major General, U.S. Army (Ret.)

Richard Friedman, J.D.
National Strategy Forum

David Grange
McCormick Tribune Foundation

Don Hamilton
Memorial Institute for the Prevention of Terrorism

David Hamon
Defense Threat Reduction Agency

Paul Hankins
Transportation Security Administration

Major General David Harris
Adjutant General of Illinois

Francis Hartmann
Harvard University

Jane Hindmarsh
California Governor's Office of Emergency Services

Arnold Howitt, Ph.D.
Harvard University

Lieutenant Colonel Gregory Huckabee
U.S. Army

Barbara Kambouris
Federal Emergency Management Agency

Dan Kaniewski
George Washington University

Juliette Kayyem, J.D.
Harvard University

Thomas Kneir
Federal Bureau of Investigation

Peter LaPorte
Emergency Management Agency
District of Columbia

Bruce Lawlor
Department of Homeland Security

Scott Layne, M.D.
University of California at Los Angeles

Marcelle Layton, M.D.
New York City Department of Health

Timothy Lowenberg
Adjutant General
State of Washington

Gene Matthews, J.D.
Centers for Disease Control and Prevention
Department of Health and Human Services

The Honorable Edwin Meese
The Heritage Foundation

Judith Miller
Williams & Connolly
Major General Paul Monroe, Jr.
California National Guard

R. Nicholas Palarino,
Subcommittee on National Security,
Veterans Affairs, and International
Relations
U.S. House of Representatives

Elizabeth Rindskopf Parker
University of the Pacific

Ann Petersen, J.D.

Charles Ramsey
Metropolitan Police Department
Washington, DC

Colonel Ronald Reed
U.S. Air Force

Dennis Reimer
Memorial Institute for the Prevention of Terrorism

Ford Rowan
Rown & Blewitt

Gregory Saathof, MD
University of Virginia

Senior Official
Canadian Security Intelligence Service (CSIS)

Senior Official
Australian Security Intelligence Organisation (ASIO)

Senior Official
Australian Federal Police (AFP)

Senior Official
Los Angeles Police Department

Senior Official
Strategic and Defense Studies Centre (SDSC)
Australian National University

The Honorable Jeff Sessions
United States Senate

Stephen Sharro
Emergency Management Institute

Brendan Shields
Department of Homeland Security

Scott Silliman
Duke University

Amy Smithson
The Henry L. Stimson Center

Brigadier General Annette Sobel
National Guard Bureau

Robert Stephan
Department of Homeland Security

Darrel Stephens, Charlotte-Mecklenburg North Carolina Police Department

Jessica Stern
Harvard University

Paul Schott Stevens
Dechert LLP

Patrick Sullivan
Cherry Creek Colorado Schools

John Sullivan
Los Angeles Sheriff's Department

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

Winston Wiley
Terrorist Threat Integration Center

John Allen Williams
Loyola University Chicago

Randy Williamson
Government Accounting Office

Frances Edwards-Winslow
San Jose California Office of Emergency Services

James Woolsey
Attorney at Law

Lee Zeichner
LegalNetWorks

The Honorable James Ziglar
Commissioner
Immigration and Naturalization Service

APPENDIX D—SUMMARY OF SELECTED SURVEY RESULTS[25]

Introduction

Since the 9/11 attacks on the World Trade Center and Pentagon, State and local governments and response organizations have focused their attention on preparing for, and responding to, acts of domestic terrorism. Of particular concern has been improving State and local response capabilities to deal with terrorist incidents involving weapons of mass destruction (WMD), such as the use of biological, radiological, or chemical weapons. Much activity has focused on what the Federal government itself can do to better support the efforts of State and local organizations in the war on terrorism.

The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (otherwise known as the Gilmore Commission), which was established by Congress on October 17, 1998, has been evaluating the progress of Federal preparedness programs for local emergency response and recommending strategies for effective coordination of preparedness and response efforts between Federal, State, and local government and response organizations.

As part of its support for this effort, and just prior to the 9/11 terrorist attacks, RAND conducted the first wave of a nationwide survey to gather in-depth data about States and local response organizations' assessments of Federal preparedness programs for combating terrorism. Two other survey waves were conducted in 2002 and 2003. Taken together, the survey waves have gathered in-depth data, beginning just prior to the 9/11 terrorist attacks up through the Fall of 2003, on the planning and preparedness activities of the key professional communities involved in preparedness and emergency response: law enforcement, fire service, office of emergency management (OEM), emergency medical services (EMS), hospitals, and public health.

We present here a selected summary of the findings from the third wave of the nationwide survey of State and local response organizations—*Survey III of Federal Preparedness Programs For Combating Terrorism*—conducted in 2003. The report is organized around five key issues of interest to the Advisory Panel: (1) intelligence, information, and warning; (2) which incident types State and local organizations consider preparations most important for; (3) organizations' views about funding support needs and the association between receipt of funding and preparedness activities; (4) differences between State and local organizations in their participation in Federal programs and expectations of the Federal government; and (5) involvement of organizations with the private sector. Tab 1 provides a summary of the survey methods and response rates.

Organizations want more intelligence about the terrorist threat, but security clearances are lagging

State and local organizations are looking to the Department of Homeland Security (DHS) for intelligence information and information about the terrorist threat within their jurisdiction or State is one of the areas that. Organizations also want more detailed information on the threat and on terrorist capabilities to help them in conducting risk assessments. In addition, organizations had a number of suggestions for improving the Homeland Advisory System. Between 60-70 percent of State and local organizations suggested providing additional information about the threat (type of incident likely to occur, where the threat is likely to occur, and during what time period) to help guide them in responding to changes in the threat level. Other suggestions for improving the Homeland Advisory System included: (1) using a regional alert system to notify emergency responders about threats specific to their jurisdiction/State; (2) providing training to emergency responders about what protective actions are necessary at different threat

[25] Lois M. Davis, Louis T. Mariano, Jennifer Pace, Sarah K. Cotton, and Paul Steinberg. Tabs 1 and 5 are largely based upon RAND PM-1236-OSD, *Sampling Design, Respondent Selection, and Construction of Survey Weights for the Federal Weapons of Mass Destruction Preparedness Programs Survey,* by Jerry Jacobson, Ronald Fricker, and Lois Davis (August 2001).

levels; and (3) after an increase in threat level, having DHS follow-up on what additional actions ought to be taken.[26]

Since September 11, 2001, about half of law enforcement and half of local and State OEMs have received guidance from the FBI about what type of information about suspected terrorist activity should be collected and/or passed onto FBI field offices. In comparison, only a quarter of paid/combination fire departments and hospitals and only a few volunteer fire departments indicated they have received such guidance.

Despite a desire for more detailed intelligence information since the 9/11 terrorist attacks, State OEMs and State public health departments are primarily the organizations that have sought security clearances for their personnel (Table 1). This finding is likely related to recent requests by DHS and the Department of Health and Human Services (DHHS) for States to apply for such clearances for their senior officials. To date, only about half of State OEMs and a third of State public health departments that applied for security clearances have received them for at least some of their personnel.

Because the survey did not ask when organizations had applied for government security clearances, we cannot distinguish between those who may have applied only recently versus those that have been waiting for a longer period of time. Regardless, there appears to be a mismatch between the desire for more intelligence information versus ability to access such information. Recently, DHS announced that in addition to the State governors, five senior officials within each State would be issued security clearances to receive classified information and to allow governors to obtain intelligence information Federal agencies may have about specific threats or targets. (These clearances are in addition to the security clearances to be issued to public health officials).[27] However, there is a concern among some State officials that the number of security clearances allocated may be too few to account for all their needs.

Table 1. How Many Organizations Have Applied for and Received Security Clearances Since 9/11?

Organization Type	Has Organization Applied for Security Clearance(s) Since 9/11? (% of All Orgs)	Of Those Organizations That Applied, How Many of Their Personnel Have Received Clearances? (% of Those Orgs That Applied)		
		All	Some	None
Local Response Organizations				
Law Enforcement	7 (2)	56 (15)	25 (13)	19 (11)
Local/Regional EMS*	5 (2)	33 (33)	33 (33)	34 (33)
Local OEM	6 (2)	60 (18)	30 (15)	10 (8)
Paid/Combo Fire	2 (1)	89 (10)	6 (8)	5 (4)
Volunteer Fire	0 (0)	--	--	--
State Organizations				
State EMS	16 (4)	0	40 (23)	60 (23)
State OEM	88 (4)	9 (4)	48 (8)	43 (8)
Health Organizations				
Hospital	6 (3)	70 (32)	30 (32)	0
Local Public Health	8 (4)	97 (3)	1 (1)	3 (3)
State Public Health	86 (3)	10 (3)	30 (5)	60 (6)

Standard error of the estimate is shown in parentheses. Dashes in the table indicate that a particular organizational type either was not asked the question or given a particular response option. . *Local/ regional EMS organizations were not selected randomly. We display standard errors for this group throughout this document so that the reader may gain a broader sense about the variability of these responses (on the same metric as the other organization types). However, generalizations of these results to a population broader than those local/regional EMS organizations that responded to the survey should not be inferred.

[26] 60-70 percent of State and local organizations listed these additional recommendations for improving the advisory system.
[27] DHS Office of the Press Secretary, August 18, 2003. "Secretary Ridge Addresses National Governors Association".

Incidents considered important to prepare for are consistent with missions, but priorities vary

State and local organizations were asked to rank which incident type--chemical, biological, radiological, nuclear, or conventional explosives--was most important for their organization to prepare for. Not surprisingly, the rankings tended to follow organizational mission. Local responders, such as law enforcement and fire departments, tended to rank conventional explosives, then chemical, incidents as being most important to prepare for, as did State OEMs. In comparison, health organizations (State and local public health, and State emergency medical services (EMS) agencies) focused on bioterrorism preparedness. Hospitals, local/regional EMS agencies, and local OEMs ranked chemical incidents as most important to prepare for.

State and local organizations differed in how high a priority they assigned to spending departmental resources on preparing for the top-ranked incident type they chose (Table 2). For example, of those organizations that chose as their top-ranked incident conventional explosives, 8 – 16 percent of fire departments and law enforcement agencies considered it a high priority for their organization to spend resources in this areas as compared to 56 percent of State OEMs (Table 2). In general, about half of local responders and two-thirds of hospitals considered it was only somewhat of a priority for their organization to spend resources on the top-ranked incident type they had chosen. In comparison, two-thirds of State public health departments and State OEMs and half of State EMS agencies and local public health agencies considered it a high priority for their organization to spend resources on the top-ranked incident type they had selected.

Table 2. How High a Priority for Organizations Is It to Spend Resources Preparing for the Top-Ranked Incident Type They Chose?

Organization Type	Percent of All Organizations			
	High Priority	Somewhat a Priority	Low Priority	Not At All a Priority
Top Ranked Incident: Conventional Explosives				
Law Enforcement	16 (5)	38 (5)	33 (5)	13 (4)
Paid/Combo Fire	13 (4)	50 (6)	28 (5)	9 (3)
Volunteer Fire	8 (4)	32 (8)	38 (9)	21 (7)
State OEM	56 (7)	40 (7)	4 (3)	0
Top Ranked Incident: Bioterrorism				
Local Public Health	40 (8)	52 (9)	6 (3)	2 (1)
State Public Health	69 (4)	22 (4)	8 (3)	0
State EMS	43 (6)	40 (6)	10 (3)	7 (3)
Top Ranked Incident: Chemical				
Hospital	14 (4)	56 (7)	23 (6)	7 (4)
Local/Regional EMS	15 (4)	52 (5)	24 (5)	9 (3)
Local OEM	29 (5)	51 (6)	15 (5)	5 (3)

Standard error of the estimate is shown in parentheses.

In addition, we found a positive association between receipt of funding and/or resources since 9/11 and the assignment of a higher priority rating to spending departmental resources on terrorism preparedness. In particular, differences in priority assigned to preparedness between State and local organizations may reflect differences in the distribution and receipt of funding from the Federal government (as well as from other sources) following the 9/11 attacks where the initial influx of funds focused on State governments and on bioterrorism preparedness. In addition, differences in priority assigned to terrorism preparedness may partly reflect differences in organizational mission. For example, State organizations that have an

overall emergency preparedness mission versus first-responder organizations, such as law enforcement or fire services, which have a broader public safety mission.

Organizations also varied in terms of which response capabilities they considered to be the weakest for the incident type they had selected as being most important to prepare for. A majority of local responders and local public health agencies were concerned about protecting response personnel and hazard identification. First responders and State and local public health agencies were also concerned about decontamination of victims and mass care capabilities. Both State and local organizations felt equally that coordination and communication between the State and local levels needed improvement. To help strengthen response capabilities, State and local organizations wanted support in terms of training courses and exercises. In addition, the majority of local response organizations wanted new or more up-to-date equipment. Among the health organizations, local public health agencies were most likely to want support in the areas of training courses, exercises, new or more up-to-date equipment, and technical support. These survey results are consistent with LaTourrette et al. study (2003) of emergency responder protection needs. Based on structured discussions with representatives from the emergency responder community, they found a common concern expressed was the need for adequate protection against terrorist attacks and the vulnerability of nonspecialist responders.[28]

An association exists between receipt of funding and steps organizations have undertaken to improve response capabilities

A recurring theme we heard from State and local organizations was that they needed funding support for such activities as training and equipping, as well as for conducting risk assessments. Organizations cited limited training and equipment procurement budgets, as well as competing or higher departmental budget priorities, as factors limiting their ability to purchase specialized equipment for terrorism preparedness and to participate in Federally sponsored training or equipment programs. Primarily, State and local organizations were looking toward DHS for financial support in these areas.

Following the 9/11 attacks, most State organizations increased spending or reallocated resources to improve their response capabilities for terrorism and indicated that they received external funding and/or resources to support these activities (Table 3). In comparison, only 1 out of 5 law enforcement agencies and 1 out of 3 paid/combination fire departments increased spending or reallocated resources following 9/11 to improve response capabilities for terrorism, and only half of those organizations received external funding to support these activities. The primary reasons organizations internally increased spending or shifted resources following 9/11 were to do planning, training of personnel, or to purchase PPE and other equipment.

Health organizations fared better than other responders because of the Federal government's focus on improving bioterrorism preparedness following 9/11. Almost all State public health departments and State EMS and two-thirds of local public health agencies and hospitals increased spending following 9/11 (Table 3). However, although not shown, while all State public health departments and 70 percent of State EMS received Federal support for bioterrorism preparedness,[29] only 44 percent of hospitals and 31 percent of local public health agencies indicated they had received additional funding or resources from their *State government* since 9/11 to support their preparedness activities.

[28] LaTourrette, T, DJ Peterson, JT Bartis, and BA Jackson. *Protecting Emergency Responders, Volume 2: Community Views of Safety and Health Risks and Personal Protection Needs*, RAND, MR-1646-NIOSH, 2003.

[29] Following 9/11 all State public health departments received funding from the Federal government through the Centers for Disease Control and Prevention (CDC) cooperative grants to improve their States' bioterrorism preparedness. State EMS organizations received funding following 9/11 through the Health Resources and Services Administration (HRSA) cooperative agreements.

Table 3. Following 9/11, Which Organizations Increased Spending or Internally Reallocated Resources to Improve Response Capabilities?

Organization Type	Did Org Increase Spending/ Shift Resources Internally Since 9/11? (%)	For What Purposes? (%)			Did Org Receive External Funding and/ or Resources to Support Activities? (%)
		Planning	Training	Purchase PPE/Equip.	
Local Organizations					
Law Enforcement	18 (4)	9 (3)	14 (3)	8 (2)	13 (4)
Local/Regional EMS	46 (5)	69 (7)	31 (5)	17 (4)	35 (5)
Local OEM	42 (6)	30 (5)	32 (6)	28 (5)	62 (6)
Paid/Combo Fire	29 (6)	19 (6)	25 (6)	20 (6)	20 (4)
Volunteer Fire	1 (1)	.10 (.7)	1 (.7)	1 (.7)	0
State Organizations					
State EMS	81 (4)	66 (5)	63 (5)	22 (5)	67 (5)
State OEM	85 (5)	81 (6)	58 (7)	38 (7)	92 (4)
Health Organizations					
Hospital	66 (7)	32 (6)	60 (7)	47 (8)	44 (7)
Local Public Health	70 (12)	--	--	--	--
State Public Health	94 (2)	--	--	--	--

Standard error of the estimate is shown in parentheses. Numbers in table represent percent of all organizations. Dashes in the table indicate that a particular organizational type either was not asked the question or given a particular response option.

One of the issues we wanted to understand was whether receiving an increase in funding or resources was related to organizations taking steps to improve preparedness compared to other organizations of the same type that did not receive such an increase.[30] In general, we found that local organizations and State EMS organizations[31] that had received an increase in funding or resources following 9/11 were also more likely than other organizations of their same type to have: (1) assigned a higher priority to expending resources on terrorism preparedness; (2) updated response plans for one or more types of CBRNE; (3) created new organizational structures to address terrorism preparedness; [32] (4) identified or scheduled training opportunities for their personnel; [33] (5) purchased terrorism-related detection or protective equipment; and (6) assessed their overall level of preparedness as higher than those organizations that had not received an increase in funding or resources.[34]

To illustrate, Table 4 shows the percent of local organizations that updated their response plans for chemical, biological, radiological, nuclear, conventional explosives (CBRNE) following the 9/11 attacks. Local OEMs and hospitals were most likely to have updated their plans than other local organizations. Within each organizational type (except volunteer fire departments), those local organizations that received external funding or support also were more likely to have updated their response plans. For example, overall 41 percent of law enforcement agencies updated their response plans for one or more types of CBRNE incidents following the 9/11 attacks. However, of those law enforcement agencies that *had received* an increase in funding or support 61 percent also updated their response plans, whereas among law enforcement agencies that *had not received* an increase only 35 percent updated their response plans for CBRNE. Of course, these identified associations do not imply a causal effect due to the receipt

[30] See Tab 2 for a detailed discussion of this analysis.
[31] Because all State public health departments and nearly all State OEMs had received Federal support following 9/11, a similar comparison could not be made.
[32] With the exception of hospitals and paid/combination fire departments.
[33] With the exception of paid/combination fire departments.
[34] Because all State public health departments and nearly all State OEMs had received Federal support following 9/11, a similar comparison could not be made.

of funding or support. For example, organizations that are more actively engaged in preparedness activities also may be more likely to both apply for funding and/or to be more successful at obtaining funding.

Table 4. Since 9/11, Percent of Local Organizations That Updated Response Plans for One or More Types of CBRNE Incidents

Organization Type	Did Organization Update Emergency Response Plans for CBRNE Following 9/11? (% of All Orgs)	Percent of Orgs That Updated Response Plans and . . .	
		HAD Received Funding or Other Support	HAD NOT Received Any Funding or Other Support
Law Enforcement	41 (6)	61 (11)	35 (7)
Local/Regional EMS	48 (5)	59 (8)	40 (7)
Local OEM	75 (5)	82 (5)	37 (15)
Local Public Health	60 (11)	77 (5)	22 (14)
Paid/Combo Fire	39 (6)	52 (7)	28 (8)
Volunteer Fire	13 (6)	10 (11)	15 (8)
Hospital	89 (4)	100	71 (10)

Standard error of the estimate is shown in parentheses.

Organizations differ in their participation in federally sponsored programs and their expectations of DHS and the Federal government in general

Since September 11, 2001, State organizations have participated more than local organizations in federally sponsored training, equipment, or funding programs.[35] In addition, while State organizations tended to participate across a variety of programs, local organizations participated in a more limited number of programs specific to their professional community. Further, State organizations tended to have much higher participation rates than local organizations. In general, State organizations that had participated in Federally sponsored programs since the 9/11 attacks also shared those resources with other organizations within their State (commensurate with their mission and role as serving as a pass-through for Federal support to local communities and response organizations). In addition, those local organizations that had received Federal support also tended to share it with other organizations within their jurisdiction.

State and local organizations differed in their views about whether Federal funding was reaching the right communities and organizations. State OEMs and State public health departments (those organizations responsible for distributing Federal funding and/or resources within their State for emergency and bioterrorism preparedness) tended to believe that Federal support was reaching those communities and organizations with the greatest need. However, local organizations were more likely to believe that Federal funding was not reaching the communities and organizations with the greatest need, regardless of whether the funding was distributed through the State governments or directly to local communities and response organizations.

States and locals were fairly consistent in what impact they expected DHS to have on their organizations (Table 5). For example, most organizations expected DHS to improve coordination, communication, and information-sharing between the Federal/State/local levels; to standardize and streamline the grant application process across Federal programs; and to consolidate multiple grant requirements. Where there were differences in views (not shown), the pattern tended to be for some organizations to want DHS to undertake a specific activity even more so than did the other organizations. For example, overall between

[35] For a detailed summary of the survey results regarding organizations participation in Federally sponsored programs, see Tab 3.

50 and 60 percent of organizations expected DHS to standardize the grant application process across Federal agencies and to consolidate multiple grant application requirements, whereas 80 percent of State OEMs expressed this view.[36]

Table 5. In What Ways Do Local/State Responders Expect the DHS to Impact Them?

Percent of Organizations	Activities
70-80% expect DHS to . . .	Improve coordination, information-sharing, and communication between Federal/State/local levels
60-70% expect DHS to . . .	Streamline grant application process across Federal grant programs
50-60% expect DHS to . . .	Standardize the grant application process across Federal agencies and consolidate multiple grant application requirements
40-60% expect DHS to . . .	Establish single point of contact at Federal level for information on available programs Provide primary contact at Federal level instead of many on training, equipment, planning and other critical needs*
45-60% expect DHS to . . .	Provide intelligence information and more detailed guidance on terrorist threat
40-60% expect DHS to . . .	Consolidate numerous training courses/ programs and numerous equipment programs**
40-60% expect DHS to . . .	Provide better/standardized templates and/or guidance to help with planning
30-40% expect DHS to . . .	Improve integration between public/private sectors' efforts to improve terrorism preparedness and protect critical infrastructure
30-40% expect DHS to . . .	Help conduct threat assessment for jurisdiction or region***

*Health organizations not given this response option. **Health organizations not asked about equipment programs. ***Hospitals were not given this response option.

However, State and local organizations differed in some of their expectations of the Federal government in general (Table 6). For example, 1 out of 5 local public health agencies wanted Federal support to enhance surveillance systems, help with the development of local/regional response plans, establish communication systems to notify health providers about disease outbreaks, and establish a laboratory network, whereas few State public health departments felt Federal support was needed in these areas.

Table 6. In What Ways Can the Federal Government Support Public Health Organizations' Efforts to Improve Preparedness?

Type of Support Looking Toward Federal Government to	Local Public Health (%)	State Public Health (%)
Enhance current surveillance systems	20 (6)	3 (2)
Assist with development of local and regional response plans	22 (6)	6 (2)
Establish centralized communication system for notification regarding disease outbreaks related to bioterrorism	19 (6)	3 (2)
Establish integrated, multi-level laboratory response network for bioterrorism	15 (5)	6 (2)
Establish rapid response and advanced technology lab for chemical agents	16 (5)	6 (2)
Assist with the exercising of local and regional response plans	19 (6)	10 (3)
Assist with development of plans to coordinate local/regional medical systems	17 (6)	0
Assist with the development of plans to coordinate local/regional veterinarian systems	12 (5)	3 (2)

Standard error of the estimate is shown in parentheses. Public health organizations were asked in what ways the Federal government (e.g., through the CDC, DHHS, USPHS) can support the efforts of public health departments like theirs to improve terrorism preparedness.

[36]The stronger desire by State OEMs for DHS' support in these areas is consistent with the mission of the State OEMs and their role in helping to distribute Federal preparedness funding and support to locals. In general, the patterns seen were consistent with the individual organizations' missions and scope of responsibilities.

Also, local organizations wanted Federal support in the areas of equipment procurement, training or training aids, and provision of technical information, whereas few State organizations indicated a need for Federal support in these areas (Table 7). These results suggest differences between the local and State levels in expectations of the Federal government. For example, State public health and State OEMs may believe their State is getting all that it needs in these areas. Given that State organizations often are responsible for distributing Federal support to local communities within their State, these results also suggest that there might be room for improvement for State organizations to get technical information and Federal support out to the local levels.

Table 7. In What Ways Can the Federal Government Support Organizations' Efforts to Improve Preparedness?--Other Areas of Disagreement

Type of Support Looking Toward Federal Government For	Percent of Orgs	Exceptions (Percent)
Equipment procurement	20-35%	None of the State public health or State OEMs wanted equipment procurement support
Training or training aids	25-40%	Only 7-8% of State public health and State OEMs wanted such support
Distribution of technical information	10-20%	Only 5-6% of State public health and State EMS wanted such support

State and local organizations also differed in what role they expected the Federal Military and National Guard to play during the response to a terrorism-related incident (Table 8). For example, most local and State EMS organizations viewed both the Federal Military's and the National Guard's role as to maintain order and provide security. However, only about a quarter of State OEMs viewed this as being a Federal Military role, reflecting perhaps a better understanding of such issues as restrictions about the Federal Military's domestic role under the Posse Comitatus Act.

Table 8. Organizations Differ in What Role They Expect the Federal Military and National Guard to Play During Response to a Terrorism-related Incident

Organization Type	Federal Military's Role		National Guard's Role	
	Maintain Order/ Provide Security (%)	Help Enforce Quarantine (%)	Maintain Order/ Provide Security (%)	Help Enforce Quarantine (%)
Local Organizations				
Law Enforcement	71 (5)	58 (6)	89 (3)	61 (6)
Local/Regional EMS	76 (5)	56 (5)	89 (3)	64 (5)
Local OEM	74 (5)	55 (6)	86 (4)	67 (6)
Paid/Combo Fire	81 (4)	53 (7)	89 (4)	60 (6)
Volunteer Fire	75 (7)	31 (7)	77 (7)	30 (7)
State Organizations				
State EMS	63 (5)	37 (5)	87 (4)	67 (5)
State OEM	27 (6)	42 (7)	77 (6)	65 (7)
Health Organizations				
Hospital	--	82 (4)	--	86 (4)
Local Public Health	--	--	95 (2)	52 (10)
State Public Health	--	--	100	53 (5)

Standard error of the estimate is shown in parentheses. Dashes in the table indicate that a particular organizational type either was not asked the question or given a particular response option.

In addition (as shown in Table 8), State and local organizations and health organizations (public health versus hospitals) seem to differ in how they view the role of the Federal Military or National Guard in the event of a major disease outbreak. About two-thirds of local organizations felt the role of the Federal Military and the National Guard should include helping to enforce a quarantine. However, fewer State

OEMs and State EMS considered this to be a role for the Federal Military, and only half of local and State public health agencies (compared to 86 percent of hospitals) viewed this as a role for the National Guard.

In some cases, these differences in views may reflect a lack of knowledge or misunderstanding about the roles and responsibilities of the Federal Military under the Federal Response Plan or the new National Response Plan, as well as a lack of knowledge about legal restrictions on the domestic use of the Federal Military. In addition, these differences in views suggest that organizations may be doing planning under different assumptions about what role they can expect the Federal Military or the National Guard to play during a response to a terrorist-related incident. In either case, it appears this is an area for improving awareness.

Room for improvement in coordination with the private sector

One issue of importance to the Advisory Panel is the role of the private sector in homeland security and in helping to ensure preparedness for terrorism. As noted by the panel in its fourth report to Congress:[37]

> The private sector controls approximately 85 percent of the infrastructure in this country and employs approximately 85 percent of the national workforce.

Enhancing coordination with the private sector is seen as critical for ensuring the preparedness of States and localities and for protecting vital infrastructure. In the third wave of the survey, we asked State and local organizations about their coordination activities with the private sector. Following the 9/11 attacks, nearly all the State organizations and between a third to three-quarters of the local organizations created new organizational structures (e.g., positions, units, committees, or groups) to address preparedness for terrorism-related incidents (Table 9).

Table 9. Have Organizations Created New Structures to Address Terrorism Preparedness Following 9/11?

Organization Type	Created New Organizational Structures Following 9/11? (% of All Orgs)	Of Those That Created New Structures, Do Duties of the New Unit or Position Include Liaison with Private Sector? (%)
Local Response Organizations		
Law Enforcement	38 (6)	45 (9)
Local/Regional EMS	62 (5)	--
Local OEM	62 (6)	48 (8)
Paid/Combo Fire	52 (6)	37 (11)
Volunteer Fire	30 (8)	36 (16)
State Organizations		
State EMS	91 (3)	--
State OEM	92 (4)	65 (7)
Health Organizations		
Hospital	81 (5)	--
Local Public Health	77 (12)	91 (3)
State Public Health	100 (0)	97 (2)

Standard error for each point estimate is shown in parentheses. Dashes in the table indicate that a particular organizational type either was not asked the question or given a particular response option.

Of those that created new structures, about half (except for public health) indicated that the duties of these new positions or units included liaison with the private sector. Although nearly all local and State public health departments indicated that part of the duties of these new positions or units included liaison with

[37] *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*, December 16, 2001, pp. 30-31. www.rand.org/nsrd/terrpanel/

the private sector, what they probably are referring to are coordination activities with hospitals, managed care organizations, or other individual healthcare providers, many of which belong to the private sector.[38]

However, when we compare these results to whether organizations say they have any formal agreements in place with the private sector about emergency planning or response, many fewer organizations indicated this to be the case. Only about 1 out of 3 local and State OEMs and 1 out of 5 of the other organizations said they had formal agreements with private companies, businesses, or labor unions to share information or resources in the event of an emergency or disaster. These agreements addressed coordination and planning, as well as response. Further, few local organizations and only about 1 out of 5 State organizations and local OEMs indicated that they would contact the private sector if they had any threat information to pass on about suspected terrorist activities within their jurisdiction or region.

State organizations, in particular, recognize there is room for improvement in strengthening coordination with the private sector. Between half to two-thirds of State organizations expect DHS to help improve integration between the public/private sectors' efforts to improve terrorism preparedness and to protect critical infrastructure.

Conclusions

A common theme heard from organizations was the desire for additional funding to support their preparedness activities and to pay for overtime and backfill costs. Another common theme was the desire for more detailed information about the nature and type of threat facing their jurisdiction or State to inform planning and their response to changes in the threat level. Organizations are looking primarily to DHS for support and have high expectations of the Department in terms of improving coordination between the Federal/State/local levels, streamlining grant processes and requirements, consolidating training courses/programs and equipment programs, and facilitating integration of the private sector in terrorism planning and preparedness.

Although organizations have undertaken a range of activities since the 9/11 terrorist attacks to improve their response capabilities, it is difficult to say how much better prepared they are without any standardized measures of organizational and community preparedness. As noted by some survey respondents, they are doing more since 9/11, but at the end of the day, how do they know whether their organization (or community) is adequately prepared?

Following the 9/11 terrorist attacks, Federal funding focused initially on bioterrorism preparedness, with nearly $1 billion set aside in early 2002 for States to help improve their public health infrastructure for biological attacks.[39] Most of the initial funding went to State public health departments (and to a lesser degree, to State EMS) to develop and implement an overarching plan for improving their State's capacity to respond to bioterrorist attacks. Since then, additional funding has been forthcoming to improve both public health and hospital preparedness. However, Federal funding through DHS did not begin to flow to the first-responder community through the State governments until approximately two and a half years after 9/11. In March 2003, DHS announced the availability of approximately $750 million to the States for police, firefighters, and EMS workers to be used for training, exercises, and the purchase of

[38]The CDC cooperative agreements for public health preparedness encourage establishing public/private partnerships, with one of the enhanced capacities calling for the strengthening of relationships between the health department and emergency responders, the business community, and other key individuals or organizations involved in healthcare, public health, or law enforcement. Source: CDC Continuation Guidance for Cooperative Agreement on Public Health Preparedness and Response for Bioterrorism--Budget Year Four Program Announcement 99051, May 2, 2003.

[39]"Federal Funds for Public Health Infrastructure Begins to Flow to States," *HHS News*, U.S. Department of Health and Human Services, January 25, 2002.

equipment.[40] Our survey was conducted from July through September 2003, about the time one might expect these initial funds to have begun reaching the first-responder community.

Overall, we found that State governments had received more Federal funding and support and have participated in a wider range of Federal preparedness programs than local organizations since the 9/11 attacks. However, the story is more complex than what it may seem on the surface. Although it appears that State organizations have fared better than local organizations, State organizations also have served as a vehicle for administering Federal grants received and as a pass-through to the locals of Federal funding and support. Nearly all State organizations indicated they had shared resources received. At the same time, local organizations predominantly believe that Federal funding has not reached either local communities or organizations with the greatest need, regardless of the mode of distribution. In the survey written comments, a common theme was the need for Federal support to be distributed directly to local organizations, bypassing the State and county governments.

With respect to local organizations, fewer indicated having received external funding or support (regardless of the source) following the 9/11 attacks to support their preparedness activities than State organizations. For example, only 13 percent of law enforcement agencies and 20 percent of paid/combination fire departments indicated having received an increase in external funding or support from any source. However, some local organizations' participation in Federal preparedness programs may be more understated than the survey results alone suggest. For example, the Emergency Management Performance Grants (EMPG) program run by FEMA provides States with funds to support all hazards preparedness activities and emergency management. The EMPG program existed prior to 9/11. An important source of funding for the fire service has been the Assistance to Firefighters Grant Program. Indeed, we found that 46 percent of paid/combination fire departments and 20 percent of volunteer fire departments indicated they had participated in this program since 9/11. Although law enforcement has not been an important component of the First Responder Equipment grant program, it had received Federal funding through the Department of Justice (DOJ) prior to 9/11 through several different programs. The Community Oriented Police Services (COPS) Program and the Local Law Enforcement Block Grant Program, for example, have been an important source of Federal support that have enabled law enforcement to hire additional personnel and purchase needed equipment. Yet in our survey, we found that only between 10-13 percent of law enforcement agencies indicated they had participated in the Local Law Enforcement Block Grant Program since 9/11; our survey did not ask about the COPS program. Further, the President's first-responder initiative had a significant impact on these programs. The FY 2003 Omnibus Appropriations bill cut by $150 million the funding requested by the Senate for the Assistance to Firefighters Grant Program[41] and the COPS and Local Law Enforcement Block Grant programs have now been absorbed by ODP. As a result, some have argued that in the long-run it is not clear to what extent there has been a net gain in the Federal support available to law enforcement and other first responders for preparedness activities.

Nonetheless, we found an association between the degree to which different activities have been undertaken by local organizations and State EMS organizations to improve preparedness for terrorism-related incidents and the receipt of external funding and/or resources since 9/11 to support such activities. Within each organizational type (e.g., law enforcement), those agencies that had received external funding or resources following the 9/11 attacks were more likely than agencies that had not received such support to undertake a range of different preparedness activities. Of course, this relationship may or may not be a causal one, and in any case, the direction of causality is indeterminate.

---

[40]U.S. Department of Homeland Security, Office of the Press Secretary, "Department of Homeland Security Announces Opening of Grant Application Process for Firefighter Assistance Grants," March 10, 2003.

[41]Funding of FEMA's Firefighter Assistance Grants in the FY 2003 bill was set at $750,000,000. These grants can be used to support training, fire prevention programs, purchase of equipment and new fire apparatus, and to enhance emergency medical services (EMS) programs. "First Responders Funding in Fiscal Year 2003 Omnibus Appropriations Bill," U.S. Senator Patrick Leahy, http://leahy.senate.gov/press/200302/021403a.html.

The tabs to the appendix contain detailed information on all aspects of the State and Local Responder Survey.

TAB 1— METHODS

TAB 2— DETAILS OF COMPARISON BETWEEN DISTRIBUTION OF FUNDING AND SUPPORT AND PREPAREDNESS ACTIVITIES

TAB 3— PARTICIPATION IN FEDERALLY SPONSORED PROGRAMS SINCE 9/11

TAB 4—WEIGHTING AND SAMPLING DESIGN

TAB 5— THE SURVEY INSTRUMENT

TAB 6—FIRE DEPARTMENT SURVEY

TAB 7—SURVEY TABULATIONS

TAB 8—SURVEY COMMENTS

TAB 1—METHODS

The third survey instrument contained seven sections: (1) Emergency Response Planning Activities (included questions about planning, joint preparedness activities, training); (2) Resourcing Preparedness Activities (including questions about increased spending since 9/11 and receipt of external funding to support these additional activities); (3) Responding to Specific Terrorist Incidents (including questions to elicit their self-assessment of response capabilities for the type of incident they considered most important for their organization to prepare for); (4) Assessment of Federal Programs (including questions about their participation in Federal preparedness programs since 9/11, expectations of the Department of Homeland Security, and their support needs); (5)Intelligence Information and Warning (including questions about intelligence support needs and suggestions for improving the Homeland Security Advisory System); (6) Other Homeland Security Issues (including questions about their threat experience since 9/11, risk assessment activities, and views regarding the role of the military), and (7) Organizational Information (including questions about organizational characteristics and asked for overall written comments). For a copy of the survey instrument, see Tab 6.

The third survey was mailed to those organizations that were selected for 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, D.C. We updated the original 2001 contact database to account for any changes over time in personnel and in six instances, we found that the organization no longer existed. For two of the cases, we were able to draw a replacement organization for their organizational type in each relevant county. In the remaining cases, we were unable to identify a replacement organization. For a detailed discussion of the Methods used for the first survey, please see RAND PM-1236-OSD, *Sampling Design, Respondent Selection, and Construction of Survey Weights for the Federal Weapons of Mass Destruction Preparedness Programs Survey,* by Jerry Jacobson, Ronald Fricker, and Lois Davis (August 2001).

Table 1A shows the current status of the first and third waves of the survey and their response rates.[42] In Wave I, the overall response rate was 65 percent with 1,068 organizations responding. By organizational type, the response rates varied from 48 percent for local/regional EMS organizations to 80 percent for State public health departments. 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. Wave I surveys were received from every State in the union and the District of Columbia. For the third survey (Wave III), our overall response rate was 56 percent with 918 organizations responding. Because this was the third time we had surveyed these organizations and given the fact that the third survey was the longest instrument by far, we expected some attrition to occur in terms of response rates. Our overall aim was to achieve at least a 50 percent response rate for each group. For most organizations, we met or exceeded this goal with five of the organizational types having responses rates approximately 60 percent or higher. The response rate for hospitals was similar to that which was achieved in Wave I, reflecting the fact that these organizations historically tend to be particularly difficult to survey. The local/regional EMS response rate was somewhat lower than the 2001 response rate for this group. This also is a group that historically is difficult to achieve high response

[42] In this report, we present the response rates for Waves I and III for comparison purposes since in these two waves the full sample of organizations were surveyed. In Wave II (2002) survey, a subset of the original sample was surveyed – those organizations that had replied to Wave I. For the Wave II response rates, please refer to 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, December 12, 2002, Appendix D.* http://www.rand.org/nsrd/terrpanel/.

rates for. We also found that since 2001 the responsibility for terrorism preparedness and planning among the EMS community in some States had been assigned to the State-level EMS organization. So in some cases, local/regional EMS organizations elected not to participate in the third survey and instead, deferred to their State EMS organization.

Table 1A. Current Status of the Surveys and Response Rates for Waves I and III

Response Organizations	WAVE I (2001)		WAVE III (2003)	
	Number of Organizations Surveyed	Response Rate	Number of Organizations Surveyed	Response Rate
Local Organizations				
Public Health	199	74%	199	63%
Law Enforcement	208	71%	208	63%
OEM	202	71%	202	53%
Fire Department*	443	68%	440	58%
Hospital	208	51%	208	49%
Local/Regional EMS	230	48%	229	40%
State Organizations				
OEM	51	78%	51	55%
EMS	51	63%	51	63%
Public Health	51	80%	51	73%
TOTAL/OVERALL RATE	**1,643**	**65%**	**1,639**	**56%**

*Includes paid, combination, and volunteer fire service organizations. **Wave I response rate includes completed surveys returned prior to September 11, 2001.

Unless otherwise indicated, results have been statistically adjusted to represent the entire population in that discipline (e.g., law enforcement).[43] For each result we also include in parentheses an estimate of the standard error. Standard errors are useful for judging the likely range of the true value: That is, the actual value for the entire population is highly likely to lie within the observed survey percentage plus or minus the standard error.

For those organizational types that were randomly selected (law enforcement, fire, local OEM, local public health, and hospitals), we investigated further weighting the survey responses to reflect identified non-response patterns. For example, hospitals in the Northeast were less likely to respond to the third survey than were hospitals in the Midwest. To account for this discrepancy, we applied additional weight to the responses from the Northeast, so that the results would not be biased toward Midwestern hospitals. The non-response weights were generated using logistic regression models to describe the probability of response, based on several county and organizational-level explanatory variables. No recognizable non-response patterns for local OEM's were identified, so no further weighting was applied to this group. For each of the other four organizational types, region of the country (Northeast, South, Midwest, and West) was a significant explanatory variable and was factored into the non-response weighting. In addition, law enforcement organizations were adjusted for the population size they serve and whether their jurisdiction has 911 service; fire departments were adjusted for whether their personnel are volunteer, paid, or a combination of paid and volunteer; hospitals were adjusted for the number of full-time-equivalent staff they employ; and local public health departments were adjusted to reflect whether they served urban areas. For further details regarding the weighting methodology and sampling design, see Tabs 4 and 5.

[43]The 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.

TAB 2— DETAILS OF COMPARISON BETWEEN DISTRIBUTION OF FUNDING AND SUPPORT AND PREPAREDNESS ACTIVITIES

We undertook a series of analyses to look at whether there is an association between receipt of funding and/or resources following 9/11and different types of preparedness activities undertaken. Survey indicators[44] used in the comparison of the distribution of funding and support and preparedness for terrorism-related activities included:

Funding and support items:

- Since September 11th, 2001, has your organization received an increase in its funding and/or resources for terrorism preparedness?[45] (Ques. 43, Fire Dept. Survey)
- Since September 11, 2001, has your organization received agency-specific funding, training, equipment, or other terrorism preparedness support from the Federal government? (Ques. 59, Fire Dept. Survey)

Preparedness indicators:

Budget/spending

- How high a priority is spending additional resources for combating terrorism, when compared to other current needs of your organization? (Q45, Fire Dept. Survey)
- Since September 11, 2001, has your organization increased its spending, or shifted resources internally, to address terrorism-related incidents? (Q41, Fire dept. Survey)

Response plans

- Has your organization updated or newly developed a written emergency response plan to specifically address…
    - Respondents were given the following options and asked to mark all that apply: chemical, biological, radiological, conventional explosives, cyberterrorism, or attacks on critical infrastructure incidents. (Ques. 13, Fire Dept. Survey)

Preparedness self-ratings

- How would you rate your organization's overall level of preparedness at present to respond to terrorism in general? (rated on a scale of 1 to 5, where 1=inadequate; 5=excellent) (Ques. 38, Fire Dept. Survey)
- How would you rate your organization's overall level of preparedness at present to respond to high consequence CBRNE terrorism, specifically? (rated on a scale of 1 to 5, where 1=inadequate; 5=excellent) (Ques. 39, Fire Dept. Survey)
- Your organization's *written emergency plan* to be used during a response to an event similar to the CBRNE event you selected as most important is: (rated on a scale of 1 to 5)[46] (Ques. 49, Fire Dept. Survey)
- Your organizations *knowledge and expertise* about response to this type of event[47] are: (rated on a scale of 1 to 5) (Ques. 50, Fire Dept. Survey)
- Your organization's *equipment* to respond to this type of event is: (rated on a scale of 1 to 5) (Ques. 51, Fire Dept. Survey)
- Your organization's *training* to prepare for this type of event is: (rated on a scale of 1 to 5) (Ques. 52, Fire Dept. Survey)

[44] Some indicators were constructed by combining categorical responses to individual survey questions.
[45] The local and State public health versions of the survey narrow this question to receipt from their State government.
[46] Where scales of 1 to 5 are indicated, the organization is asked to chose a whole number between 1 and 5 where 1=inadequate and 5=excellent.
[47] "this type of event" refers to the CBRNE event the organization identified as most important.

- Your organization's *exercises* to prepare for this type of event are: (rated on a scale of 1 to 5) (Ques. 53, Fire Dept. Survey)
- Your organization's ability to *communicate and coordinate* with other organizations likely to be involved in a response to this type of even is: (rated on a scale of 1 to 5) (Ques. 54, Fire Dept. Survey)
- How would you rank your organization's overall preparedness to respond to this type of event? (on a scale of 1-5) (Ques. 55, Fire Dept. Survey)

Organization/personnel

- Since September 11, 2001, has your organization created a new (a) position, (b) unit, or (c) group to address prevention, preparedness, response or recovery for terrorism-related incidents, or (d) specially assigned personnel for this task? (Ques. 2, Fire Dept. Survey)
- Since September 11, 2001, has your organization identified, or scheduled, training opportunities for emergency response to terrorism-related incidents? (Ques. 25, Fire Dept. Survey)
- Does your organization have any unit(s) specially trained and/or equipped to respond to terrorism-related incidents? [48] (Ques. 36, Fire Dept. Survey)

Protective/detection equipment

- Since September 11, 2001, has your organization purchased (or is it in the process of purchasing) specialized protective, monitoring, or detection equipment? [49] (Ques. 32, Fire Dept. Survey)
- Since September 11, 2001, has your organization purchased (or is it in the process of purchasing) monitoring and detection equipment for any chemical, biological or radiological agents, equipment for cyber detection, or equipment for decontamination of victims and/or sites? [50] (Ques. 30, Fire Dept. Survey)

Analysis and Results

We found a strong association between the distribution of funding and support mechanisms and the preparedness activities of local organizations to respond to terrorism-related incidents. Specifically, with the exception of public health departments, the survey contained two separate funding and support questions:

1. "Since September 11th, 2001, has your organization received an increase in its funding and/or resources for terrorism preparedness?", and
2. "Since September 11th, 2001, has your organization received agency-specific funding, training, equipment, or other terrorism preparedness support from the Federal government?"

The second question is narrower in the sense that it restricts focus to support received from the Federal government, yet it is broader in the categories of support cited. Thus, it is possible for an individual organization to answer "yes" to both of these questions or either one individually without the other. We first looked at the distribution of responses to these two funding and support questions. The weighted percentages in Table B1 indicate which responding local organizations answered affirmatively to the above two questions regarding receipt of support.

Almost all State OEMs and about two-thirds of local OEMs and State EMS organizations answered affirmatively to both questions in Table B1 regarding receipt of external funding and/or resources following 9/11. On the other hand, 71 percent of law enforcement agencies and about half of paid/combination fire departments and local/regional EMS answered in the negative to both questions indicating that they had not received external funding and/or resources from any source following 9/11.

[48] Question not posed to State or local public health organizations.
[49] Question not posed to hospitals or State or local public health organizations.
[50] Question not posed to State or local public health organizations.

Also, few volunteer fire departments indicated receipt of any external funding and/or resources following 9/11. About a quarter of hospitals answered affirmatively to both questions in Table 2A regarding receipt of external funding and/or resources following 9/11; whereas, 40 percent of hospitals answered in the negative to both support questions.

Table 2A. Receipt of External Funding and/or Resources Following 9/11 to Support Preparedness Activities

	Percent of All Organizations			
	Only Answered Yes to Ques. 1 - *Has Organization Received an Increase in External Funding and/or Resources from Any Source Since 9/11?*	**Only Answered Yes to Ques. 2 – *Has Organization Received Support From the Federal Government Since 9/11?***	**Answered Yes to both Questions 1 and 2 regarding receipt of funding and/or other support Since 9/11**	**Answered no to both questions – Organization Did Not Receive Any External Funding and/or Resources Since 9/11**
LOCAL ORGANIZATIONS				
Law Enforcement	4 (2)	16 (4)	9 (3)	71 (5)
Local/Regional EMS	10 (3)	11 (3)	25 (5)	54 (5)
Local OEM	6 (3)	23 (6)	56 (6)	15 (4)
Paid/Combo Fire	1 (1)	26 (5)	18 (4)	55 (6)
Volunteer Fire	0	16 (7)	0	84 (7)
STATE ORGANIZATIONS				
State EMS	7 (3)	10 (3)	60 (6)	23 (5)
State OEM	0	8 (4)	92 (4)	0
HEALTH ORGANIZATIONS				
Hospitals	17 (5)	17 (9)	26 (6)	40 (7)

Standard error of the estimate is shown in parentheses.

Under the CDC cooperative agreements, all State public health departments received Federal funding following 9/11 to increase their State's bioterrorism preparedness. With the expectation that this funding would be shared with local-level public health departments, instead of the two questions indicated above, all public health departments were asked a single funding and support question: "Since September 11, 2001 has your health department received from your State government an increase in funding and/or resources for terrorism preparedness?" Response proportions to this question are indicated in Table 2B.

Table 2B. Receipt by Public Health Organizations of External Funding and/or Resources From Their State Government To Support Preparedness Activities Following 9/11

	Percent Of All Public Health Organizations That Received Increase In Funding/Resources For Terrorism Preparedness From Their State Government	
	Received Increase	**Did Not Receive Increase**
Local Public Health	69 (12)	31 (12)
State Public Health	25 (4)	75 (4)

In summary, we found that among local organizations, since September 11TH, 2001 local OEMs were most likely to receive Federal support and external funding/resources in general, while law enforcement and volunteer fire departments were least likely to receive such funding or support. In considering positive associations between receipt of funding/resources and preparedness activities, a greater proportion of local OEM's currently benefit from such associations while the benefit of these associations exists in a smaller proportion of the other organization types.

To gain a sense of the association between funding distribution and preparedness, we compared responses to these two funding and support questions individually with responses to twenty-one indicators of

preparedness (which are listed above). These indicators, listed above, fell into five broadly related categories: i) a shift in budget/spending; ii) updating written response plans; iii) self-ratings of preparedness; iv) a shift in organizational/ personnel structure; and v) purchasing terrorism-related protective/ detection equipment. Comparisons were first made on an exploratory basis via cross-tabulations. Where appropriate, weighted logistic regression models were fit to test whether an association exists between individual preparedness indicators and the individual funding and support questions. [51]

Across law enforcement, paid/combination fire, local OEMs, hospitals, and local public health agencies, dependencies were observed between the two funding and support questions and preparedness indicators within each of the five indicator categories cited above. [52] For some categories, every indicator was significant for a particular organization type; for all combinations of these organization types and indicator categories, at least one of the indicators within each category demonstrated a significant dependency with the receipt funding or support.[53] For example, within the organizational/personnel category, paid/combination fire departments demonstrated a significant positive relationship between an increase in funding or resources and having any unit(s) specially trained and/or equipped to respond to terrorism-related incidents, but not the other indicators in this category. These dependencies were observed even if an organization only benefited from one of the funding and support sources. Volunteer fire organizations were anomalous in that the direction of the association was not always positive, i.e., for some indicators, the increase in support was associated with less preparedness (see, for example, Table B3 below). For all other organization types, the observed associations were positive; more funding/support was associated with improved preparedness.

To illustrate, Table 2C shows the percent of organizations that updated their response plans following 9/11 for CBRNE. Overall, State and local offices of emergency management (OEMs), State public health, and hospitals were most likely to have updated their plans as compared to other organizations. Within each organizational type (except volunteer fire), those organizations that received external funding or support as indicated in at least one of the funding and support questions listed above also were more likely to update their response plans. For example, although overall only 41 percent of law enforcement agencies updated their response plans for one or more types of CBRNE incidents following 9/11, those law enforcement agencies that indicated receipt of funding or support under at least one of the survey questions above were above were more likely (61 percent versus 35 percent) to have updated their written response plans for one or more types of CBRNE than law enforcement agencies that had not received funding or support.

[51] The hypothesis test used was a Wald test that all the explanatory logistic regression coefficients are zero. A non-zero coefficient would imply the existence of a relationship between the preparedness indicator and the funding question.
[52] The lone exception was that hospitals did not demonstrate a shift in organizational/personnel structure or an increase in preparedness self-ratings.
[53] Overall, roughly 200 hypothesis test were conducted. Typically, conducting this many hypothesis test creates a multiple testing problem—in general, testing multiple independent hypotheses at the .05 significance level, we would expect 5 percent of the tests to reject the null hypothesis randomly, just by chance, when no actual relationship exists. Given that the goal of this analysis is to gain a general sense of the relationship between funding and preparedness, and not to specifically examine each individual organization-indicator combination, this concern is somewhat mitigated.

Table 2C.Since 9/11, Percent Of Local Organizations That Updated Response Plans For One Or More Types Of CBRNE Incidents

	Percent of Local Organizations Overall That Updated Their Response Plans For CBRNE	Updated Response Plans AND Received Funding or Other Support (Percent)	Updated Response Plans BUT Did Not Receive Funding or Other Support (Percent)
Law Enforcement	41 (6)	61 (11)	35 (7)
Local/Regional EMS	48 (5)	59 (8)	40 (7)
Local OEM	75 (5)	82 (5)	37 (15)
Local Public Health	60 (11)	77 (5)	22 (14)
Paid/Combo Fire	39 (6)	52 (7)	28 (8)
Volunteer Fire	13 (6)	10 (11)	15 (8)
Hospital	89 (4)	100	71 (10)

Standard error of the estimate shown in parentheses.

In addition, although not shown, on a scale from 1 (inadequate) to 5 (excellent), paid/combination fire departments who received an increase in its funding or resources for terrorism preparedness were more likely to rate their organization's equipment as adequate (a score of 3) or higher for responding to the type of CBRNE incident they ranked as most important for preparation; 64 percent of those receiving an increase in funding or resources for terrorism preparedness rated their organization's equipment as adequate or higher while only 34 percent of those not receiving such support rated their equipment as adequate or better. Hospitals that received agency-specific Federal support were more likely (19 percent versus 77 percent) to purchase specific monitoring and decontamination equipment than hospitals that had not received an increase in funding or resources.

In general, local organizations (except volunteer fire organizations) that received an increase in funding or resources for terrorism preparedness or received agency specific Federal support were more likely than other organizations of their same type to have self-reported:

- Increased spending or reallocated internal resources after September 11th, 2001, to address terrorism preparedness
- Assigned a higher priority to expending departmental resources on terrorism preparedness
- Updated their written response plans for one or more types of CBRNE
- Created new organizational structures following September 11th, 2001, to address terrorism preparedness (except hospitals and paid/combination fire departments)
- Identified and scheduled training opportunities in terrorism-related incidents for their personnel (except paid/combination fire departments)[54]
- Purchased terrorism-related protective or detection equipment
- Assessed their level of terrorism preparedness higher (except hospitals).[55]

Although formal statistical tests for association were not appropriate for the local/regional EMS organizations since they were a convenience sample, patterns of dependence were easily observable here

[54] Although the observed frequency was higher for those paid/combination fire organizations that received an increase in funding or agency-specific support, the difference was not large enough to generate a statistically significant result.

[55] Within the self-rating category, the directional differences for hospitals were ambiguous, with some showing a positive relationship and others demonstrating a negative relationship with increased funding or support.

as well for all twenty-one of the indicators. For example, rating their organizations overall level of preparedness to respond to terrorism in general on a scale from 1 (inadequate) to 5 (excellent), 67 percent of the local EMS organizations who indicated they had not received an increase in funding or resources for terrorism preparedness gave a rating of 1 or 2, while 63% of those local EMS organizations who responded that they had received such an increase rated their preparedness at 3 or above.

Of course, these identified associations do not imply a causal effect due to the receipt of funding or support. For example, it would be reasonable to believe that an organization, which has made the decision to improve their terrorism response capabilities, would seek out both additional funding and training opportunities.

The same questions regarding funding and support were also asked of the State-level organizations. All the State public health organizations as well as all the responding State OEMs received agency-specific support, so there are no meaningful comparisons to be made between organizations that did or did not receive any support. However, we can directly examine the observed responses of the State EMS organizations for positive associations between receipt of funding/resources and preparedness activities (as with the local EMS organizations, formal statistical tests for association between these questions and the twenty-one indicators of preparedness (listed above) were not appropriate since the State-level organizations were not sampled randomly).

Of the responding State EMS organizations, those that received an increase in funding and support were more likely to update response plans for CBRNE, internally increase spending or reallocate resources to address terrorism preparedness, create new organizational structures to address response preparedness, and purchase specialized equipment. Among these observed associations, State EMS organizations who received an increase in funding or resources for terrorism preparedness were twice as likely to increase spending for terrorism related incidents and classify such spending as a high or somewhat high priority, 50 percent more likely to create a new terrorism-related unit or assign individual(s) specifically to terrorism preparedness, and 23 percent more likely to update their terrorism response plans; those who purchased monitoring and detection all received an increase. However, those State EMS organizations that did not receive an increase in funding or support rated their overall level of preparedness to respond to CBRNE terrorism at equal levels as those State EMS who did receive such benefits.

TAB 3—PARTICIPATION IN FEDERALLY SPONSORED PROGRAMS SINCE 9/11

The following tables show what percent of State and local organizations have participated in Federally sponsored funding, training, or equipment programs since 9/11 and the primary Federal programs they have participated in. The reader should be careful in over-interpreting these results in that the responses are highly dependent on how knowledgeable the individual who filled out the questionnaire for their organization was regarding the numerous Federal programs available and which ones their organization may have actually participated in. For example, a law enforcement officer filling out the survey with knowledge about training programs may be less knowledgeable about his or her organization's participation in equipment programs, etc. Also, because the number of Federally sponsored training, equipment, or funding programs are numerous, it was not possible to list all in the questionnaire. We gave respondents the option of writing in "other programs" participated in, however, relatively few wrote in additional programs. Thus, the results give us only an approximate idea about differences in participation rates since 9/11 and the range of Federal preparedness programs in which different organizational types have participated.

Table 3A.Since 9/11, Percent of Local Response Organizations That Have Participated in Federally Sponsored Funding, Equipment, Or Training Programs

Percent of Orgs Have Participated in Any Federally Sponsored Programs Since 9/11	Primary Federal Program(s) Participated in Since 9/11 (Percent of All Organizations)
Law Enforcement 42 (6)	**Since 9/11, law enforcement has participated in:** ▪ 10% (2) FEMA Emergency Management Institute Course(s) ▪ 13% (4) ODP/DHS State and Local Preparedness Equip. Program ▪ 12% (4) ODP/DHS State Homeland Security Grant Program ▪ 4% (3) BJA/OJP Local Law Enforcement Block Grants Program 58% (6) Participated in None
Local/Region. EMS 46 (5)	**Since 9/11, local/regional EMS has participated in:** ▪ 16% (4) ODP/DHS State Homeland Security Grant Program ▪ 11% (3) FEMA Emergency Management Institute Course(s) ▪ 10% (3) National Fire Academy Emergency Response to Terrorism course(s) ▪ 9% (3) ODP/DHS State and Local Preparedness Equipment Program ▪ 8% (3) ODP/DHS State and Local Preparedness Exercise Program ▪ 54% (5) Have not participated in any Federally sponsored programs
Local OEM 83 (5)	**Since 9/11, local OEMs have participated in:** ▪ 8% (3) EPA Emergency Response Training Program (ERTP) ▪ 9% (4) DOE Training for Radiological Emergencies ▪ 11% (3) Other National Domestic Preparedness Consortium Training Courses ▪ 31% (5) ODP/DHS State and Local Preparedness Exercise Program ▪ 25% (6) OJP Anti-Terrorism State and Local Training Grants (SLATT) ▪ 19% (4) National Fire Academy Emergency Response to Terrorism course(s) ▪ 15% (4) NM Tech's Incident Response to Terrorist Bombings Course ▪ 39% (6) FEMA Emergency Management Institute Course(s) ▪ 34% (6) Assistance to Firefighters Grant Program ▪ 31% (5) ODP/DHS State and Local Preparedness Exercise Program ▪ 48% (6) ODP/DHS State and Local Preparedness Equip. Program ▪ 55% (6) ODP/DHS State Homeland Security Grant Program ▪ 17% (5) Have not participated in any Federally sponsored programs
Paid/Combo Fire 73 (5)	**Since 9/11, paid/combination fire departments have participated in:** ▪ 5% (3) EPA Emergency Response Training Program (ERTP) ▪ 5% (1) DOE Training for Radiological Emergencies ▪ 6% (2) NM Tech's Incident Response to Terrorist Bombings Course ▪ 6% (2) Other National Domestic Preparedness Consortium Training Courses ▪ 6% (2) ODP/DHS State and Local Preparedness Exercise Program ▪ 5% (2) ODP/DHS State and Local Domestic Preparedness Training and Technical Assistance Program ▪ 13% (3) ODP/DHS State Homeland Security Grant Program ▪ 10% (3) OJP Anti-Terrorism State and Local Training Grants (SLATT) ▪ 21% (5) FEMA Emergency Management Institute Course(s) ▪ 24% (5) National Fire Academy Emergency Response to Terrorism course(s) ▪ 20% (6) ODP/DHS State and Local Preparedness Equip. Program ▪ 46% (7) Assistance to Firefighters Grant Program ▪ 27% (5) Have not participated in any Federally sponsored programs
Volunteer Fire 31 (7)	**Since 9/11, paid/combination fire departments have participated in:** ▪ 5% (3) EPA Emergency Response Training Program (ERTP) ▪ 5% (1) DOE Training for Radiological Emergencies ▪ 6% (2) NM Tech's Incident Response to Terrorist Bombings Course ▪ 6% (2) Other National Domestic Preparedness Consortium Training Courses ▪ 6% (2) ODP/DHS State and Local Preparedness Exercise Program ▪ 5% (2) ODP/DHS State and Local Domestic Preparedness Training and Technical Assistance Program ▪ 13% (3) ODP/DHS State Homeland Security Grant Program ▪ 10% (3) OJP Anti-Terrorism State and Local Training Grants (SLATT) ▪ 21% (5) FEMA Emergency Management Institute Course(s) ▪ 24% (5) National Fire Academy Emergency Response to Terrorism course(s) ▪ 20% (6) ODP/DHS State and Local Preparedness Equip. Program ▪ 46% (7) Assistance to Firefighters Grant Program ▪ 27% (5) Have not participated in any Federally sponsored programs

Standard error of the estimate is shown in parentheses.

Table 3B. Since 9/11, Percent of State Organizations That Have Participated in Federally-Sponsored Funding, Equipment, Or Training Programs

Percent of State Orgs Have Participated in Any Federally-Sponsored Programs Since 9/11	Primary Federal Program(s) Have Participated in Since 9/11 (Percent of All Organizations)
State EMS 87 (4)	Since 9/11, State EMS has participated in: ▪ 23% (5) ODP/DHS State and Local Domestic Preparedness Training and Technical Assistance Program ▪ 40% (6) ODP/DHS State Homeland Security Grant Program ▪ 7% (3) Assistance to Firefighters Grant Program ▪ 30% (5) ODP/DHS State and Local Preparedness Exercise Program ▪ 27% (5) ODP/DHS State and Local Preparedness Equip. Program ▪ 10% (3) EPA Emergency Response Training Program (ERTP) ▪ 27% (5) Other National Domestic Preparedness Consortium Training Courses ▪ 7% (3) NM Tech's Incident Response to Terrorist Bombings Course ▪ 7% (3) DOE Training for Radiological Emergencies ▪ 24% (5) National Fire Academy Emergency Response to Terrorism course(s) ▪ 43% (6) FEMA Emergency Management Institute Course(s) ▪ 20% (5) OJP Anti-Terrorism State and Local Training Grants (SLATT) ▪ 37% (5) Other 13% (4) Have not participated in any Federally sponsored programs
State OEM 100	Since 9/11, State OEMs have participated in: ▪ 65% (7) ODP/DHS State and Local Domestic Preparedness Training and Technical Assistance Program ▪ 38% (7) ODP/DHS Urban Areas Security Initiative (2003) ▪ 81% (6) ODP/DHS State Homeland Security Grant Program ▪ 4% (3) BJA/OJP Local Law Enforcement Block Grants Program ▪ 23% (6) BJA/OJP Byrne Formula Grant Program ▪ 23% (6) Assistance to Firefighters Grant Program ▪ 88% (4) ODP/DHS State and Local Preparedness Exercise Program ▪ 92% (4) ODP/DHS State and Local Preparedness Equip. Program ▪ 12% (4) FBI Hazardous Devices School ▪ 23% (6) EPA Emergency Response Training Program (ERTP) ▪ 65% (7) Other National Domestic Preparedness Consortium Training Courses ▪ 58% (7) NM Tech's Incident Response to Terrorist Bombings Course ▪ 50% (7) DOE Training for Radiological Emergencies ▪ 15% (5) US Army Chemical School Training Program (USACLMS) ▪ 46% (7) National Fire Academy Emergency Response to Terrorism course(s) ▪ 77% (6) FEMA Emergency Management Institute Course(s) ▪ 38% (7) OJP Anti-Terrorism State and Local Training Grants (SLATT) ▪ 8% (4) NDPO Equipment Research and Development Program ▪ 8% (4) Other Federal Programs

Standard error of the estimate is shown in parentheses.

Table 3C. Since 9/11, Percent of Health Organizations That Have Participated in Federally-Sponsored Training Programs or Academic Conferences

Percent Of Health Orgs Have Participated In Any Federally-Sponsored Training Programs or Academic Conferences	Primary Federal Program(s) Participated in Since 9/11 (Percent of All Health Organizations)
Hospitals 51 (8)	Since 9/11, hospitals have participated in: ▪ 37% (7) CDC Satellite Broadcasts or Conferences ▪ 16% (4) CDC's MMWR Continuing Medical Education Program ▪ 32% (6) CDC Training Modules ▪ 16% (4) FEMA Emergency Management Institute Course(s) ▪ 5% (3) US Army Chemical School Training Program (USACLMS) ▪ 3% (2) DOE Training for Radiological Emergencies ▪ 8% (3) Other 49% (8) Said we have not participated in any such Federally sponsored training programs or conferences
Local Public Health 70 (12)	Since 9/11, local public health has participated in: ▪ 5% (2) US Army Chemical School Training Program (USACLMS) ▪ 27% (7) CDC's MMWR Continuing Medical Education Program ▪ 59% (11) CDC Training Modules ▪ 64% (11) CDC Satellite Broadcasts or Conferences ▪ 13% (5) Other 30% (12) Said we have not participated in any such Federally sponsored training programs or conferences
State Public Health 100	Since 9/11, State public health has participated in: ▪ 97% (2) CDC Satellite Broadcasts or Conferences ▪ 97% (2) CDC Training Modules ▪ 54% (5) CDC's MMWR Continuing Medical Education Program ▪ 51% (5) FEMA Emergency Management Institute Course(s) ▪ 37% (5) DOE Training for Radiological Emergencies ▪ 23% (4) Other 0% Said we have not participated in any such Federally sponsored training programs or conferences

Standard error of the estimate is shown in parentheses. Note, health organizations were asked a somewhat different question than local responders or State organizations. Health organizations also were given fewer response options than local and State organizations.

TAB 4-WEIGHTING AND SAMPLING DESIGN

This tab describes the construction of sampling and non-response weighting used in the analysis of responses to Wave III of the survey. Together, these adjustments permit findings from the survey to be generalized to the larger population of response organizations nationwide. Wave III solicited the same sample of organizations as were solicited for Wave I. This choice combined the practicality of not having to absorb the expense of creating a second sample with the advantage of facilitating possible longitudinal analyses on the set of organizations that responded to common survey items in both of those waves. The discussion in this tab is based largely on RAND PM-1236-OSD, *Sampling Design, Respondent Selection, and Construction of Survey Weights for the Federal Weapons of Mass Destruction Preparedness Programs Survey,* by Jerry Jacobson, Ronald Fricker, and Lois Davis (August 2001) which has been updated to incorporate information relevant to the third survey.

Updating the sample

Responses to Wave III of the survey were solicited from the same sample of organizations that were solicited to participate in Wave I. An effort was made to update all addresses and points of contact for the sample prior to placing Wave III into the field. This effort was necessary due to the possibility that the sample organizations may have had a turnover in personnel--in particular, the employee most appropriate to fill out the survey--or may have moved to a new address. Additionally, some organizations may have no longer existed and would therefore need to be replaced.

Two organizations were identified as no longer existing, one law enforcement and one fire organization. Each of these organizations was replaced by another qualified organization in that same county.[56] The implications of these replacements on the probability of selection of these organizations into the sample are described in the next section. The act of replacing these two organizations did not impact the probability of selection of organizations in other counties or other organizational types in the same county.

In addition, several local EMS organizations forwarded their surveys on to their respective State organizations for completion. As these events occurred after the survey was in the field and the set of local EMS organizations were as convenience sample, no attempt was made to replace these organizations, which essentially self-selected out of the sample.

Constructing the survey sampling weights

Survey weights account for differential probability of being sampled among strata and for non-response. These statistical adjustments allow the analysis to properly infer back to the correct 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

[56] Each replacement was chosen randomly from a compiled list of similar organizations in that same county. The associated sampling weights described in Section 3 were adjusted accordingly.

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 eligible organizations 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^R_{igj}, 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:

$$P_{igj} = \pi_j * \pi_{igj} * \pi^R_{igj} \qquad (1)$$

The first terms above, π_j and 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^R_{igj}, has a different meaning: it is an adjustment to account for the fact that some organizations that were asked to complete the survey were more likely than others to actually complete and return it. π^R_{igj}, is referred to as the "probability of response"; it accounts for observed patterns of response that can only be determined after all surveys have been returned and processed. For example, we observed that, on average, hospitals in which the number of full-time equivalent (FTE) physicians was below the median FTE were less likely to complete and return the survey than their larger counterparts. In this case, the adjustment is necessary to ensure that smaller hospitals' views are not underemphasized because of differences in response rates when results from hospitals of all FTE sizes are aggregated.

The next sections derive the right-hand side probabilities in equation (1) 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 generated different sampling rules. The impact of these differences on each term in equation (1), summarized in Table D1, is to follow. The derivation of the "probabilities of selection" was originally described in Jacobson, et. al (2001). For completeness, they are described again herein.

Weights have not been constructed for EMS respondents, since the sample of EMS organizations is a convenience sample. Findings from the local and regional EMS samples cannot be generalized to the larger EMS population. Weights also have not been constructed for State-level respondents, since the State surveys are censuses rather than randomly selected samples.

Probability of Selection for Counties

The sample of $n = 200$ counties was drawn without replacement from the $N = 3{,}105$ counties in the contiguous United States, Alaska, and Hawaii, with probabilities of selection proportional to the square root of each county's population.[57] If we call county *j's* population ρ_j, then the probability of selection for the j[th] county was[58]

[57] Population estimates were taken from the February, 2000 release of the DHHS's Area Resource File. Sampling was carried out using SAS's SURVEYSELECT procedure.
[58] Tab 4 describes the assumptions necessary for Equation (2) to represent true probabilities.

$$\pi_j = \frac{n\sqrt{\rho_j}}{\sum_{k=1}^{N}\sqrt{\rho_k}} \quad (2)$$

Note that later sections will describe adjustments to the π_j required for public health, OEM, and hospital respondents.

Probability of Selection for Organizations

Apart from the exceptions described in the next section and in the section on County Weighting Details below, only one representative from each group was selected per county. Therefore, the probability of selection for any organization *i* in group *g* and county *j*, given county *j* was selected in the first stage, was just

$$\pi_{igj} = \frac{1}{N_{gj}} \quad (3)$$

where N_{gj} is the number of organizations from group *g* eligible for sampling within county *j*.

Adjustment for OEMs and Public Health Respondents

A number of public health departments and OEMs have jurisdiction over neighboring counties that have no such organizations within their borders. For these (which we term "regional" organizations), the county probability of selection given in equation (2) must be augmented to account for the fact that if *any* county under their jurisdiction had been selected in the first stage sample of counties, then the regional organization in question would have been selected into the sample in the second stage.

Let π_R' be the adjusted probability of selection for a public health department or OEM in county *R* (for "regional") that has $N_R>1$ counties under its jurisdiction. Then,

$$\pi_R' = \pi_R + \sum_{c=1}^{N_R}\pi_c \quad (4)$$

where the right-hand side probabilities are just the π_j probabilities from equation (2).

Adjustment for Hospitals

Hospitals with trauma centers were over-sampled in order to ensure selection of an adequate number of hospitals involved in emergency response. In each county, a sampling procedure was constructed to ensure a 70% or greater chance of selecting a hospital with a trauma center.[59] Essentially, the list of trauma center hospitals was replicated an integer *Z* number of times until trauma center hospitals comprised at least 70 per cent of all hospitals. Let T_j and NT_j be the number of hospitals with, and without, trauma centers, respectively, in county *j*. Then *Z* is $ceil(0.7NT_j/0.3T_j)$, where the *ceil* operator rounds its argument to the next highest integer.

[59] In counties where no trauma center hospital was present, the usual selection mechanism was employed: one hospital was selected at random from all of the eligible hospitals (eligibility was discussed in Section 3).

This procedure results in a probability of selection for each trauma center hospital *t* in county *j* of

$$\pi_{t,hj} = \frac{Z_j}{Z_j * T_j + NT_j} \quad (5)$$

and for each hospital *nt*, that does not have a trauma center, of

$$\pi_{nt,hj} = \frac{1}{Z_j * T_j + NT_j} \quad (6)$$

where *h* in the subscripts indicates the hospital respondent group. The equations above replace equation (3) for hospitals in the calculation of survey weights.

One final adjustment to the hospital weights is necessary to account for the "nearest neighbor" selection rule that was employed when no hospital could be identified within a county. The adjustment, described below, results in an expression similar to the regional adjustment for public health departments and OEMs in equation (4) in the sense that it does not affect the adjustments given in (5) and (6) above, but instead replaces the hospitals' county probabilities of selection given in equation (2).
When no hospital could be identified within a county *c*, a hospital from the county nearest to *c* was selected at random. Consequently, hospitals in the sample could have been selected either because they a) were located within a sample county, or b) because they were in a county, call it *R*, that *did* have a hospital within its borders and happened to be the county closest to *c*. Thus, an adjustment to each hospital's probability of selection is required. In this case, it is more straightforward to make the adjustment to each hospital's county probability of selection, π_j, than to the organizational probability of selection, π_{ihj}. Let N_R be the number of counties surrounding *c* that contain no hospital and for which *R* is the nearest county that does contain a hospital. If we interpret *R* and N_R in this manner, equation (4) gives the correctly adjusted π_j for hospitals.

Table 4A below summarizes the above discussion. For each respondent group, it lists the number of the equation used to form the county probability of selection and the organizational probability of selection, respectively. These give the correct inputs to equation (1), adjusted as necessary for the different sampling rules required for each group. The derivation of survey weights for fire departments is more involved and appears below.

Table 4A. Equation References for Adjusted Probabilities of Selection due to Special Weighting Considerations

Respondent group *g*	π_j	π_{igj}	Reason for weighting adjustment
Law enforcement	(2)	(3)	No adjustment necessary
Fire	(2)	*	Stratification by HAZMAT; paid, volunteer, combination departments
EMS	(2)	$\pi_{igj}=1$	Convenience sample
Public health	(4)	(3)	Regional, multi-county jurisdictions
OEM	(4)	(3)	Regional, multi-county jurisdictions
Hospitals	(4)	(5)/(6)	Over-sampling of trauma centers; nearest neighbor rule

*See section on Probabilities of Selection for Fire Departments.

Constructing the Survey Non-Response Weights

Probability of Non-Response

Non-response was accounted for using the propensity score method of Little and Rubin (1987) to determine the probability, π^{R}_{igj} from equation (1), that organization *i* in group *g* in county *j* responded given that organization *i* was sampled. This probability was calculated by fitting a separate logistic regression model for each respondent group of the form

$$\pi^{R}_{igj} = \frac{\exp(\beta_g + \mathbf{X}_i + \mathbf{Y}_j)}{1 + \exp(\beta_g + \mathbf{X}_i + \mathbf{Y}_j)} \quad (7)$$

where β_g is the intercept coefficient for the respondent group (e.g., hospitals), and $\boldsymbol{X}_g$, and $\boldsymbol{Y}_j$ are vectors of organization-specific and county-specific characteristics, respectively.
At both the county and organization level, covariates were candidates for inclusion in the model if they were predictive of observed patterns of non-response[60] or willingness to respond (e.g., urbanicity of the respondent's county). Data availability also restricted the covariates available for inclusion in (7): only variables from the datasets used to construct the sampling frame—with few missing values for all respondents in the sample—could be included since the variables, defined on the population, must be available for both survey respondents and non-respondents alike.[61]

For a county *j*, the following factors hypothesized to influence a respondent's willingness to respond were considered for inclusion in the model:

- $region_j$ is a categorical variable indicating whether the county is in the Midwest, Northeast, South, or West
- pop_j is the county's 1998 population (on the natural logarithm scale)
- $land_j$ is the land area of the county (on the natural logarithm scale)
- $density_j$ is the population density, $pop_j/land_j$ of the county in 1998 (on the natural logarithm scale)
- $urban_j$ is an indicator for urban versus rural[62]

Apart from the *region* variables, all of the above are proxies for a county's size or its urbanicity. As we would expect, these variables are often collinear. This poses no problem, however, as it does in other settings, because the purpose of the non-response models here is prediction, as opposed to evaluating the statistical significance of any particular coefficient. Population, land area, and density all possess a skew in the positive direction. To improve model fit, these variables were transformed to the natural logarithm scale, which shifts the distribution of these variables much closer to that of a Normal distribution. In addition to the county-level characteristics above, variables specific to the individual organizational types were also considered when appropriate. Additional detail on the sources of the variables may be found later in this Tab.

---

[60] The significance of each covariate was a standard z-test within the logistic framework.
[61] Where possible, missing values were inferred from the survey responses (to any of the waves where such information was solicited). The number of full time equivalent physicians, used in the nonresponse model for hospitals, was missing in the AHA's database for several hospitals that completed surveys. Since the initial Federal Weapons of Mass Destruction Preparedness Programs Survey (FWMDPPS) asked hospitals a similar question, values were imputed from the survey for use in prediction of the non-response model for these respondents. The FWMDPPS values were found to be well within the range of values reported for this variable in the AHA dataset.
[62] These variables were provided by the DHHS's Area Resource File, which contains projections for 1998 based on the 1990 Census.

For each respondent group, a number of models were identified whose covariates satisfied the criteria described above. Individual t-tests were used to identify those variables with strong explanatory potential. However, relying only on these tests poses a multiple testing problem. For example, the seven county level coefficients (three region coefficients and one each for the four quantitative variables) occur in each of the five organizational non-response models, for a total of 35 individual t-tests. Using the standard level .05 significance test (a more liberal threshold was actually employed in the analysis), we should expect two of the coefficients to demonstrate an effect when no effect is actually present just by the luck of the draw. For this analysis, the final model presented was chosen using the Akaike Information Criterion (AIC), which characterizes overall model fit on a likelihood basis while penalizing for over-parameterization.

Law Enforcement

In addition to the county-level characteristics above, the size of law enforcement organizations and other indicators of emergency response capabilities were considered for inclusion in the non-response model. For law enforcement organization *i*:

- $have\_911_i$ is an indicator corresponding to whether organization *i* participates in a 911 emergency dispatch system.
- $officers_i$ is the organization's number of sworn officers

The presence of a 911 emergency dispatch system proved informative upon non-response, with those without a 911 system being more likely to respond to the survey. As in Wave I, region of the country and county population were found to be good predictors. Law enforcement organizations in the West were more likely to complete the survey than respondents in any other region, as were respondents in counties with relatively large populations. Law organizations in the Midwest and South were more likely to respond than those in the Northeast. The values of the estimated logistic coefficients (β_l*'s*), along with the estimated β*'s* for the other respondent groups, are given in the section on Estimated Coefficients for Non-Response Models.

Fire Departments

Factors considered for the fire department non-response model included measures of organizational size, structure, and emergency response capabilities. For fire department *i*:

- $fire\_type_i$ is a categorical variable classifying personnel at department *i* as all *volunteer*, all *paid*, or some *combination*
- $hazmat_i$ is an indicator corresponding to whether department *i* has HAZMAT capability
- $have\_911_i$ is an indicator corresponding to whether department *i* participates in a 911 emergency dispatch system.

The National Public Safety Information Bureau's (NPSIB, see the section on Description of the Data Files) variable for number of personnel was excluded from the analysis because it was inconsistent with values provided by respondents in Wave I of the FWMDPPS. Other variables from the NPSIB were found to be more consistent (agreement on 80 per cent or more observations).

A pooled model with indicators for *volunteer* and *combination* was used (*paid was used as the reference category)*. The final pooled model indicates that all-volunteer departments were least likely to respond. Paid and combination departments were almost equally likely to respond, with paid being slightly less. Departments with HAZMAT capability were also more likely to respond, as were departments in the Midwest, followed by the West, and then the South and Northeast.

Hospitals

Covariates considered for inclusion in the hospital non-response model were organizational size and management structure. For hospital *i*:

- $Hosp\_type_i$ is a categorical variable classifying the organizational type of hospital *i* as *government or Federal, not-for-profit,* or *for-profit*
- $hosp\_bed_i$ is the number of staffed hospital beds
- fte_i is the number of full-time-equivalent medical staff
- $trauma_i$ is an indicator corresponding to whether the hospital has a trauma center
-

Of the above, only FTE was predictive of response. Like the county-level continuous variables, FTE had a heavy positive skew (i.e. there existed some atypically large hospitals). A correction to the natural logarithm scale was not successful in compensating for the skew, so the variable parsed into four categories, one for each quartile of the sample distribution. The hospitals with the fewest number of FTE physicians (those in the first quartile) were least likely to respond, followed by the second and then the fourth quartiles; the hospitals in the third quartile were most likely to respond.

Region of the county was also a strong predictor of hospital response. Hospitals in the Midwest were most likely to respond, with those on the South and West equally likely to respond. Northeastern hospitals were least likely to respond.

Public Health Departments

The data sets, described in the section on Description of the Data Files, do not provide reliable organizational-level data for public health organizations (recall that they were used primarily to obtain contact information for these respondents). For this reason, only the county level covariates were considered for these organizations

The final model for public health departments indicates that public health departments in the Midwest were most likely to respond, with the likelihood of response for the other three regions being almost equal. Urban departments were more likely to respond than rural health departments.

Offices of Emergency Management

Reliable organizational-level data for emergency management offices were also not available from the datasets in the section on Description of the Data Files. Among the county-level covariates, none proved to be predictive of response. Thus, no adjustment for non-response was made for these organizations.

References

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. Fourth Annual Report to the President and Congress, December 16, 2001, www.rand.org/nsrd/terrpanel/.

Akaike, H. (1973), "Information Theory and an Extension of the Maximum Likelihood Principal," in *Second International Symposium on Information Theory,* eds. B.N. Petrox and F. Caski, Budapest: Akademiai Kiado, p.267

Centers for Disease Control and Prevention (CDC). Continuation Guidance for Cooperative Agreement on Public Health Preparedness and Response for Bioterrorism--Budget Year Four Program Announcement 99051, May 2, 2003.

U.S. Department of Health and Human Services, Office of Research and Planning, Bureau of Health Professions. *Area Resource File*. February, 2000 release.

U.S. Department of Health and Human Services. "Federal Funds for Public Health Infrastructure Begins to Flow to States," *HHS News*, January 25, 2002.

U.S. Department of Homeland Security, Office of the Press Secretary. "Department of Homeland Security Announces Opening of Grant Application Process for Firefighter Assistance Grants," March 10, 2003.

U.S. Department of Homeland Security, Office of the Press Secretary. "Secretary Ridge Addresses National Governors Association," Press Release August 18, 2003.

Fowler, F. Jr. *Survey Research Methods* (2nd ed.), Newbury Park, CA, Sage Publications, 1993.

Fox, D.R. (1989), "Computer Selection of Sized-Biased Samples," *The American Statistician*, 43(3), 168–171.

Jacobson, J., Fricker, R., and Davis, L. (2001), RAND/PM-1236-OSD, *Sample Design, Respondent Selection, and Construction of Survey Weights for the Federal Weapons of Mass Destruction Preparedness Programs Survey*. Santa Monica, CA: RAND.

LaTourrette, T, DJ Peterson, JT Bartis, and BA Jackson. *Protecting Emergency Responders, Volume 2: Community Views of Safety and Health Risks and Personal Protection Needs*, RAND, MR-1646-NIOSH, 2003.

U.S. Senator Patrick Leahy. "First Responders Funding in Fiscal Year 2003 Omnibus Appropriations Bill," http://leahy.senate.gov/press/200302/021403a.html.

Little, R.J.A. and Rubin, D.B. (1987), *Statistical Analysis with Missing Data*. John Wiley and Sons. New York, New York.

Rice, J. (1995), *Mathematical Statistics and Data Analysis*, Second Edition, Duxbury Press, Belmont, California.

Vijayan, K. (1968), "An Exact π_{ps} Sampling Scheme: Generalization of a Method of Hanurav," *Journal of the Royal Statistical Society, Series B*, 30, 556–566.

County weighting details

The sample of n=200 counties was drawn without replacement from the N=3,105 counties in the contiguous United States, Alaska, and Hawaii, with probabilities of selection proportional to the square root of each county's population. Population estimates were taken from the February, 2000 release of the Department of Health and Human Services' (DHHS) Area Resource File. Sampling based on population size allowed for a representative number of larger counties to be included in the sample. However, using the actual population values, instead of their square roots, the sample would have been skewed too heavily in favor of the larger counties, and the number of smaller counties in the sample would have been too small to be representative. Transforming to the square root provided a means for balancing the number of counties sampled across the various county sizes.

If we call county j's population ρ_j, then the probability π_j of selection into the sample for the j^{th} county was:

$$\pi_j = \frac{n\sqrt{\rho_j}}{\sum_{k=1}^{N}\sqrt{\rho_k}} \tag{1}$$

where

$$\max_j \sqrt{\rho_j} \le \frac{\sum_{k=1}^{N}\sqrt{\rho_k}}{n} \tag{2}$$

Equation (2) implies that the square root of the population of the largest U.S. county must be no greater than the sum of the square root of the population in each U.S. county, divided by the sample size.

Sampling was carried out using SAS's SURVEYSELECT procedure, which utilizes the Hanurav-Vijayan (Vijayan, 1968; see also Fox, 1989) algorithm for probability proportional to size (PPS) selection without replacement. Provided that the assumption of Equation (2) holds, this algorithm produces a sample with probabilities of selection as displayed in Equation (1). Note that if we had attempted to used the actual county populations for sampling, instead of their square roots, the assumption of Equation (2) would fail to hold, which reflects that the skew is too heavy in favor of the larger counties in this case.

Probabilities of Selection for Fire Departments

This section describes the construction of the probabilities of selection, π_{ifc}, for a fire department i in a county c. π_{ifc} is required to compute survey weights for fire departments, as described in the main document.

Determining the Sampling Scheme

We followed one of two schemes in each county to select departments for the sample, depending on the distribution of departments with HAZMAT capability across the departments' organizational strata: all volunteer, all paid, and combination. From here on, department stratum refers to this classification. Which scheme we used will affect how the weights are computed in the county.

Let N_c be the total number of fire departments in county c. For each department $i \in \{1 \ldots Nc\}$ in county c, define:

v_{ic} = 1 if department is Volunteer, else 0

p_{ic} = 1 if department is Paid, else 0
c_{ic} = 1 if department is Combination, else 0
h_{ic} = 1 if department has HAZMAT capability, else 0

Then the number of HAZMAT departments in each stratum, volunteer, paid, and combination, respectively, in county *c* is:

$$HV_c = \sum_{i=1}^{N_c} v_{ic} h_{ic} \quad (1)$$

$$HP_c = \sum_{i=1}^{N_c} p_{ic} h_{ic} \quad (2)$$

$$HC_c = \sum_{i=1}^{N_c} c_{ic} h_{ic} \quad (3)$$

Now, the number of *strata* of departments in county *c* with HAZMAT capability is:

$HT_c = \min(1, HV_c) + \min(1, HP_c) + \min(1, HC_c)$

We chose the sampling scheme, $S_c \in \{1, 2\}$, for county *c* according to:

$$S_c = \begin{cases} 1 & if \quad HT_c < 2 \\ 2 & if \quad HT_c \geqslant 2 \end{cases}$$

More Definitions

We need a few more definitions before we can write down the expressions for weighting under each scheme in each county *c*:

$V_c = \sum_{i=1}^{N_c} v_{ic}$ # of volunteer departments
$P_c = \sum_{i=1}^{N_c} p_{ic}$ # of paid departments
$C_c = \sum_{i=1}^{N_c} c_{ic}$ # of combination departments
$H_c = HV_c + HP_c + HC_c$ # of HAZMAT departments

Sampling Scheme One

This scheme was used if, out of the three department strata in a county, at most one had any fire departments with HAZMAT capability. In this case, we considered volunteer, paid, and combination departments separately and randomly selected one respondent from each group so that the probability of selection, π_{ifc}, for a department just depends on its stratum.

So, for a county with $S_c = 1$,

$$\pi_{ifc} = \begin{cases} \frac{1}{V_c} & if \quad v_{ic} = 1 \\ \frac{1}{P_c} & if \quad p_{ic} = 1 \\ \frac{1}{C_c} & if \quad c_{ic} = 1 \end{cases} \quad (4)$$

or just

$$\pi_{ifc} = \frac{1}{p_{ic}P_c + v_{ic}V_c + C_c c_{ic}} \qquad (5)$$

Sampling Scheme Two

Here there were two stages. First, one department was selected randomly from all HAZMAT departments, irrespective of its stratum. We then noted the stratum of the department that was selected and ruled this stratum out from further sampling in the county. This left either one or two strata of departments, depending on the county. In the second stage, one department was randomly selected from each of the remaining strata.

For HAZMAT departments, then, π_{ifc} is determined by the chance of getting selected in the first round, $\frac{1}{H_c}$, plus the likelihood of getting selected in a subsequent round given *i*'s stratum wasn't the same as the department chosen in the first round. For example, for a volunteer department *i*, the chance *i*'s stratum was not chosen in the first round is $1 - \frac{HV_c}{H_c}$. That is one minus the chance a HAZMAT of *i*'s stratum, volunteer, *was* selected from among all HAZMATs. So, if $S_c = 2$ and $h_{ic} = 1$:

$$\pi_{ifc} = \begin{cases} \frac{1}{H_c} + (1 - \frac{HV_c}{H_c})\frac{1}{V_c} & if\ v_{ic} = 1 \\ \frac{1}{H_c} + (1 - \frac{HP_c}{H_c})\frac{1}{P_c} & if\ p_{ic} = 1 \\ \frac{1}{H_c} + (1 - \frac{HC_c}{H_c})\frac{1}{C_c} & if\ c_{ic} = 1 \end{cases} \qquad (6)$$

The last case is if $h_{ic} = 0$, a non-HAZMAT department in a county using the second sampling scheme. Here, there is no chance of selection in the first round, but the chance of selection in a subsequent round is the same.

So, if $S_c = 2$ and $h_{ic} = 0$:

$$\pi_{ifc} = \begin{cases} (1 - \frac{HV_c}{H_c})\frac{1}{V_c} & if\ v_{ic} = 1 \\ (1 - \frac{HP_c}{H_c})\frac{1}{P_c} & if\ p_{ic} = 1 \\ (1 - \frac{HC_c}{H_c})\frac{1}{C_c} & if\ c_{ic} = 1 \end{cases} \qquad (7)$$

Estimated Coefficients for Non-response Models

Dependent Variable is Response=1 (i.e. Response=yes)

	Law Enforcement	Fire Departments	Hospitals	Public Health Departments
County-level Variables:				
Northeast	-0.93	-0.60	-1.24	-0.92
South	-0.09	-0.55	-0.39	-0.87
West	0.79	-0.24	-0.39	-0.87
pop	0.20	---	---	---
urban	---	---	---	0.69
Organizational variables:				
have_911	-0.76	---	---	---
paid	---	0.11	---	---
volunteer	---	-1.14	---	---
hazmat	---	0.39	---	---
fte Q2	---	---	0.22	---
fte Q3	---	---	1.17	---
fte Q4	---	---	0.86	---
β_{g0}	-1.15	0.93	-0.28	0.42
N*	208	443	208	202

*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.

"---" indicates that the variable was excluded from the model.

The characters fte Q2, fte Q3 and fte Q4 are indicators of the 2nd, 3rd and 4th quartiles of the sample distribution of full-time equivalent physicians.

The Midwest region, combination fire departments and the 1st quartile of FTE were all used as reference categories for identifiability of the logistic regression models (i.e. the effects of the Northeast, South and West regions are all relative to the Midwest).

Description of the Data Files

Law Enforcement

National Public Safety Information Bureau's (NPSIB's) 2000 National Directory of Law Enforcement Administrators (NDLEA) provides contact information for over 36,600 law enforcement organizations throughout the U.S. with descriptions of personnel, size of population served, type of department, and department specializations, among others. The NDLEA had been used previously in a separate RAND study, the 2000 Law Enforcement Technology Survey, where no serious questions were encountered regarding the completeness or bias of the NDLEA data.

Fire Departments and Emergency Medical Services

The NPSIB's 2000 National Directory of Fire Chiefs and EMS Administrators provides contact information for the administrators of over 28,700 fire departments and 6,000 EMS departments throughout the U.S. In 1991, the NPSIB compiled its initial list of departments by requesting a listing from State agencies. Each year since 1991, the NPSIB has contacted each department in the directory in order to verify and update data for each entry, including contact information, size of population served, number of emergency response personnel, type of department, specializations, and financial structure. New entries are added to the list passively, as NPSIB is updated by various agencies or gets word of a new department at trade shows and other events.

Unfortunately, the NPSIB does not attempt to summarize the quality of its data or estimate the fraction of departments unaccounted for, so that the completeness of sampling frames based on NPSIB data is unknown. However, the directory is the most comprehensive listing available and is the only nationwide listing that claims comprehensiveness with respect to volunteer departments.

Hospitals

The American Hospital Association's (AHA) 1997 Annual Survey of Hospitals profiles a universe of more than 6,000 hospitals throughout the United States. The survey is mailed in October of each year to the hospital administrator of every hospital in the U.S. Estimates are generated for missing data on the basis of their values in previous years. Individual hospitals are contacted for clarification and verification of specific responses that fail edit tests. There are seven separate subject areas presented in the data: reporting period, classification, facilities and services, beds and utilization by inpatient service, total beds and utilization, financial data, and hospital personnel. Although the AHA's survey provides the most comprehensive sampling frame of hospitals available, the frame is incomplete to the extent that hospitals do not respond to AHA's survey. In 1997, the AHA achieved a response rate of 85% for the subset of general medical and surgical hospitals.

Public Health Departments

The National Association of City and County Health Organization's (NACCHO's) membership list for the current year, 2001, provides contact information for 2,948 public health organizations throughout the U.S. The list is not a complete enumeration of all city and county public health organizations, but instead a list of those organizations who have chosen to become members in the Association. To the extent that organizations do not choose to become members, the sampling frame is incomplete.

Offices of Emergency Management

We were unable to identify any current and comprehensive list of OEMs or emergency managers. The most relevant list we identified through an extensive search was compiled in 1987 by the International Association of Emergency Managers. As expected, due to its age the contact it provided were largely inaccurate. Though time intensive, nearly all county OEMs were identified through calls to other county agencies and State offices of emergency management.

Data sources used to identify State-level organizations are described in the main document, in the section titled, "Selecting State-level Organizations."

TAB 5—THE SURVEY INSTRUMENT

Survey Format

The information collected across the various local and State response organizations followed a similar format as shown in the survey outline in Figure 5A. The third survey instrument contained seven sections: (1) Emergency Response Planning Activities; (2) Resourcing Preparedness Activities; (3) Responding to Specific Terrorist Incidents; (4) Assessment of Federal Programs; (5) Intelligence Information and Warning; (6) Other Homeland Security Issues, and (7) Organizational Information.

Figure 5A. Survey III Instrument Outline

Section 1. Emergency Response Planning Activities
▪ Organizational participation in emergency response planning activities ▪ Changes made to emergency response plans since September 11, 2001 ▪ Joint preparedness activities ▪ Training and exercises ▪ Equipment acquisition or purchasing since September 11, 2001 ▪ Creation of new organizational structures since September 11, 2001 ▪ Communications interoperability issues
Section 2. Resourcing Preparedness Activities
▪ Changes in spending or reallocation of resources made following September 11, 2001 ▪ Receipt of external funding and/or resources to support preparedness activities ▪ Priority assigned by organizations to expending resources in this area
Section 3. Responding to Specific Terrorist Incidents
▪ Ranking incident types according to importance to the organization to prepare for ▪ Self-assessed ratings of preparedness to respond to top-ranked incident type ▪ Self-assessed areas of weaknesses and support needs to improve response capabilities
Section 4. Assessment of Federal Programs
▪ Participation in Federal programs since September 11, 2001 ▪ Factors that limit participation in Federal programs ▪ Views and expectations of Federal preparedness programs ▪ Expectations of the Department of Homeland Security
Section 5. Intelligence Information and Warning
▪ Intelligence warning and application for security clearances ▪ Views regarding the Homeland Advisory Security System
Section 6. Other Homeland Security Issues
▪ Organizational experience since September 11, 2001 with actual terrorist hoaxes and/or incidents ▪ Risk assessment and support needs ▪ Views regarding the role of the Federal Military and State National Guard ▪ Organizational experience with call-ups of reserve personnel
Section 7. Organizational Information
▪ Organizational characteristics including type of organization, size of organization, size of jurisdiction and size of population served

In addition to the above sections, several questions at the end collected information on the individual completing the survey, and provided an opportunity for the respondent to share additional, open-ended comments and suggestions regarding changes or improvements in Federal and State programs for terrorism preparedness, as well as other issues of importance to their organization that the survey had not addressed.

Pretesting The Survey Instrument

Once the initial draft instrument was ready, the surveys were reviewed and pretested over a period of three months to refine and test the draft questionnaire. Individuals pretesting the surveys included members of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, in addition to other experts in each survey field. Survey instruments then were revised according to feedback between each round of pretest and/or review. This iterative testing process was essential in helping us to pinpoint and fix instrument problems, streamline questioning, and attempt to reduce respondent burden.

Overview Of The Fielding Process

The data collection process for this study followed the model of that designed for the first wave of the study in 2001: that is, it operated as a mail survey (with telephone follow-up) with individually crafted questions for each responder population. The primary components involved in the fielding of the study were as follows: an advance letter accompanied by a one-page summary of how previous survey results had helped informed the Advisory Panel's third and fourth reports to Congress; inclusion of a motivating cover letter signed by the Chairman of the Advisory Panel (James S. Gilmore, III), enclosed with the survey packet itself; telephone follow-up to assure arrival of the survey and to emphasize the importance of the study; establishment of a toll-free 800 number to field respondent questions; follow-up postcard reminders mailed two weeks post-survey mailing; the mailing of a second, replacement survey; a final round of telephone follow-up; and lastly, an endorsement letter signed by designated Panel members representing each of the responder communities were sent to those groups with low response rates (EMS, hospitals, public health, and volunteer fire departments).

Fielding of the Survey

Data collection for this survey was primarily conducted between July and September 2003. In order to better manage the fielding process, the nine types of organizations were divided into groups, or "waves." The data collection schedule for each was staggered by approximately 6 days to allow the telephone survey staff adequate time to contact each respondent during the various phases of telephone follow-up. Each survey wave opened with an advance letter to the respondent indicating the importance of the survey, and alerting them to its imminent arrival. With the advance letter was enclosed the one-page summary described above. Advance letters were printed on RAND stationary, and signed by both the RAND study director, and former Virginia Governor and Panel Chairman James S. Gilmore, III. Seven days following the advance letter mailing, the survey was sent out with a cover letter, printed on Panel stationary and signed by Chairman Gilmore. As with the previous Panel surveys, the cover letter gave the addressee the option of assigning a knowledgeable survey designee if they deemed it appropriate. The survey itself was bound in the same brightly colored cover as was mailed to each in the Panel's first survey, designed to attract attention once removed from its envelope.

Seven days following the survey mailing, reminder postcards were sent out to all cases. The postcard thanked respondents if they had already filled out and returned the survey, but also prodded them to complete the survey if they had not already. The importance of the study and their participation in it was again communicated.

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 (the exception being State OEM, whose second packets were mailed five weeks after the initial survey mailing). In an effort to draw greater attention to the second packet and mitigate it getting lost in an inbox, brightly colored labels

printed with "A Request from the Gilmore Commission" were affixed to the front of each envelope, excepting the law enforcement and fire department samples (whose second mailings had already been mailed when this idea was conceived), and hospitals (to whom we mailed all second surveys via FedEx, based on our previous outreach experiences during fielding of the first and second surveys in 2001 and 2002 reaching this hard-to-reach population). A total of 171 second survey packets were mailed to the hospital sample via FedEx, with 64 hospital responses attributed to that FedEx mailing, which comprised 65 percent of the total hospital cases returned.

One week following this second survey mailing, second-round telephone follow-up began, with interviewers stepping up attempts to convert potential survey refusals. For the samples with the higher response rates at this stage, the second round calling was less intense than for those groups for which we had fewer responses. In particular, this period of telephone follow-up was most intensive and lengthy for the hospital group, as their response rates were substantially lower than for the other groups. Hospital respondents also proved to be the most difficult to reach by telephone, due to the nature of their occupations, and a particular emphasis in the second calling round was made to reach the respondents' assistants and managing nurses.

While the response rates for the majority of the groups were higher than 50 percent as the fielding period drew to a close, response rates for EMS, hospitals, public health, and volunteer fire remained low. Based on this, a decision was made to send out a final "endorsement" letter on RAND letterhead to those groups for whom response rates were lower than desirable. This endorsement letter (or in the case of OEM, an endorsement "announcement"), followed after the second survey had been mailed and the second round of phone follow-up completed. Each endorsement was made by the appropriate Gilmore Commission Panel member in each field, as follows: for hospitals, the endorsement letter was sent out under the signature of Kenneth Shine, MD, Former President of the Institute of Medicine; for public health, Patricia Quinlisk, MD, MPH, Medical Director and State Epidemiologist, Iowa Department of Public Health; for volunteer fire departments, Deputy Chief A.D. Vickery, Seattle Fire Department; and for EMS, Paul Maniscalco, MPA EMT/P, Past President, National Association of Emergency Medical Technicians; and Ellen Gordon, current President of the National Association of Emergency Managers (NAEM), who made an announcement at the NAEM conference on the study's behalf, asking OEM managers at their annual meeting to please complete the survey and return it to RAND.

BAR CODE LABEL

SURVEY III OF FEDERAL PREPAREDNESS PROGRAMS FOR COMBATING TERRORISM

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.

BATCH: | | | | |

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.

- ***Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives (CBRNE)*** – CBRNE incidents are typically defined as involving chemical, biological, radiological, or nuclear devices or high-yield explosives.

- ***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. Terrorist incidents may involve the use of CBRNE to cause mass casualties or higher probability/lower consequence attacks involving conventional explosives or chemical, biological, or radiological agents.

- ***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.

- *In this survey, we ask the respondent to keep in mind while answering the following questions that "preparedness" encompasses awareness, prevention, preparedness, response, and recovery.*

Acronyms Used in this Survey

ATTF	Anti-terrorism Task Force
BJA/OJP	Bureau of Justice Assistance/Office of Justice Programs
BW	Biological Weapon
CB	Chemical/Biological
CBIAC	Chemical and Biological Information Analysis Center
CBRN	Chemical, Biological, Radiological, Nuclear
CDC	Centers for Disease Control and Prevention, Department of Health and Human Services
CMI	Consequence Management Interoperability
CW	Chemical Weapon
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
EMS	Emergency Medical Services
EPA	Environmental Protection Agency
Epi-X	Epidemic Information Exchange
ER	Emergency Room
ERTP	Emergency Response Training Program, Environmental Protection Agency
FBI	Federal Bureau of Investigation, Department of Justice
FEMA	Federal Emergency Management Agency
FinCEN	Financial Crimes Enforcement Network
HAN	Health Alert Network
HAZMAT	Hazardous Materials
HHS	Department of Health and Human Services
ICS	Incident Command System
IRP	Improved Response Program
JTTF	Joint Terrorism Task Force
LEPC	Local Emergency Planning Committee or Commission
NDPO	National Domestic Preparedness Office, Federal Bureau of Investigation
NEIC	National Enforcement Investigation Center, Environmental Protection Agency
ODP/DHS	Office of Domestic Preparedness/Department of Homeland Security
OEP	Office of Emergency Preparedness, Department of Health and Human Services
OJP	Office of Justice Programs, Department of Justice
OSLDPS	Office for State and Local Domestic Preparedness Support, Office of Justice Programs, Department of Justice
PPE	Personal Protection Equipment
RRIS	Rapid Response Information System
SBCCOM	U.S. Army Soldier and Biological Chemical Command
SOP	Standard Operating Procedure
USACLMS	U.S. Army Chemical School
2-PAM	Pralidoxime chloride

Section 1:

EMERGENCY RESPONSE PLANNING ACTIVITIES

1. Does your organization have any individuals specifically assigned (full-time or part-time) to do emergency management or response planning?

(Mark One)

1 ❒ Yes

2 ❒ No

2. Since September 11, 2001, has your organization created a new position, unit, or group to address prevention, preparedness, response or recovery for terrorism-related incidents, or specially assigned personnel for this task?

(Mark All That Apply)

1 ❒ Created a special unit or position to address emergency preparedness for terrorism-related incidents

2 ❒ Assigned individual(s) (full-time or part-time) to specifically address emergency preparedness for terrorism-related incidents

3 ❒ Created an internal task force to address emergency preparedness for terrorism-related incidents within our organization

4 ❒ Assigned personnel to serve as liaisons to other responder agencies and/or task forces that are addressing emergency planning for terrorism-related incidents

5 ❒ Other *(please specify)*: _____

_____

6 ❒ **No, no such new positions, units, or groups have been created or assigned for terrorism-related purposes since September 11, 2001 ➔ *Skip to Question 4, Next Page***

3. Which of the following duties does this new position, unit, group, or specially assigned personnel perform?

(Mark All That Apply)

1 ❒ Analysis and dissemination of information

2 ❒ Training of other fire departments' personnel

3 ❒ Training of our own fire department personnel

4 ❒ Liaison with other local fire departments

5 ❒ Liaison with local law enforcement agencies

6 ❒ Provide logistical support to other fire departments in our jurisdiction or region

7 ❒ Liaison with state agencies

8 ❒ Liaison with Federal agencies

9 ❒ Liaison with the private sector (e.g., business, industry, nongovernmental organization)

10 ❒ Investigate specific terrorist incidents (e.g., arson-related)

11 ❒ Other (specify): _____

_____

4. Is your organization a member of an interagency disaster preparedness committee, task force, or working group <u>in your jurisdiction or region</u>?

(Mark One)

1 ❒ Yes ➔ ***Continue to Question 5***

2 ❒ No ➔ ***Skip to Question 7, Next Page***

5. Does this interagency disaster preparedness committee, task force, or working group address <u>local planning</u> for terrorism-related incidents?

(Mark One)

1 ❒ Yes

2 ❒ No

6. Does this interagency disaster preparedness committee, task force, or working group address <u>regional</u> (i.e., multi-jurisdictional) <u>planning</u> for terrorism-related incidents?

(Mark One)

1 ❒ Yes

2 ❒ No

7. Numerous task forces have been established to address terrorism prevention, preparedness, response and/or recovery. Of the following task forces, which ones does your organization participate in, liaison with, or are you an official member of?

(Mark All That Apply)

1 ❒ Your State's homeland security office task force

2 ❒ County/city-level interagency task force

3 ❒ Other (specify): _____

4 ❒ **None of the above**

8. Does your organization have formal agreements with other fire departments or response agencies for mutual aid?

(Mark One)

1 ❒ Yes

2 ❒ No

9. Since September 11th, 2001, 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 terrorism-related incidents in general

3 ❒ No new changes have been made to such agreements since 9/11

4 ❒ **No mutual aid agreements exist**

10. Does your organization have formal agreements with private companies, businesses, or labor unions in your jurisdiction or region to share information or resources in the event of an emergency or disaster?

(Mark One)

1 ❒ Yes, for coordination purposes

2 ❒ Yes, for response purposes (i.e., specialized equipment and/or personnel)

3 ❒ Yes, for planning purposes

4 ❒ No

11. Does your organization have a written emergency response plan?

(Mark One)

1 ❒ Yes ➔ ***Continue to Question 12, Next Page***

2 ❒ No ➔ ***Skip to Question 14, page 8***

12. 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 a plan for communicating with the public and / or the media?	1 ❒ Yes	2 ❒ No
c. 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
d. Address how your organization would communicate with health responders (e.g., hospitals, public health agencies) within your jurisdiction?	1 ❒ Yes	2 ❒ No
e. Address procedures for mass decontamination of victims? ..	1 ❒ Yes	2 ❒ No
f. Address procedures for individual decontamination?	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
i. Address integration with other local response plans?	1 ❒ Yes	2 ❒ No
j. Address integration with state response plans?	1 ❒ Yes	2 ❒ No
k. Address integration with the Federal Response Plan?	1 ❒ Yes	2 ❒ No
l. Address recovery phase and/or post-incident remediation ...	1 ❒ Yes	2 ❒ No
m. Address coordination with hospitals for multi-casualty incidents?	1 ❒ Yes	2 ❒ No

13. Has your organization updated or newly developed a <u>written emergency response plan</u> 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?

6 ❒ Attacks on critical infrastructure?

7 ❒ No, none of the above

14. Has your jurisdiction developed a contingency plan to accommodate (e.g., provide shelter to) large numbers of people seeking refuge from a nearby community or jurisdiction as a result of a terrorism-related incident?

(Mark One)

1 ❒ Yes, and we have exercised this contingency plan

2 ❒ Yes, but we have not yet exercised this contingency plan

3 ❒ No

4 ❒ Don't know

15. In the table below, please mark the appropriate boxes to indicate whether your organization has participated since September 11, 2001, in joint preparedness activities for natural disasters and / or terrorism-related incidents with any of the local organizations listed.

Since September 11, 2001, our organization has participated in *joint preparedness* activities with . . .

(Please Mark All That Apply)

	Natural disasters and emergencies with:	Terrorism-related incident response with:
A. LOCAL LAW ENFORCEMENT ORGANIZATIONS	1 ❒	2 ❒
B. OTHER FIRE DEPARTMENTS	1 ❒	2 ❒
C. FREE-STANDING HAZMAT ORGANIZATIONS	1 ❒	2 ❒
D. LOCAL HOSPITALS OR OTHER MEDICAL INSTITUTIONS	1 ❒	2 ❒
E. EMERGENCY MEDICAL SERVICES (EMS)	1 ❒	2 ❒
F. LOCAL HEALTH DEPARTMENTS	1 ❒	2 ❒
G. PUBLIC OR PRIVATE UTILITIES (E.G., WATER, POWER)	1 ❒	2 ❒
H. PUBLIC OR PRIVATE TRANSPORTATION ORGANIZATIONS	1 ❒	2 ❒
I. LOCAL OFFICE OF EMERGENCY MANAGEMENT OR PREPAREDNESS	1 ❒	2 ❒
J. SURROUNDING MUTUAL AID AGENCIES	1 ❒	2 ❒
K. LOCAL MILITARY INSTALLATIONS	1 ❒	2 ❒

0 ❒ **Our organization has not participated in joint preparedness activities with any of the above local organizations since September 11, 2001.**

16. In the table below, please mark the appropriate boxes to indicate whether your organization has participated in the past year in joint preparedness activities for natural disasters and / or terrorism-related incidents with any of the following state or federal organizations listed.

Our organization has participated (since September 11, 2001), in *joint preparedness* activities with . . .

(Please Mark All That Apply)

	Natural disasters and emergencies with:	Terrorism-related incident response with:
A. STATE LAW ENFORCEMENT AGENCIES	1 ❒	2 ❒
B. NATIONAL GUARD	1 ❒	2 ❒
C. STATE OFFICE OF EMERGENCY MANAGEMENT	1 ❒	2 ❒
D. STATE PUBLIC HEALTH DEPARTMENT	1 ❒	2 ❒
E. STATE EMERGENCY MEDICAL SERVICES (EMS)	1 ❒	2 ❒
F. FEDERAL MILITARY	1 ❒	2 ❒
G. FEDERAL BUREAU OF INVESTIGATION (FBI)	1 ❒	2 ❒

0 ❒ **Our organization has not participated in joint preparedness activities with any of the above state or federal organizations since September 11, 2001.**

17. What formal protocol for command and control does your organization use for emergency incidents?

(Mark All That Apply)

1 ❒ Incident Command System (ICS) as taught by the National Fire Academy

2 ❒ Incident management system (IMS)

3 ❒ Other standardized incident command and control or management system

4 ❒ None of the above

18. Does your organization participate in a statewide adopted incident command system?

(Mark One)

1 ❒ Yes

2 ❒ No, our organization does not participate in the statewide adopted incident command system

3 ❒ No, our state does not currently have a statewide adopted incident command system

Now we'd like to ask you some questions about communications interoperability.

By interoperability, we mean the ability of responders involved in an emergency to communicate in real-time within their organization and across agencies and/or jurisdictions via radio or telephone, in order to mount a well-coordinated response.

19. 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 units or organizations?

(Circle One Number For Each Line)

	INADEQUATE				EXCELLENT
Within your organization.....	1	2	3	4	5
Within your jurisdiction.....	1	2	3	4	5
Across multiple jurisdictions.....	1	2	3	4	5

20. Please indicate below if your organization has experienced communications interoperability problems with any of the following groups since September 11, 2001.

(Please Mark All That Apply)

	Within Your Jurisdiction	Outside Your Jurisdiction
A. Fire Departments	1 ❒	2 ❒
B. Police	1 ❒	2 ❒
C. EMS	1 ❒	2 ❒
D. Medical Organizations	1 ❒	2 ❒
E. Public Health Agencies	1 ❒	2 ❒
F. County Agencies	1 ❒	2 ❒
G. National Guard	1 ❒	2 ❒
H. State Agencies	1 ❒	2 ❒
I. Federal Military	1 ❒	2 ❒
J. Other Federal Agencies	1 ❒	2 ❒
K. Other (Please Specify): _____	1 ❒	2 ❒

0 ❒ **Yes, interoperability problems exist, but we've been able to find work-arounds (such as co-locating staff from different agencies in the emergency operations center).**

21. What factors, if any, limit efforts to improve the interoperability of your organization's communications system?

(Mark All That Apply)

1 ❒ Aging communications system and hardware

2 ❒ Lack of information or guidance on what technologies to purchase

3 ❒ Uncertainty surrounding the availability of spectrum for public safety use

4 ❒ Frequency incompatibility between emergency response organizations in our region

5 ❒ Lack of funding

6 ❒ Inter-agency politics / disagreements

7 ❒ Differences between jurisdictions in rules and regulations

8 ❒ Differences between jurisdictions or agencies in resource priorities

9 ❒ Differing technologies due to different brands of communications equipment

10 ❒ Other *(please specify)* _____

11 ❒ **No limits to improvement encountered**

22. Has any portion of your organization been trained in the following areas?

(Mark <u>One Box</u> for Each Item)

a. Incident command management	1 ❒ Yes	2 ❒ No
b. Threat and risk assessment	1 ❒ Yes	2 ❒ No
c. Decontamination procedures	1 ❒ Yes	2 ❒ No
d. Emergency response to biological incidents	1 ❒ Yes	2 ❒ No
e. Emergency response to hazardous materials incidents (e.g., chemical)	1 ❒ Yes	2 ❒ No
f. Emergency response to radiological/nuclear incidents	1 ❒ Yes	2 ❒ No
g. Use of personal protection equipment (PPE)	1 ❒ Yes	2 ❒ No
h. Detection of release of chemical or biological agents	1 ❒ Yes	2 ❒ No
i. Detection of release of radiological/nuclear agents	1 ❒ Yes	2 ❒ No
j. Prevention of terrorism-related incidents	1 ❒ Yes	2 ❒ No

23. What specific training courses have your personnel taken since September 11, 2001?

1 ❒ Name of training course(s): *(please specify)* _____

_____

_____

_____

24. What percentage of your <u>response personnel</u> are trained in the following areas?

(Please give your best estimate)

	Percent of Response Personnel Trained
a. Incident command or incident management	☐☐☐ %
b. Personal Protective Equipment Level A	☐☐☐ %
c. Personal Protective Equipment Levels B or C	☐☐☐ %
d. Hazardous Materials technician / specialist	☐☐☐ %
e. Certified Emergency Medical Technician - Intermediate	☐☐☐ %
f. Certified Emergency Medical Technician - Paramedic	☐☐☐ %
g. CBRNE awareness or response	☐☐☐ %

25. Since September 11th, 2001, has your organization . . .

(Mark <u>One Box</u> for Each Item)

a. Increased (or shifted over) the number of staff dedicated to addressing emergency preparedness for terrorism-related incidents ..... 1 ❒ Yes 2 ❒ No

b. Identified training opportunities for emergency response to terrorism-related incidents? ..... 1 ❒ Yes 2 ❒ No

c. Scheduled training for terrorism-related incidents? ..... 1 ❒ Yes 2 ❒ No

d. Trained personnel on emergency response for terrorism-related incidents (or are personnel in the process of being trained)? ..... 1 ❒ Yes 2 ❒ No

26. Since September 11, 2001, has your organization participated in any table-top exercises?
(Mark One)

1 ❒ Yes, and we received funding to participate in the exercise(s)

2 ❒ Yes, but we did not receive any funding for this purpose

3 ❒ No ➔ ***Skip to Question 29, Next Page***

27. Since September 11, 2001, has your organization participated in any field exercises?
(Mark One)

1 ❒ Yes, and we received funding to participate in the exercise(s)

2 ❒ Yes, but we did not receive any funding for this purpose

3 ❒ No ➔ ***Skip to Question 29, Next Page***

28. If so, please indicate for which type(s) of incidents and with what type of organizations.

(For Each Row, Mark All That Apply)

	With Local Organizations	***With State Organizations***	***With Federal Organizations***
In the past year, our organization has participated in exercises for:			
A. Chemical Incidents	1 ❒	2 ❒	3 ❒
B. Biological Incidents	1 ❒	2 ❒	3 ❒
C. Radiological Incidents	1 ❒	2 ❒	3 ❒
D. Cyber-Terrorism Incidents	1 ❒	2 ❒	3 ❒
E. Conventional Explosives Incidents	1 ❒	2 ❒	3 ❒
F. Natural Disasters	1 ❒	2 ❒	3 ❒
G. Critical Infrastructure Protection	1 ❒	2 ❒	3 ❒
H. Other *(Please Specify)*: _____	1 ❒	2 ❒	3 ❒

Equipment Issues

29. Since September 11th, 2001, has your organization purchased (or is it in the process of purchasing) any of the following types of equipment? If so, please indicate how much of your total force is being outfitted.

(Check One Choice For Each Line)

	All of the Force	*A Portion of the Force*	*Specialized Units Only*	*None of the Force*
Personal Protective Suits (PPE)				
A. PPE Level A: fully encapsulated	1 ❒	2 ❒	3 ❒	4 ❒
B. PPE Level B: liquid splash resistant	1 ❒	2 ❒	3 ❒	4 ❒
C. PPE Level C: liquid splash resistant	1 ❒	2 ❒	3 ❒	4 ❒
Respiratory protection				
D. N95 Respirator Masks	1 ❒	2 ❒	3 ❒	4 ❒
E. Self-contained breathing apparatus	1 ❒	2 ❒	3 ❒	4 ❒
F. Powered air purifying respirator	1 ❒	2 ❒	3 ❒	4 ❒
G. Closed-circuit breathing apparatus	1 ❒	2 ❒	3 ❒	4 ❒
H. Air purifying respirator	1 ❒	2 ❒	3 ❒	4 ❒
Additional equipment				
I. In-suit communications system	1 ❒	2 ❒	3 ❒	4 ❒
J. Personnel alert safety system (PASS)	1 ❒	2 ❒	3 ❒	4 ❒
K. Personal cooling system	1 ❒	2 ❒	3 ❒	4 ❒

30. Since September 11, 2001, has your organization purchased (or is it in the process of purchasing) any of the following types of equipment?

(Mark All That Apply)

1 ❒ Monitoring and detection equipment for chemical agents

2 ❒ Monitoring and detection equipment for radiological agents

3 ❒ Monitoring and detection equipment for biological agents

4 ❒ Monitoring and detection equipment for cyber detection

5 ❒ Equipment for decontamination of victims and/or sites

6 ❒ **No, we have not purchased any of these types of equipment since September, 11, 2001**.

31. Have antidotes for chemical or nerve agents been issued to your organization's response personnel?

(Mark One)

1 ❒ Yes

2 ❒ No

32. What funding sources were used to purchase the equipment listed in Questions 29 & 30?

(Mark All That Apply)

1 ❒ Used department's existing equipment budget to purchase the new equipment

2 ❒ Received additional funding from the city or county to purchase the new equipment

3 ❒ Received funding from our state government to purchase the new equipment

4 ❒ Received a federal grant to purchase the new equipment *(please specify name of the grant programs):* _____

5 ❒ We did not purchase ourselves the equipment indicated in Questions 29 & 30, but rather acquired some or all of it through another group (e.g., the military) that had received grant funding to purchase new equipment.

6 ❒ We did not purchase ourselves the equipment indicated in Questions 29 & 30, but rather acquired some or all of it through another group (e.g., the military) that gave our organization excess equipment they no longer needed.

7 ❒ We have not purchased nor are in the process of purchasing any of the equipment listed in Questions 29 & 30.

33. Is your organization coordinating its equipment/technology procurement process for terrorism-related needs with any other organizations?

(Mark All That Apply)

1 ❒ Coordinating with *similar* types of response organizations inside or outside of your jurisdiction or region (e.g., other fire departments)

2 ❒ Coordinating with *other* types of response organizations (e.g., police, EMS) within your jurisdiction or region

3 ❒ Coordinating with other response organizations within your mutual aid network

4 ❒ Coordinating with your local emergency planning group (or inter-agency task force)

5 ❒ Coordinating with a *multi-county* emergency planning group

6 ❒ Coordinating with your state's emergency planning group

7 ❒ Other *(please specify)*: _____
_____

8 ❒ **We are not coordinating our equipment procurement process with any other organization.**

34. Does your organization address both annual recurring maintenance costs and have a timetable for replacement of equipment needed to address terrorism?

(Mark One)

1 ❒ Yes

2 ❒ No

35. What factors, if any, limit your organization's ability to purchase equipment or technology for terrorism-related needs?

(Mark All That Apply)

1 ❒ Lack of standardization as to what equipment is available

2 ❒ Lack of information as to what equipment has been certified for use by our responder community

3 ❒ Available equipment is not appropriate for our concept of operations

4 ❒ Unsure as to what equipment/technology is needed to ensure our organization's preparedness for terrorism

5 ❒ Unsure what specific terrorism threats are most important for our organization to prepare for

6 ❒ Competing/higher priorities for spending our organization's equipment budget

7 ❒ Lack of sufficient funding

8 ❒ Other *(please specify)*: _____

_____

9 ❒ **No limits to purchasing ability**

36. Does your organization have any unit(s) specially trained and/or equipped to respond to terrorism-related incidents?

(Mark One)

1 ❒ Yes ➔ ***Continue to Question 37***

2 ❒ No, but other organizations we work with in our jurisdiction have such units ➔ ***Continue to Question 37***

3 ❒ No ➔ ***Skip to Question 38, Next Page***

37. What types of terrorism-related incidents are they trained to respond to?

(Mark All That Apply)

1 ❒ Chemical

2 ❒ Biological

3 ❒ Radiological

4 ❒ Cyber-terrorism

5 ❒ Large-scale conventional explosives

6 ❒ Nuclear

7 ❒ Other *(please specify)*: _____

38. How would you rate your organization's overall level of preparedness at present to respond to terrorism in general?

(Circle One Number)

INADEQUATE				EXCELLENT
1	2	3	4	5

39. How would you rate your organization's overall level of preparedness at present to respond to high consequence CBRNE terrorism, specifically?

(Circle One Number)

INADEQUATE				EXCELLENT
1	2	3	4	5

40. Since September 11, 2001, has your organization or jurisdiction used FEMA's Local Capability Assessment for Readiness (LCAR) tool to assess your community's readiness and emergency response capabilities?

(Mark One)

1 ❒ Yes

2 ❒ No

Section 2:

RESOURCING PREPAREDNESS ACTIVITIES

41. Since September 11th, 2001, has your organization increased its spending, or shifted resources internally, to address terrorism-related incidents?

(Mark All That Apply)

1 ❒ Yes, internally increased spending ➔ ***Continue to Question 42***

2 ❒ Yes, internally shifted resources ➔ ***Continue to Question 42***

3 ❒ No ➔ ***Skip to Question 43, Next Page***

42. If so, for what purpose(s)?

(Mark All That Apply)

1 ❒ Additional security for your organization

2 ❒ Staff overtime

3 ❒ Additional training of personnel

4 ❒ Purchase of personal protective equipment or other equipment (e.g., sensor equipment) specific to terrorism response

5 ❒ Planning activities specific to terrorism response

6 ❒ Additional security for your airport

7 ❒ Conduct or participate in tabletop and/or field exercises

8 ❒ Develop emergency response or contingency plans

9 ❒ Support interagency planning and coordination activities

10 ❒ Conduct a needs assessment for your organization

11 ❒ Create an anti-terrorism position, unit, or division

12 ❒ Assign personnel (full-time or part-time) to the local terrorism-related task force

13 ❒ Assign personnel (full-time or part-time) to the state terrorism-related task force

14 ❒ Other *(please specify)* _____

_____

43. Since September 11th, 2001, has your organization received an increase in its funding and / or resources for terrorism preparedness?

(Mark One)

1 ❒ Yes ➔ ***Continue to Question 44***

2 ❒ No ➔ ***Skip to Question 45***

44. 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)* _____

45. How high a priority is spending additional resources for combating terrorism, when compared to the other current needs of your organization?

(Mark One)

1 ❒ High priority

2 ❒ Somewhat of a priority

3 ❒ Low priority

4 ❒ Not at all a priority

Section 3:
RESPONDING TO SPECIFIC TERRORIST INCIDENTS

46. In what ways is your organization better or worse prepared today to respond to terrorism-related incidents as compared to September 11, 2001?

(Mark One Box for Each Line)

	Our organization is… Better Prepared	Worse Prepared
a. Adequate equipment for terrorism related incidents involving hazardous agents (e.g., chemical, biological, radiological)	1 ❒	2 ❒
b. Personnel trained in terrorism-related response	1 ❒	2 ❒
c. Personnel trained in incident command/management	1 ❒	2 ❒
d. Resources (e.g., personnel, funding) to address terrorism-related preparedness	1 ❒	2 ❒
e. Planning for terrorism-related incidents	1 ❒	2 ❒
f. Coordination of preparedness activities with other local response organizations and/or interagency task forces	1 ❒	2 ❒
g. Integration of preparedness activities with that of State and/or Federal agencies	1 ❒	2 ❒
h. Personnel dedicated to addressing terrorism-related preparedness	1 ❒	2 ❒
i. Other *(please specify)*: _____ _____.	1 ❒	2 ❒

1 ❒ Additional comments: _____

_____

_____

47. For the following types of incidents, please rank order to indicate how important it is for your organization to prepare for them, where 1=most important and 5=least important.

Please rank in order of importance, 1 – 5.

_____ **Biological**
_____ **Chemical**
_____ **Radiological**
_____ **Nuclear**
_____ **Conventional explosives**

48. How high a priority is it for your organization to expend resources preparing for the type of incident you ranked as most important in Question 47?
(Mark One)

1 ❒ High priority

2 ❒ Somewhat of a priority

3 ❒ Low priority

4 ❒ Not at all a priority

Considering the type of incident you ranked as most important in Question 47, please rate your organization's level of readiness on a scale of 1 to 5, with 1 being INADEQUATE and 5 being EXCELLENT.

Please circle one number for each question on the 5-point scale given below.

49. Your organization's written emergency **plan** to be used during a response to an event similar to the one you selected is:

INADEQUATE				EXCELLENT
1	2	3	4	5

50. Your organization's **knowledge and expertise** about response to this type of event are:

INADEQUATE				EXCELLENT
1	2	3	4	5

51. Your organization's **equipment** to respond to this type of event is:

INADEQUATE				EXCELLENT
1	2	3	4	5

52. Your organization's **training** to prepare for this type of event is:

INADEQUATE				EXCELLENT
1	2	3	4	5

53. Your organization's **exercises** to prepare for this type of event are:

INADEQUATE				EXCELLENT
1	2	3	4	5

54. 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

55. How would you rank your organization's **overall preparedness to respond** to this type of event?

INADEQUATE				EXCELLENT
1	2	3	4	5

56.Again, for the type of incident you ranked as most important in Question 47, which of your response capabilities do you think are the weakest?

(Mark All That Apply)

1 ❒ Hazard ID and detection

2 ❒ Protection of response personnel from exposure to harmful agents

3 ❒ Medical treatment of victims

4 ❒ Mass care (e.g., bulk distribution of food, shelter, and basic necessities)

5 ❒ Decontamination of victims

6 ❒ Communication / coordination with local response organizations

7 ❒ Communication / coordination with state and Federal agencies

8 ❒ Media and information management

9 ❒ Coordination with local hospitals

10 ❒ Coordination with local public health agencies

11 ❒ Basic operations during this kind of incident

12 ❒ None of the above ➔ ***Skip to Question 58, Page 24***

57. What item(s) would be <u>most</u> helpful to strengthen the response capabilities you indicated as weaknesses in Question 56?

(Mark All That Apply)

1 ❒ New or more up-to-date equipment

2 ❒ Training courses for personnel (including "train the trainers")

3 ❒ Exercises

4 ❒ Better integration of preparedness activities with local response organizations

5 ❒ Better integration of preparedness activities with state agencies

6 ❒ Better integration of preparedness activities with Federal agencies

7 ❒ Information and reference materials about responding to this kind of incident

8 ❒ Improved facilities

9 ❒ Personnel

10 ❒ Technical support

11 ❒ Funding of overtime/backfill costs to send personnel to training

12 ❒ Other *(please specify)*:

_____

_____

Section 4:
ASSESSMENT OF FEDERAL PROGRAMS

In answering Questions 58-60, please also keep in mind applications submitted, but for which funding has not yet been received.

58. Since September 11, 2001, has your organization been informed about or applied for agency-specific funding, training, equipment, or other terrorism preparedness support available from the Federal government, regardless of whether or not you received it?

(Mark One)

1 ❒ Yes

2 ❒ No

59. Since September 11, 2001 has your organization received agency-specific funding, training, equipment, or other terrorism preparedness support from the Federal government?

(Mark One)

1 ❒ Yes ➔ ***Continue to Question 60***

2 ❒ No ➔ ***Skip to Question 61, Next Page***

60. How were the Federal terrorism resources that your organization received used?

(Mark One)

1 ❒ Shared with other organizations in your region

2 ❒ Used only by your organization

61. Since September 11, 2001, has your organization participated in any Federally-sponsored programs for funding, equipment, or training to improve terrorism preparedness? If so, please indicate which ones:

(Mark All That Apply)

1 ❒ NDPO Equipment Research and Development Program

2 ❒ OJP Anti-Terrorism State and Local Training Grants (SLATT)

3 ❒ FEMA Emergency Management Institute course(s) (terrorism-related only)

4 ❒ National Fire Academy Emergency Response to Terrorism course(s)

5 ❒ U.S. Army Chemical School (USACLMS) Training Program

6 ❒ DOE Training for Radiological Emergencies

7 ❒ New Mexico Tech's Incident Response to Terrorist Bombings course

8 ❒ Other National Domestic Preparedness Consortium training courses

9 ❒ EPA Emergency Response Training Program (ERTP)

10 ❒ FBI Hazardous Devices School

11 ❒ ODP/DHS State and Local Domestic Preparedness Equipment program

12 ❒ ODP/DHS State and Local Domestic Preparedness Exercise program

13 ❒ Assistance to Firefighters Grant Program

14 ❒ ODP/DHS State Homeland Security Grant Program (2003)

15 ❒ ODP/DHS Urban Areas Security Initiative (2003)

16 ❒ ODP/DHS State and Local Domestic Preparedness Training and Technical Assistance Program

17 ❒ Other *(please specify)* : _____

18 ❒ **We have not participated in any such Federally-sponsored programs.**

62. Which of the above programs have been the most helpful to your organization?

Name of Program: _____

_____

63. Since September 11, 2001, has your organization used or obtained <u>information or technical assistance</u> for terrorism preparedness or response from any of the following Federally-sponsored resources?

(Mark All That Apply)

1 ❒ Chemical Weapons Improved Response Program (CW IRP)

2 ❒ Biological Weapons Improved Response Program (BW IRP)

3 ❒ CDC's Health Alert Network (HAN)

4 ❒ CDC's Epidemic Information Exchange (Epi-X)

5 ❒ FBI's National Domestic Preparedness Office (NDPO)

6 ❒ FEMA Rapid Response Information System (RRIS)

7 ❒ Chemical and Biological (CB) Hotline

8 ❒ DOT Emergency Response Guidebook

9 ❒ DoD Chemical and Biological Information Analysis Center (CBIAC)

10 ❒ DoD Consequence Management Interoperability Services (CMI)

11 ❒ ODP Technical Assistance Program

12 ❒ ODP State and Local Domestic preparedness Support Helpline

13 ❒ SBCCOM technical evaluation and information program

14 ❒ Interagency Board (IAB)

15 ❒ Other *(please specify)*:_____

16 ❒ **We have not used or obtained information or technical assistance from any of the above sources since September 11, 2001.**

Please indicate how much you agree or disagree with the following statements:

64. Federal terrorism preparedness funding that is being distributed <u>through state governments</u> is reaching local organizations and communities with the greatest need.

(Mark One Box)

Strongly Disagree	*Disagree*	*Neither Agree Nor Disagree*	*Agree*	*Strongly Agree*
1 ❒	2 ❒	3 ❒	4 ❒	5 ❒

65. Terrorism preparedness funding being distributed by the Federal government <u>directly to local communities and local responders</u> is reaching the organizations and communities with the greatest need.

(Mark One Box)

Strongly Disagree	*Disagree*	*Neither Agree Nor Disagree*	*Agree*	*Strongly Agree*
1 ❒	2 ❒	3 ❒	4 ❒	5 ❒

66. Our jurisdiction has had to move forward on its own with measures to improve local preparedness for terrorism without guidance from the Federal level.

(Mark One Box)

Strongly Disagree	*Disagree*	*Neither Agree Nor Disagree*	*Agree*	*Strongly Agree*
1 ❒	2 ❒	3 ❒	4 ❒	5 ❒

67. Information and guidance from the Federal government about terrorism preparedness is adequate for helping local responders prepare for terrorism.

(Mark One Box)

Strongly Disagree	*Disagree*	*Neither Agree Nor Disagree*	*Agree*	*Strongly Agree*
1 ❒	2 ❒	3 ❒	4 ❒	5 ❒

68. Federal Government programs for improving local responder terrorism preparedness . . .

(Circle One Choice for Each Line)

	Strongly Disagree		***Neither Agree Nor Disagree***		***Strongly Agree***
a. are carefully coordinated and well-organized	1	2	3	4	5
b. are flexible enough to allow our organization to use Federal funding and resources as we see fit.....	1	2	3	4	5
c. are taking funding and resources away from more important priorities	1	2	3	4	5
d. are focused on highly unlikely scenarios at the expense of more likely scenarios	1	2	3	4	5
e. should provide threat and risk assessment information to local response organizations	1	2	3	4	5
f. are so numerous that we have difficulty in figuring out what is relevant to our organization	1	2	3	4	5
g. are of little use to our organization	1	2	3	4	5
h. fit well with our community's local preparedness strategy	1	2	3	4	5
i. should involve dedicated Federal assets so that local response organizations can concentrate on their primary mission	1	2	3	4	5
j. should provide intelligence about terrorist activities to local response organizations	1	2	3	4	5
k. should promote research and development of new technologies to combat terrorism.....	1	2	3	4	5
l. should involve better coordination between the Federal Government and local responders	1	2	3	4	5
m. should help our organization strengthen the security of our computer systems against cyber-terrorist attacks	1	2	3	4	5
n. provide insufficient time between notices of funding opportunities and grant submittal deadlines	1	2	3	4	5

69. What is the *single most important* way that the Federal government can support the efforts of local organizations like yours to improve their terrorism preparedness?

(Mark <u>ONE</u> Box Only)

1 ❒ Direct financial support

2 ❒ Equipment procurement

3 ❒ Training or training aids

4 ❒ Exercise coordination and support

5 ❒ Distribution of terrorism technical information

6 ❒ Research and development on terrorism preparedness and response

7 ❒ Outreach to state and local organizations

8 ❒ Dissemination of intelligence data

9 ❒ Evaluation of new technologies and equipment

10 ❒ Setting standards for equipment and training

11 ❒ Perform technical evaluation

12 ❒ Provide venues for information sharing

13 ❒ Provide guidance on benchmarks for measuring or assessing organizational preparedness

14 ❒ Provide funding to pay for overtime/backfill costs for sending personnel to training courses

15 ❒ Other *(please specify)*:_____

16 ❒ **No improvement needed**

70. In general, what factors limit your organization's ability to participate in Federally-sponsored <u>training</u> programs?

(Mark All That Apply)

1 ❒ Not eligible to participate in these programs

2 ❒ Unaware of what Federal training programs are available

3 ❒ Content is not relevant to our organization's needs

4 ❒ Time commitment is excessive

5 ❒ Training is not scheduled during times when our personnel can attend

6 ❒ Backfill requirements to send personnel for training are burdensome

7 ❒ Personnel shortages do not allow our organization to free up personnel for training

8 ❒ Lack dollars to pay staff overtime to attend training (or to pay backfill)

9 ❒ Programs are poorly organized and/or difficult to understand

10 ❒ Limited training budget

11 ❒ Application process is too involved

12 ❒ We do not have an individual dedicated to researching and/or training opportunities to filling out applications for our organization

13 ❒ Uncertain as to what training programs would be most beneficial for our organization to improve preparedness for terrorism

14 ❒ Training is not conducted at locations convenient to our organization

15 ❒ Other *(please specify)*: _____

_____

16 ❒ We have other more important training priorities to worry about

17 ❒ Our organization's preparedness would not be improved through participation

18 ❒ **We have not been limited in our ability to participate in Federally-sponsored training programs.**

71. In general, what factors limit your organization's ability to participate in Federally-sponsored <u>equipment</u> programs?

(Mark All That Apply)

1 ❒ Not eligible to participate in these programs

2 ❒ Unaware of what Federal equipment programs are available

3 ❒ The equipment made available is not relevant to our organization's needs

4 ❒ Application process is too involved

5 ❒ Programs are poorly organized and/or difficult to understand

6 ❒ Limited equipment procurement budget

7 ❒ We do not have an individual dedicated to researching equipment program opportunities and/or to filling out applications for our organization

8 ❒ Uncertain as to what equipment programs would be most beneficial for our organization to improve preparedness for terrorism

9 ❒ Other *(please specify)*: _____

_____

10 ❒ We have other more important equipment procurement priorities to worry about

11 ❒ Our organization's preparedness would not be improved through participation

12 ❒ **We have not been limited in our ability to participate in Federally-sponsored equipment programs.**

72. In the event of a terrorist-related incident, what type of support do you expect the Federal government to provide for your locality?

(Mark All That Apply)

1 ❒ Provide technical expertise during the event

2 ❒ Assist with crisis management

3 ❒ Assist with consequence management

4 ❒ Provide technical information during the event in an actionable form

5 ❒ Assist our organization or locality in obtaining specialized equipment, personnel or units to augment local response capabilities

6 ❒ Assist with intelligence gathering

7 ❒ Provide logistical support

8 ❒ Other *(please specify)*:_____

_____

73. Setting aside incident-specific support, what other type of ongoing support would you like the Federal government to provide to your locality?

(Mark One)

1 ❒ Threat assessment intelligence information (information as to what type of threat your locality should be preparing for)

2 ❒ Technical information on ways of preparing for terrorism (e.g., certification, ___ standardization)

3 ❒ Information as to what resources are available to your organization

4 ❒ Information on training and equipment grant programs

5 ❒ Information on best practices for terrorism-related preparedness

6 ❒ Other *(please specify)*:_____

Now we are going to ask you specifically about the new Department of Homeland Security (DHS).

74. What type of support are you looking specifically to the new Department of Homeland Security to provide to local responders?

(Mark All That Apply)

1 ❒ Funding

2 ❒ Training

3 ❒ Assistance with planning

4 ❒ Standardization and certification of equipment and training

5 ❒ Research and development

6 ❒ Testing of new equipment

7 ❒ Assistance with emergency response

8 ❒ Guidance on benchmarks that can be used to measure or assess organizational preparedness

9 ❒ Other *(please specify)*: _____

75. In what way(s) do you expect the new Department of Homeland Security to impact your organization?

(Mark All That Apply)

1 ❒ Improve coordination between the federal/state/local levels in terrorism preparedness

2 ❒ Improve information-sharing between the federal/state/local levels

3 ❒ Improve communications among federal/state/local levels

4 ❒ Provide better/standardized templates and/or guidance to assist with planning

5 ❒ Improve integration between the public and private sectors' efforts to improve terrorism preparedness and to protect critical infrastructure

6 ❒ Establish a single point of contact at the federal-level for information on available programs (including means for state and local response organizations to provide feedback on programs)

7 ❒ Establish a primary contact at the federal-level instead of many on training, equipment, planning, and other critical needs

8 ❒ Consolidate the numerous training courses and programs being offered to local responders

9 ❒ Consolidate the numerous equipment programs

10 ❒ Streamline the grant application process for federally-sponsored training and/or equipment programs

11 ❒ Provide intelligence information and more detailed guidance on terrorist threat

12 ❒ Assist in the conduct of threat assessments for your jurisdiction or region

13 ❒ Standardize the grant application process across federal agencies

14 ❒ Consolidate multiple grant application requirements into a single set of requirements

15 ❒ Other *(please specify)*:_____

Section 5:

INTELLIGENCE INFORMATION AND WARNING

76. What organizations does your organization contact if it has threat information to pass on regarding suspected terrorist activities within your jurisdiction or region?

(Mark All That Apply)

1 ❒ Local FBI field office

2 ❒ FBI's Joint Terrorism Task Force (JTTF)

3 ❒ County/city-level interagency task force

4 ❒ Your State's Homeland Security Office

5 ❒ U.S.-led Attorney General Anti-Terrorism Task Force (ATTF) within your State

6 ❒ Other law enforcement agencies (state or local)

7 ❒ Private sector groups (e.g., businesses, airlines, utilities, etc.)

8 ❒ Public health agencies (if a biological, radiological, or chemical threat)

9 ❒ Bureau of Immigration and Customs Enforcement

10 ❒ U.S. Department of Homeland Security (DHS)

11 ❒ U.S. Department of Energy (DoE)

12 ❒ Other local responders

13 ❒ Other state responders

14 ❒ Other *(please specify)*:_____

77. Since September 11, 2001, has your organization received any guidance from the FBI regarding what type of information about suspected terrorist activity should be collected by local fire departments and/or passed onto FBI field offices?

(Mark One)

1 ❒ Yes

2 ❒ No

78. Since September 11, 2001, has your organization <u>applied for</u> government security clearances for its personnel?

(Mark One)

1 ❒ Yes ➔ ***Continue to Question 79, Next Page***

2 ❒ No ➔ ***Skip to Question 81, Next Page***

79. If yes, for how many personnel?

(Please give your best estimate)

Number of personnel that have applied for government security clearances: _____

80. How many of these personnel have <u>received</u> their government clearance?

(Mark One)

1 ❒ All of the personnel that have applied

2 ❒ Some of the personnel that have applied

3 ❒ None that have applied since 9/11 have received their government clearances

The following questions are about the Homeland Security Advisory System (5-colored system), where the five threat conditions represent differing levels of risk of terrorist attacks.

81. When the threat-level increases from elevated (yellow) to high (orange), does your organization make changes to its normal operations?

(Mark One)

1 ❒ Yes ➔ ***Continue to Question 82***

2 ❒ No ➔ ***Skip to Question 83, Next Page***

82. If yes, what changes are made?

(Mark All That Apply)

1 ❒ Increase the security for your organization

2 ❒ Stand-up the emergency operations center

3 ❒ Mobilize specialized units (e.g., anti-terrorism teams)

4 ❒ Redirect personnel from non-essential areas

5 ❒ Increase overtime

6 ❒ Increase length of work shifts

7 ❒ Cancel staff vacations and leave

8 ❒ We investigate first whether the threat is relevant to our jurisdiction before making any changes (e.g., contact our local FBI field office or colleagues)

9 ❒ Other *(please specify)*:_____

_____

83. In your opinion, what modifications, if any, would improve the usefulness of the Homeland Security Advisory System for your organization?

(Mark All That Apply)

1 ❒ Use a regional alert system to notify emergency responders about threats specific to their jurisdiction or region

2 ❒ Provide more detailed information through existing communications channels (not the media) as to what type of incident is likely to occur

3 ❒ Provide more detailed information as to where the threat is likely to occur

4 ❒ Provide more detailed information as to during what period of time the threat is likely to occur

5 ❒ Provide training to emergency responders as to what protective actions are necessary at different threat levels

6 ❒ After an increase in threat-level, have the DHS follow-up on what additional actions ought to be undertaken

7 ❒ Other *(please specify)*: _____

_____

8 ❒ **No improvements are necessary to the Homeland Security Advisory System.**

Section 6:

OTHER HOMELAND SECURITY ISSUES

84. 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?

(Mark One)

1 ❒ Yes ➔ ***Continue to Question 85***

2 ❒ No ➔ ***Skip to Question 86, Next Page***

85. Did any of these terrorist incidents and/or hoaxes involve the use (or threat of use) of the following?

(Mark All That Apply)

1 ❒ Anthrax

2 ❒ Other biological agent

3 ❒ Toxic industrial materials

4 ❒ Toxic industrial chemicals

5 ❒ Other chemical agents

6 ❒ Radiological agent

7 ❒ Conventional explosives

8 ❒ Cyber-terrorism

9 ❒ Military-grade weapons (e.g., automatic weapons, rifles, mortars)

10 ❒ Agroterrorism

11 ❒ Arson and/or incendiary devices

12 ❒ Attacks on critical infrastructure

13 ❒ Other *(please specify)*:_____

14 ❒ **None of the above**

86. <u>Since September 11, 2001</u>, has your organization conducted a risk assessment to identify key threats or vulnerabilities within your jurisdiction or region?

(Mark One)

1 ❒ Yes, a risk assessment was conducted specifically for terrorism

2 ❒ Yes, a risk assessment was conducted for a wide range of contingencies including terrorism

3 ❒ No, a risk assessment was not conducted ➔ ***Skip to Question 88***

87. Who conducted the risk assessment?

(Mark All That Apply)

1 ❒ Our fire department

2 ❒ Jointly conducted by our fire department and local law enforcement

3 ❒ An inter-agency task force

4 ❒ FBI

6 ❒ Other *(please specify)*: _____

7 ❒ Don't know

88. What type of support does your organization need in order to conduct future risk assessments?

(Mark All That Apply)

1 ❒ Protocols for conducting and/or evaluating risk assessments

2 ❒ Training on how to conduct risk assessments

3 ❒ Better intelligence and terrorist threat/capability information from the Federal government

4 ❒ Outside consultant expertise to assist with risk assessment

5 ❒ Funding and/or personnel to conduct the assessment

6 ❒ Other (briefly describe): _____

_____

7 ❒ **No additional support is needed.**

B. Role of the Military

89. What roles do you feel would be appropriate for the Federal military to play during a response to a domestic terrorism-related incident?

(Mark All That Apply)

1 ❒ Maintain order and / or provide security

2 ❒ Advise other response organizations on technical and / or logistical matters

3 ❒ Conduct a rapid needs assessment to determine what kind of response is required

4 ❒ Provide personnel and equipment to support local, State, and / or Federal agencies

5 ❒ Set up kitchens, clinics, and mass care facilities for victims and relief workers

6 ❒ No form of participation by the military would be appropriate

7 ❒ Enforcement of quarantine

8 ❒ Other *(please specify)*:_____

90. What roles do you feel would be appropriate for the State National Guard to play during a response to a domestic terrorism-related incident?

(Mark All That Apply)

1 ❒ Maintain order and / or provide security

2 ❒ Advise other response organizations on technical and / or logistical matters

3 ❒ Conduct a rapid needs assessment to determine what kind of response is required

4 ❒ Provide personnel and equipment to support local, State, and / or Federal agencies

5 ❒ Set up kitchens, clinics, and mass care facilities for victims and relief workers

6 ❒ No form of participation by the National Guard would be appropriate

7 ❒ Enforcement of quarantine

8 ❒ Other *(please specify)*:_____

91. Does your organization keep records on the military reserve status (Federal Reservists or State National Guard) of its personnel?

(Mark One)

1 ❒ Yes ➔ ***Continue to Question 92***

2 ❒ No ➔ ***Skip to Question 93***

92. How many call-ups of personnel who are military reservists has your organization experienced since September 11, 2001?

(Please give your best estimate)

1 ❒ **Number of Response Personnel: _____**

2 ❒ **Number of Senior Staff: _____**

3 ❒ **Number of Total Staff: _____**

4 ❒ **None of our personnel were called-up ➔ *Skip to Question 94***

93. To what extent did these call-ups impact the ability of your organization to respond to emergencies?

(Mark One)

1 ❒ Greatly impacted our ability to respond to emergencies

2 ❒ Moderately impacted our ability to respond to emergencies

3 ❒ Mildly impacted our ability to respond to emergencies

4 ❒ No impact on our ability to respond to emergencies

94. Does your organization have a plan in place to backfill personnel who are mobilized as part of a call-up of military reservists (Federal reservists or State National Guard)?

(Mark One)

1 ❒ Yes

2 ❒ No

95. How would you rate the likelihood of the following types of major terrorism-related incidents (e.g., more than 30 individuals with serious injuries) occurring within your jurisdiction or region in the next 5 years?

Please keep in mind that "cyber-terrorism" is defined as the disruption of critical infrastructure or key information systems for more than one day.

(Mark One Box on Each Row)

	Very Unlikely	*Somewhat Unlikely*	*Somewhat Likely*	*Very Likely*
a. Terrorism-related chemical incident	1 ❒	2 ❒	3 ❒	4 ❒
b. Terrorism-related biological incident	1 ❒	2 ❒	3 ❒	4 ❒
c. Terrorism-related radiological incident	1 ❒	2 ❒	3 ❒	4 ❒
d. Terrorism-related nuclear incident	1 ❒	2 ❒	3 ❒	4 ❒
e. Conventional explosives terrorism incident	1 ❒	2 ❒	3 ❒	4 ❒
f. Cyber-terrorism incident	1 ❒	2 ❒	3 ❒	4 ❒
g. Terrorism incident involving the use of military-grade weapons (e.g., automatic weapons, rifles, mortars)	1 ❒	2 ❒	3 ❒	4 ❒
h. Attack on critical infrastructure	1 ❒	2 ❒	3 ❒	4 ❒
i. Arson and/or incendiary device	1 ❒	2 ❒	3 ❒	4 ❒
j. Other *(please specify)*: _____	1 ❒	2 ❒	3 ❒	4 ❒

Section 7:
ORGANIZATIONAL INFORMATION

96. Does your organization specialize in any of the following functions, in addition to your core fire department role?

(Mark All That Apply)

1 ❒ Hazardous materials containment and / or clean-up (HAZMAT)

2 ❒ Emergency Medical Services (EMS)

3 ❒ Specialized rescue response capabilities

4 ❒ Other *(please specify)*: _____

5 ❒ **None of the above ➔ *Skip to Question 98***

97. Which of the following services does your organization provide regionally or to another jurisdiction as part of a mutual aid agreement?

(Mark All That Apply)

1 ❒ Hazardous materials containment and/or clean-up (HAZMAT)

2 ❒ Emergency Medical Services (EMS)

3 ❒ Specialized rescue response capabilities

4 ❒ Other *(please specify)*: _____

5 ❒ **We do not provide any of the above services regionally or to other jurisdictions**

98. Which of the following categories best describes your agency?

(Mark One)

1 ❒ Volunteer department only

2 ❒ Paid department only

3 ❒ Combination department (both paid and volunteer personnel)

99. What is the size of your organization? ***(Please give your best estimate)***

- Number of paid firefighter personnel: ..... ☐☐,☐☐☐
- Number of volunteer firefighter personnel: ..... ☐,☐☐☐
- Number of HAZMAT personnel: ..... ☐,☐☐☐
- Number of EMS personnel: ..... ☐,☐☐☐

100. What is the size of the population your organization serves?
(Mark One)

1 ❒ 1 – 15,000

2 ❒ 15,001 – 30,000

3 ❒ 30,001 – 65,000

4 ❒ 65,001 – 250,000

5 ❒ 250,001 – 1,000,000

6 ❒ 1,000,001 +

101. What type of jurisdiction does your organization serve?
(Mark One)

1 ❒ City

2 ❒ City/County

3 ❒ County

4 ❒ Multi-county or regional (within your state)

5 ❒ State

6 ❒ Other *(please specify)*: _____

ADDITIONAL COMMENTS

102. Do you personally serve a specific terrorism-related role within your organization?

(Mark One)

1 ❒ Yes *(briefly describe)* : _____

_____

2 ❒ No

Thank you for taking the time to complete this survey. If this questionnaire did not address all of the terrorism-related issues of importance to your organization, please use this space or attach additional pages to add comments or clarifications.

103. Does your organization have other suggestions for changes or improvements in *Federal programs* for terrorism preparedness that this survey has not covered?

_____

_____

_____

_____

_____

_____

_____

104. Does your organization have other suggestions for changes or improvements in *State programs* for terrorism preparedness that this survey has not covered?

_____

_____

_____

_____

_____

_____

_____

105. Has your organization's experiences or challenges in preparing for domestic terrorism incidents resulted in other lessons learned that were not addressed in this survey?

_____

_____

_____

_____

_____

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 R**, tel. 877-287-4995, or feel free to e-mail me at Lois_Davis@rand.org).**

TAB 7—SURVEY TABULATIONS

This Tab presents the tables of results summarized in the main body of Appendix D. The table results have been statistically adjusted to account for oversampling and non-response. The reader should refer to Tab 2 for a discussion of the comparison between the distribution of funding and support and preparedness activities and to Tab 3 for details regarding participation in Federally-sponsored programs. Tabs 1, 4, and 5 discuss the methodology used in this study. For each table, we show in the table note and in parentheses the question numbers that correspond to the fire department survey instrument (shown in Tab 6). This Tab is organized around the sections shown in Appendix D.

Want More Intelligence Information About The Terrorist Threat, But Security Clearances Are Lagging

Table 7A. Percent of Organizations That Would Like the Federal Government to Disseminate Intelligence Data

	Percent of Organizations That Would Like the Federal Government to Disseminate Intelligence Data	Percent of Organizations That Would Like DHS Specifically to Provide Intelligence Information and More Detailed Guidance on Terrorist Threat
Local Response Organizations		
Law Enforcement	18 (5)	62 (5)
Local/Regional EMS*	13 (3)	43 (5)
Local OEM	9 (3)	46 (6)
Paid/Combo Fire	7 (2)	45 (7)
Volunteer Fire	18 (2)	35 (8)
State Organizations		
State EMS	3 (2)	59 (5)
State OEM	19 (6)	73 (6)
Health Organizations		
Hospital	9 (4)	--
Local Public Health	17 (6)	45 (9)
State Public Health	10 (3)	56 (5)

Standard error of the estimate is shown in parentheses. Dashes in the tables indicate that a particular organizational type was not asked the question or given a particular response option. For example, in Table 7A hospitals were not asked the question regarding DHS. * Local/ regional EMS organizations were not selected randomly. We display standard errors for this group throughout this document so that the reader may gain a broader sense about the variability of these responses (on the same metric as the other organization types). However, generalizations of these results to a population broader than those local/regional EMS organizations that responded to the survey should not be inferred. (Questions 69 and 75)

Table 7B. Suggestions for Improving the Usefulness of the Homeland Security Advisory System With Respect to Threat Information Provided

	PERCENT OF ALL ORGANIZATIONS		
	"Provide more detailed information through existing communications channels as to the type of incident likely to occur"	**"Provide more detailed information as to where the threat is likely to occur"**	**"Provide more detailed information as to during what period of time the threat is likely to occur:**
Local Response Organizations			
Law Enforcement	71 (5)	77 (5)	65 (6)
Local/Regional EMS	75 (5)	67 (5)	61 (5)
Local OEM	75 (5)	73 (6)	62 (6)
Paid/Combo Fire	67 (7)	80 (4)	69 (5)
Volunteer Fire	69 (8)	59 (9)	49 (9)
State Organizations			
State EMS	72 (5)	65 (5)	66 (5)
State OEM	76 (6)	88 (5)	76 (6)
Health Organizations			
Hospital	75 (5)	60 (8)	63 (8)
Local Public Health	--	--	--
State Public Health	--	--	--

Standard error of the estimate is shown in parentheses. Local and State public health not asked this question. (Question 83)

Table 7C. Since 9/11, Have Organizations Received Guidance from the FBI as to What Type of Information They Should Collect Regarding Suspected Terrorist Activity?

	Percent of Organizations That Have Received Guidance from the FBI since 9/11 on Type of Information About Suspected Terrorist Activity That Should be Collected and/or Passed onto FBI Field Offices
Local Response Organizations	
Law Enforcement	47 (6)
Local/Regional EMS	--
Local OEM	42 (6)
Paid/Combo Fire	23 (5)
Volunteer Fire	2 (1)
State Organizations	
State EMS	--
State OEM	50 (7)
Health Organizations	
Hospital	25 (6)
Local Public Health	--
State Public Health	--

Standard error of the estimate is shown in parentheses. Local/regional and State EMS and local and State public health were not asked this question. (Question 77)

Table 7D. Whom Do Organizations Contact to Pass On Threat Information?

	Local FBI Field Office	FBI's JTTF	City/County Interagency Task Force	State's Homeland Security Office	U.S.-led ATTF
Local Response Organizations					
Law Enforcement	81 (5)	25 (5)	25 (5)	22 (5)	14 (4)
Local/Regional EMS	39 (5)	4 (2)	29 (5)	9 (3)	1 (1)
Local OEM	69 (6)	8 (2)	35 (6)	33 (7)	5 (2)
Paid/Combo Fire	53 (6)	13 (6)	40 (7)	13 (4)	8 (6)
Volunteer Fire	28 (9)	0.5 (0.5)	42 (9)	11 (6)	0
State Organizations					
State EMS	38 (5)	3 (2)	9 (3)	47 (5)	6 (3)
State OEM	73 (6)	54 (7)	15 (5)	77 (6)	38 (7)
Health Organizations					
Hospital	39 (7)	--	39 (8)	10 (4)	--
Local Public Health	--	--	44 (9)	20 (7)	0.1 (0.1)
State Public Health	--	--	22 (4)	81 (4)	17 (3)
	Law Enforcement (Other Than FBI)	**Public Health Agencies (if CBR threat)**	**Other Local Responders**	**Other State Responders**	**Private Sector**
Local Response Organizations					
Law Enforcement	66 (5)	15 (4)	30 (5)	22 (5)	6 (2)
Local/Regional EMS	78 (4)	30 (5)	21 (4)	10 (3)	7 (3)
Local OEM	74 (5)	55 (6)	52 (6)	29 (6)	14 (4)
Paid/Combo Fire	64 (6)	25 (6)	38 (6)	12 (4)	6 (3)
Volunteer Fire	72 (9)	12 (5)	24 (8)	24 (8)	3 (3)
State Organizations					
State EMS	69 (5)	66 (5)	13 (4)	41 (5)	6 (3)
State OEM	77 (6)	38 (7)	31 (6)	38 (7)	19 (6)
Health Organizations					
Hospital	88 (4)	69 (6)	--	--	--
Local Public Health	82 (5)	57 (10)	49 (9)	34 (7)	13 (5)
State Public Health	67 (4)	72 (4)	36 (4)	47 (5)	17 (3)

Standard error of the estimate is shown in parentheses. (Question 76)

Table 7E. Since 9/11, Which Organizations Have Applied for Security Clearances?

	Percent
LOCAL ORGANIZATIONS	
Law Enforcement	7 (2)
Local/Regional EMS	5 (2)
Local OEM	6 (2)
Paid/Combo Fire	2 (1)
Volunteer Fire	0 (0)
STATE ORGANIZATIONS	
State EMS	16 (4)
State OEM	88 (4)
HEALTH ORGANIZATIONS	
Hospital	6 (3)
Local Public Health	8 (4)
State Public Health	86 (3)

Standard error of the estimate is shown in parentheses. (Question 78)

Table 7F. Of Those Organizations That Applied for Security Clearances, How Many Orgs Have Received Clearances for Their Personnel?

	Of Those Organizations That Applied For A Security Clearance, How Many of Their Personnel Have Received a Clearance?		
	All of Their Personnel That Applied (Percent of Orgs That Applied)	Some of Their Personnel That Applied (Percent of Orgs That Applied)	None of Their Personnel That Applied (Percent of Orgs That Applied)
Local Response Organizations			
Law Enforcement	56 (15)	25 (13)	19 (11)
Local/Regional EMS	33 (33)	33 (33)	34 (33)
Local OEM	60 (18)	30 (15)	10 (8)
Paid/Combo Fire	89 (10)	6 (8)	5 (4)
Volunteer Fire	--	--	--
State Organizations			
State EMS	0	40 (23)	60 (23)
State OEM	9 (4)	48 (8)	43 (8)
Health Organizations			
Hospital	70 (32)	30 (32)	0
Local Public Health	97 (3)	1 (1)	3 (3)
State Public Health	10 (3)	30 (5)	60 (6)

Standard error of the estimate is shown in parentheses. (Question 80)

Table 7G. Since 9/11, How Many Organizations Have Conducted Risk Assessments and Where Do They Need Support?

Has Your Org. Conducted a Risk Assessment Since 9/11?		Type of Support Needed to Conduct Future Risk Assessments (Percent of All Orgs)			
Local Response Organizations	Percent of All Orgs	Better Intelligence on Terrorist Threat/ Capability Info	Protocols	Training on How to Conduct	No Additional Support Needed
Law Enforcement	59 (6)	30 (5)	44 (6)	57 (6)	14 (4)
Local/Region-al EMS	45 (5)	41 (5)	66 (5)	67 (5)	5 (2)
Local OEM	85 (4)	44 (6)	57 (6)	48 (6)	5 (2)
Paid/Combo Fire	65 (7)	41 (7)	55 (7)	57 (7)	8 (3)
Volunteer Fire	18 (6)	34 (8)	65 (8)	75 (7)	7 (5)
State Organizations					
State EMS	57 (6)	39 (6)	43 (6)	61 (6)	0
State OEM	92 (4)	54 (7)	50 (7)	38 (7)	8 (4)
Health Organizations					
Hospital	70 (8)	36 (7)	56 (8)	61 (7)	5 (3)
Local Public Health	42 (8)	31 (7)	68 (8)	68 (8)	1 (1)
State Public Health	80 (4)	50 (5)	58 (5)	53 (5)	8 (3)

Standard error of the estimate is shown in parentheses.(Questions 86,88)

Incident Types Organizations Consider Most Important To Prepare Is Consistent With Their Mission, But They Vary In Priority Placed

Table 7H. How do Local and State Responders Rank Each Type of Incident in Order of Importance?

	Rank Order of Incidents by Organizational Type									
Incident Type	**Fire Vol.**	**Fire Paid**	**Law**	**Local OEM**	**Local/RegEMS**	**State OEM**	**State EMS**	**Hosp**	**Loc PH**	**State PH**
Biological	3	3	3	3	3	3	1	2	1	1
Chemical	42	32	32	1	1	2	2	1	2	2
Radiol.	44	44	44	4	4	4	4	4	3	3
Nuclear	55	55	55	5	5	5	5	5	5	5
Conv. Explosive	1	1	1	2	2	1	3	3	4	4

State and local organizations were asked to rank order the different types of incidents – biological, chemical, radiological, nuclear, conventional explosives – in terms how important it is for their organization to prepare for that type of incident. Organizations were asked to rank order the incidents from 1 to 5, where 1=most important to prepare for and 5=least important to prepare for. Based on the mean scores, Table 8 shows the relative ranking of each type of incident by the different organizations. (Question 47)

Table 7I. How High a Priority is the Top-Ranked Incident to Expend Resources Preparing For?

	Percent of All Organizations			
Organizational Type	**High Priority**	**Somewhat of a Priority**	**Low Priority**	**Not at all a Priority**
Top-Ranked Incident: Conventional Explosives				
Law Enforcement	16 (5)	38 (5)	33 (5)	13 (4)
Paid/Combo Fire	13 (4)	50 (6)	28 (5)	9 (3)
Volunteer Fire	8 (4)	32 (8)	38 (9)	21 (7)
State OEM	56 (7)	40 (7)	4 (3)	0
Top-Ranked Incident: Bioterrorism				
Local Public Health	40 (8)	52 (9)	6 (3)	2 (1)
State Public Health	69 (4)	22 (4)	8 (3)	0
State EMS	43 (6)	40 (6)	10 (3)	7 (3)
Top-Ranked Incident: Chemical				
Hospital	14 (4)	56 (7)	23 (6)	7 (4)
Local/Regional EMS	15 (4)	52 (5)	24 (5)	9 (3)
Local OEM	29 (5)	51 (6)	15 (5)	5 (3)

Standard error of the estimate is shown in parentheses. (Question 48)

Table 7J. What Do Organizations View as Being Their Weakest Response Capabilities for Top-Ranked Incident?

	Percent of All Organizations						
			Communic/Coord				
Local Response Organizations	**Hazard ID and Detect**	**Protection of Response Personnel**	**W/Local Response Orgs.**	**With State or Fed. Orgs**	**Medical Treatment of Victims**	**Mass Care**	**Decon of Victims**
Law Enforcement	41 (6)	68 (5)	24 (5)	39 6)	20 (4)	41(6)	43 (6)
Local/Region. EMS	39 (5)	55 (5)	30 (5)	50(5)	25 (5)	42(5)	39 (5)
Local OEM	47 (6)	59 (6)	30 (6)	44(6)	37 (6)	50(6)	38 (6)
Paid/Combo Fire	42 (7)	56 (7)	17 (3)	52(7)	35 (7)	52(7)	39 (7)
Volunteer Fire	39 (9)	77 (7)	25 (7)	39(9)	50 (9)	61(9)	65 (8)
State Organizations							
State EMS	34 (5)	31 (5)	45 (6)	34(5)	21 (5)	24(5)	45 (6)
State OEM	28 (6)	12 (5)	36 (7)	36(7)	40 (7)	24(6)	16 (5)
Health Organizations							
Hospital	47 (8)	40 (7)	16 (5)	30(8)	13 (5)	--	28 (6)
Local Public Health	48 (9)	54 (9)	17 (5)	24(6)	24 (6)	48(10)	60 (8)
State Public Health	21 (4)	18 (4)	24 (4)	9 (3)	48 (5)	58(5)	27 (4)

Standard error of the estimate is shown in parentheses. (Question 56)

Table 7K. What Would Be Most Helpful to Strengthen Indicated Weaknesses in Response Capabilities?

	Percent of All Organizations				
Local Response Organizations	**Training Courses**	**Exercises**	**New or More Up-to-date Equipment**	**More Personnel**	**Tech. Support**
Law Enforcement	88 (3)	76 (5)	85 (4)	63 (6)	61 (6)
Local/Region. EMS	--	64 (6)	58 (6)	42 (6)	53 (6)
Local OEM	76 (5)	64 (6)	79 (4)	57 (6)	37 (6)
Paid/Combo Fire	87 (3)	74 (5)	73 (5)	64 (7)	45 (6)
Volunteer Fire	74 (11)	66 (10)	68 (10)	35 (9)	42 (9)
State Organizations					
State EMS	--	74 (6)	41 (6)	41 (6)	30 (6)
State OEM	52 (8)	67 (8)	33 (8)	57 (8)	10 (5)
Health Organizations					
Hospital	64 (8)	55 (8)	34 (6)	27 (6)	32 (6)
Local Public Health	88 (4)	79 (6)	59 (9)	39 (8)	63 (8)
State Public Health	44 (5)	56 (5)	19 (4)	53 (5)	28 (5)

Standard error of the estimate is shown in parentheses. (Question 57)

Organizations' Views Regarding Funding Needs

Table 7L.Organizations Desire Funding Support from the Federal Government to Help Improve Preparedness for Terrorism

	Percent of Orgs Desire Funding Support from the Federal Government to Pay for Overtime/ Backfill Costs for Sending Personnel to Training	**Percent of Orgs Indicated Direct Financial Support from the Federal Government Would Help Them Improve Their Preparedness for Terrorism**	**Percent of Orgs That Are Looking Toward DHS Specifically for Funding Support**
LOCAL ORGANIZATIONS			
Law Enforcement	19 (5)	62 (6)	89 (3)
Local/Regional EMS	22 (4)	55 (5)	82 (4)
Local OEM	20 (5)	66 (6)	95 (3)
Paid/Combo Fire	21 (5)	64 (6)	89 (4)
Vol Fire	7 (3)	70 (8)	91 (4)
STATE ORGANIZATIONS			
State EMS	20 (5)	37 (5)	88 (4)
State OEM	15 (5)	50 (7)	92 (4)
HEALTH ORGANIZATIONS			
Hospital	--	63 (7)	68 (9)
Local Public Health	--	67 (7)	--
State Public Health	--	81 (4)	--

Standard error of the estimate is shown in parentheses. Hospitals and public health organizations not asked about overtime/backfill costs; public health not asked about type of support looked toward DHS for. (Questions 69 and 74)

Table 7M. Funding Cited as a Limiting Factor In Ability of Organizations to Participate in Federal Training and Equipment Programs

	Funding as a Limiting Factor in Terms of Participation in Federal Training Programs		Funding as a Limiting Factor in Terms of Participation in Federal Equipment Programs
	Lack Budget to Pay Staff Overtime to Participate in Training (Percent)	Org Has a Limited Training Budget (Percent)	Org Has a Limited Equipment Procurement Budget (Percent)
LOCAL ORGANIZATIONS			
Law Enforcement	72 (5)	70 (5)	62 (5)
Local/Regional EMS	50 (5)	48 (5)	40 (5)
Local OEM	58 (6)	65 (6)	--
Paid/Combo Fire	67 (6)	57 (7)	40 (6)
Vol Fire	26 (7)	66 (8)	58 (8)
STATE ORGANIZATIONS			
State EMS	40 (6)	66 (8)	17 (4)
State OEM	44 (7)	20 (6)	--
HEALTH ORGANIZATIONS			
Hospital	55 (8)	55 (7)	--
Local Public Health	--	--	--
State Public Health	--	--	--

Standard error of the estimate is shown in parentheses. Public health organizations not asked about what factors limit participation in Federal training programs. Health organizations not asked about what factors limit their participation in Federal equipment programs. (Questions 70 and 71)

Table 7N. What Factors Limit Organizations' Ability to Purchase Specialized Equipment for Terrorism Response?

	Percent of All Organizations		
	Competing/ Higher Budget Priorities	Unsure of Org's Equipment Needs	Lack Information as to What Equipment Has Been Certified
LOCAL ORGANIZATIONS			
Law Enforcement	65 (5)	41 (6)	25 (5)
Local/Regional EMS	63 (5)	30 (5)	25 (5)
Local OEM	57 (6)	24 (5)	20 (5)
Paid/Combo Fire	41 (6)	26 (4)	22 (5)
Vol Fire	37 (8)	36 (8)	17 (5)
STATE ORGANIZATIONS			
State EMS	45 (6)	17 (4)	21 (5)
State OEM	36 (7)	16 (5)	20 (6)
HEALTH ORGANIZATIONS			
Hospital	66 (8)	39 (7)	30 (6)
Local Public Health	-	--	--
State Public Health	--	--	--

Standard error of the estimate is shown in parentheses. Public health not asked this question. (Question 35)

Table 7O. Percent of Organizations Indicated Need for Funding and/or Personnel to Support Risk Assessment Activities

	Indicated Need for Funding And/or Personnel To Conduct Future Risk Assessments (Percent)
LOCAL ORGANIZATIONS	
Law Enforcement	61 (6)
Local/Regional EMS	68 (5)
Local OEM	76 (5)
Paid/Combo Fire	65 (7)
Vol Fire	65 (10)
STATE ORGANIZATIONS	
State EMS	61 (6)
State OEM	77 (6)
HEALTH ORGANIZATIONS	
Hospital	51 (8)
Local Public Health	78 (7)
State Public Health	50 (5)

Standard error of the estimate is shown in parentheses. (Question 88)

Table 7P. Following 9/11, Which Organizations Increased Spending or Internally Reallocated Resources to Improve Response Capabilities?

	Did Org Increase Spending/Shift Resources Internally Since 9/11?	To Do Planning	To do Training	To Purchase PPE/Equip.	Did Org Receive External Funding and/ or Resources To Support These Activities?
LOCAL ORGANIZATIONS	**Percent**	**%**	**%**	**%**	**Percent**
Law Enforcement	18 (4)	9 (3)	14 (3)	8 (2)	13 (4)
Local/Regional EMS	46 (5)	69 (7)	31 (5)	17 (4)	35 (5)
Local OEM	42 (6)	30 (5)	32 (6)	28 (5)	62 (6)
Paid/Combo Fire	29 (6)	19 (6)	25 (6)	20 (6)	20 (4)
Vol Fire	1 (1)	.10 (.70)	1 (.70)	1 (.70)	0
STATE ORGANIZATIONS					
State EMS	81 (4)	66 (5)	63 (5)	22 (5)	67 (5)
State OEM	85 (5)	81 (6)	58 (7)	38 (7)	92 (4)
HEALTH ORGANIZATIONS					
Hospital	66 (7)	32 (6)	60 (7)	47 (8)	44 (7)
Local Public Health	70 (12)	--	--	--	--
State Public Health	94 (2)	--	--	--	--

Standard error of the estimate is shown in parentheses. Numbers represent percent of all organizations. (Questions 41, 42, and 43)

For tables of results and comparison regarding association between receipt of funding and steps organizations have undertaken to improve response capabilities—see Tab 2 to Appendix D.

Organizations Differ in their Participation in Federally Sponsored Programs and their Expectations of DHS and the Federal Government in General

Table 7Q.Since 9/11, Percent of Organizations That Have Participated in Federally Sponsored Programs

	Percent of Organizations That Have Participated in Federally Sponsored Programs Since 9/11
LOCAL ORGANIZATIONS	
Law Enforcement	42 (6)
Local/Region. EMS	46 (5)
Local OEM	83 (5)
Paid/Combo Fire	73 (5)
Vol Fire	31 (7)
STATE ORGANIZATIONS	
State EMS	87 (4)
State OEM	100
HEALTH ORGANIZATIONS	
Hospital	50 (8)
Local Pub. Health	70 (12)
State Pub. Health	100

Standard error of the estimate is shown in parentheses. Organizations were asked whether since 9/11 they had participated in agency-specific Federally sponsored funding, training, or equipment programs. (Question 61)

Table 7R. Since 9/11, Percent of Organizations Received Support from the Federal Government for Terrorism Preparedness

	Informed About/ Applied for Support From Federal Government (Percent All Orgs)	Rec'd Funding, Training, Equipment, or Other Support from Federal Government (Percent All Orgs	Of Those Orgs That Received Federal Support, How Was it Used?	
			Shared With Other Organizations in Region (Percent)	Used Only by Their Organization (Percent)
Local Organizations				
Law Enforcement	52 (6)	24 (5)	69 (13)	31 (13)
Local/Regional EMS	55 (5)	36 (5)	78 (7)	22 (7)
Local OEM	95 (3)	79 (5)	88 (5)	12 (5)
Paid/Combo Fire	75 (5)	44 (6)	71 (7)	29 (7)
Vol Fire	65 (8)	15 (7)	47 (25)	53 (25)
State Organizations				
State EMS	84 (4)	72 (5)	96 (3)	4 (3)
State OEM	100	100	100	0
Health Organizations				
Hospital	69 (7)	42 (8)	43 (13)	57 (13)
Local Public Health	--	--	--	--
State Public Health	--	--	--	--

Standard error of the estimate is shown in parentheses. Public health not asked question since all would have been informed about bioterrorism funding released by the Federal government following 9/11. (Questions 58, 59, and 60)

Table 7S. Does Distribution Mode of Federal Funding Affect Whether It Reaches Those with Greatest Need?

	Opinion Regarding Federal Support Distributed Through the State (Mean)	Opinion Regarding Federal Support Distributed Directly to Local Communities and Responders (Mean)
Local Organizations		
Law Enforcement	2.3 (0.1)	2.3 (0.1)
Local/Regional EMS	2.2 (0.1)	2.3 (0.1)
Local OEM	3.0 (0.1)	2.8 (0.1)
Paid/Combo Fire	2.6 (0.1)	2.7 (0.1)
Vol Fire	2.2 (0.2)	2.3 (0.2)
State Organizations		
State EMS	2.7 (0.1)	2.4 (0.1)
State OEM	4.2 (0.1)	2.9 (0.1)
Health Organizations		
Hospital	2.6 (0.1)	2.7 (0.1)
Local Public Health	3.0 (0.3)	--
State Public Health	4.0 (0.1)	--

Standard error for each point estimate is shown in parentheses. Scale runs from 1=strongly disagree; 3=neither agree or disagree; 5=strongly agree. (Questions 64 and 65)

Table 7T. Do Organizations Feel Jurisdiction/State Has Had to Move Forward with Terrorism Preparedness Without Federal Guidance?

	Mean Score
Local Organizations	
Law Enforcement	3.3 (0.1)
Local/Regional EMS	3.4 (0.1)
Local OEM	3.0 (0.1)
Paid/Combo Fire	3.2 (0.1)
Vol Fire	3.4 (0.2)
State Organizations	
State EMS	2.8 (0.1)
State OEM	3.0 (0.2)
Health Organizations	
Hospital	3.3 (0.1)
Local Public Health	--
State Public Health	--

Standard error for each point estimate is shown in parentheses. Scale runs from 1=strongly disagree; 3=neither agree or disagree; 5=strongly agree. Public health not asked this question. (Question 66)

Table 7U. In What Ways Do Local/State Responders Expect the DHS to Impact Them?

	Activities
70-80% expect DHS to…	▪ Improve coordination, information-sharing, and communication between Federal/State/local levels
60-70% expect DHS to…	▪ Streamline grant application process across Federal grant programs
50-60% expect DHS to…	▪ Standardize the grant application process across Federal agencies and consolidate multiple grant application requirements
40-60% expect DHS to…	▪ Establish single point of contact at Federal level for information on available programs ▪ Provide primary contact at Federal level instead of many on training, equipment, planning and other critical needs o *Health orgs. not asked this question*
45-60% expect DHS to…	▪ Provide intelligence information and more detailed guidance on terrorist threat
40-60% expect DHS to…	▪ Consolidate numerous training courses/ programs and numerous equipment programs o *Health orgs. not asked about equipment programs*
40-60% expect DHS to…	▪ Provide better/standardized templates and/or guidance to help with planning
30-40% expect DHS to…	▪ Improve integration between public/private sectors' efforts to improve terrorism and protect critical infrastructure
30-40% expect DHS to…	▪ Help conduct threat assessment for jurisdiction or region o *Hospitals not asked this question*

(Question 75)

Table 7V. In What Ways Can the Federal Government Support Public Health Organizations' Efforts to Improve Preparedness?

Type of Support Looking Toward Federal Government For	Local Public Health (Percent)	State Public Health (Percent)
Enhance current surveillance systems	20 (6)	3 (2)
Assist with development of local and regional response plans	22 (6)	6 (2)
Establish centralized communication system for notification regarding disease outbreaks related to bioterrorism	19 (6)	3 (2)
Establish integrated, multi-level laboratory response network for bioterrorism	15 (5)	6 (2)
Establish rapid response and advanced technology lab for chemical agents	16 (5)	6 (2)
Assist with the exercising of local and regional response plans	19 (6)	10 (3)
Assist with development of plans to coordinate local/regional medical systems	17 (6)	0
Assist with the development of plans to coordinate local/regional veterinarian systems	12 (5)	3 (2)

Standard error of the estimate is shown in parentheses. Public health organizations were asked in what ways the Federal government (e.g., through the CDC, DHHS, USPHS) can support the efforts of public health departments like theirs to improve terrorism preparedness. (Question 58, Local Public Health Survey)

Table 7W. In What Ways Can the Federal Government Support Organizations' Efforts to Improve Preparedness? – Areas of Disagreement

Type Of Support Looking Toward Federal Government For	Percent of Orgs	Exceptions (Percent)
Equipment procurement	20-35%	0% of State Public Health and State OEMs
Training or training aids	25-40%	7-8% of State Public Health and State OEMs
Outreach to State/local organizations	10-20%	3-4% of State Public Health and State OEMs
Distributing technical information	0-20%	5-6% of State Public Health and State EMS

(Question 69)

Table 7X. In What Ways Can the Federal Government Support Organizations' Efforts to Improve Preparedness? – Areas of Agreement

Type Of Support Looking Toward Federal Government For	Percent of All Orgs
Provide funds to pay for overtime/backfill costs**	10-20%
Set standards for equipment/training*	15-20%
Exercise coordination and support	10-25%
Provide venues for information sharing*	10-15%
Through R&D on terrorism preparedness and response	10-15%
Provide guidance on benchmarks for measuring preparedness**	5-15%
Perform technical evaluations*	5-10%
Evaluate new technologies and equipment*	5-10%

*Local and State public health not given response option. **Hospitals and local and State public health not given response option. (Question 69)

Table 7Y. Organizations Differ in Views Regarding Appropriate Role of Federal Military and National Guard During Response to a Terrorism-related Incident?

	Federal Military's Role		National Guard's Role		
	Maintain Order/ Provide Security (Percent)	Help with Enforcement of Quarantine (Percent)	Maintain Order/ Provide Security (Percent)	Help with Enforcement of Quarantine (Percent)	Set-up Kitchens, Clinics, and Mass Care Facilities (Percent)
Local Organizations					
Law Enforcement	71 (5)	58 (6)	89 (3)	61 (6)	70 (5)
Local/Regional EMS	76 (5)	56 (5)	89 (3)	64 (5)	51 (5)
Local OEM	74 (5)	55 (6)	86 (4)	67 (6)	73 (5)
Paid/Combo Fire	81 (4)	53 (7)	89 (4)	60 (6)	63 (6)
Vol Fire	75 (7)	31 (7)	77 (7)	30 (7)	74 (7)
State Organizations					
State EMS	63 (5)	37 (5)	87 (4)	67 (5)	40 (6)
State OEM	27 (6)	42 (7)	77 (6)	65 (7)	58 (7)
Health Organizations					
Hospital	--	82 (4)	--	86 (4)	45 (7)
Local Public Health	--	--	95 (2)	52 (10)	51 (9)
State Public Health	--	--	100	53 (5)	53 (5)

Standard error of the estimate is shown in parentheses. (Questions 89 and 90)

TAB 8—SURVEY COMMENTS

In the third wave of the survey, we provided room for written comments asking respondents to comment on: (1) their suggestions for improving Federal and State programs for terrorism preparedness; and (2) their organization's experiences or challenges in preparing for these types of incidents that may have resulted in lessons learned not addressed in the survey. Hospitals were also asked for suggestions for changes or improvements in national/professional organizations for terrorism preparedness. The comments received in these areas are presented below, organized by each organizational type. We have listed here each of the written comments received without any editing other than to fix grammatical errors or to mask the identify of the respondent. For example, if a comment gave the name of a respondent's city we edited the comment to replace the actual name of the city with a generic reference (e.g., "our city"). The written comments below are listed in their entirety and do not represent the views of the Advisory Panel or of RAND, but instead the views of the individual organizations that responded to the survey.

Law Enforcement

Federal Programs for Terrorism Preparedness:
It appears to be a common perception that the Federal government approach is uncoordinated. There is replication of effort in certain areas, and no effort in others. There is no Federal coordination with local governments below the county level.
State Programs for Terrorism Preparedness:
Coordination of training (standards) in the area of WMD and terrorism response. There are so many courses out there – different directions. Not everyone is on the same page.
Organization's Experiences or Lessons Learned:
You must prepare locally to handle situations with your own resources.

Federal Programs for Terrorism Preparedness:
We are totally unaware of what Federal programs are available.
State Programs for Terrorism Preparedness:
We are totally unaware of what state programs are available.
Organization's Experiences or Lessons Learned:
We have learned that unless you have access to the web and someone dedicated solely to surfing the web information is extremely difficult to obtain.

Federal Programs for Terrorism Preparedness:
Quit changing color threat levels. (Terrorists are watching TV also)! More money for us to hire more police officers. Quit spending money in overseas policy. Start concentrating on USA more.
State Programs for Terrorism Preparedness:
More money to small depts. like ours to hire more police, [purchase] equipment and be ready when it hits.

Federal Programs for Terrorism Preparedness:
Funding and informing of training would be a good start.
State Programs for Terrorism Preparedness:
Funding and informing of training would be a good start.

Federal Programs for Terrorism Preparedness:
Faster direct funding!

Federal Programs for Terrorism Preparedness:
The FBI, Secret Service, INS, etc., all Federal agencies that we have worked with in the past have been very good!

Federal Programs for Terrorism Preparedness
Better controls on distribution of funds and equipment by county emergency management agencies

---

Federal Programs for Terrorism Preparedness:
Federal programs need to include localities in training-funding-planning to prepare for a terror attack.

State Programs for Terrorism Preparedness:
Same as Federal – increase towns-villages, counties etc., in a training program.
Organization's Experiences or Lessons Learned:
This survey drives home the need for us to have an ongoing terrorism program in-place with the proper training available.

Federal Programs for Terrorism Preparedness:
1. [Federal] Programs should better integrate local needs and capabilities.
2. Need better coordination among Federal entities themselves.
State Programs for Terrorism Preparedness:
[State] Programs should better integrate local needs and capabilities.
Organization's Experiences or Lessons Learned:
A great benefit has resulted from lateral information sharing among law, fire & health agencies (i.e. agency-to-agency) in the areas of threat/intelligence and operational concepts. Not all "experience" resides at the Federal level. This is not just a top-down issue, bottom-up and lateral efforts are also needed and proving valuable.

Organization's Experiences or Lessons Learned:
We attempt to update officers and training.

Federal Programs for Terrorism Preparedness:
Interoperable radios needed

Federal Programs for Terrorism Preparedness:
We need money for training and equipment
We need regional meetings

State Programs for Terrorism Preparedness:
Set clear requirements the state must follow to fund equipment needs of local jurisdictions based on a threat/risk analysis, NOT equitable distribution, or to agencies with low priority needs. OR bypass state in distribution process.

Federal Programs for Terrorism Preparedness:
There needs to be much faster ability to field test suspected biological agents.
Organization's Experiences or Lessons Learned:
During the period of time of the anthrax cases and hoax cases, the number of calls to these types of incidents and the nature of them were extremely taxing on agency resources. I don't feel that it is well known that the Emergency Response Community and State Dept. of Health labs were very much over-burdened at that time.

Federal Programs for Terrorism Preparedness:
Consistency could be provided if supplemental funding was available to support administrative personnel to manage emergency management programs. Currently, most small rural areas only attempt to qualify for grants, for equipment and training, when available through State level government aid.

State Programs for Terrorism Preparedness:
The agency or agencies tasked with grant application should contact response agencies to assess their needs before purchases are made.
Their Organization's Experiences or Lessons Learned:
Better observation techniques have resulted in suspicious event calls increasing. Officers take situations more seriously when unknown substances are reported, etc.

Federal Programs for Terrorism Preparedness:
Don't allow the FBI to classify information or stop them from putting their own classification on info[rmation]. They hamper the sharing of info[rmation] to those who need to know.
Organization's Experiences or Lessons Learned:
Some local, State and Federal laws put in place for HazMat hamper training and response. Hybrid laws or changes need to be done to place terrorism in its own class.

State Programs for Terrorism Preparedness:
Training. We have yet to be offered any training. We have been given PPE, but no training.

Federal Programs for Terrorism Preparedness:
Training offered is not clearly publicized. It needs to be clear, what the training is, and what the bottom dollar line will be in regards to who funds the training.
State Programs for Terrorism Preparedness:
Better channels of communication between the State program coordinators and local governmental organizations.
Organization's Experiences or Lessons Learned:
We had problems getting information from our local Emergency Services Coordinator.

Comment About State Programs for Terrorism Preparedness:
Municipalities should apply for assistance directly – not through counties.
Organization's Experiences or Lessons Learned:
We will be on our own for some time. You cannot rely on County level emergency managers as they aggressively protect County assets without regard to local community needs.

Federal Programs for Terrorism Preparedness:
Better lines of communication would enhance awareness of programs, training and funding available to state/local agencies.
State Programs for Terrorism Preparedness:
Require states to publish plans and require specific time frames for grants to be applied for (State has published & closed time frame in as little as 5 days.)
Organization's Experiences or Lessons Learned:
We created a citywide multi-disciplinary team to plan and prepare grant applications for Homeland Security funds.

Organization's Experiences or Lessons Learned:
We have had a fair amount of experience for a small city with pipe bombings of vehicles and planned our state Militia Assault. We had good interagency experience and several good experiences with ATF and FBI. We had a flood of "[white] powder in envelope" calls after the anthrax disaster (all fake) or nothing. Very little help in dealing with them.

Organization's Experiences or Lessons Learned:
Yes, local government officials, which are unwilling to support local enforcement efforts, and don't believe that "bad things can happen" are the biggest obstacle. Local politics, not Federal, determine how well each is prepared. Only Federal mandates which address funding, training, equipment, and manpower needs at the local level will resolve this issue. Local politics only care about what is popular not that which is needed.

Fire Departments

Federal Programs for Terrorism Preparedness:
Basic guidance; self-evaluation checklists.

State Programs for Terrorism Preparedness:
Training should be coordinated within state guidelines.

Federal Programs for Terrorism Preparedness:
Need more EMS Programs
State Programs for Terrorism Preparedness:
Same as above

Federal Programs for Terrorism Preparedness:
We were not aware of many of the Federally sponsored programs listed in this questionnaire/survey. Available programs information needs to be sent directly to local agencies along with the state and county.
State Programs for Terrorism Preparedness:
Make sure programs are passed down to all local agencies.

Federal Programs for Terrorism Preparedness:
Aid for additional personnel – our mission has increased and our training and equipment has increased, but our number of personnel has stayed the same.

Federal Programs for Terrorism Preparedness:
Fund cross training with the U.S. Coast Guard. We are an ocean community and deal with the U.S.C.G. more than any other Federal agency.
State Programs for Terrorism Preparedness:
Improved information on training programs and response aids.
Organization's Experiences or Lessons Learned:
We have spent a lot of time and resources to secure funding for countywide public safety communications improvements, County Fire Hazmat JPA equipment upgrades, and county-wide bomb squad equipment upgrades. Very little of the money available has filtered down to our small community needs. It has been focused on countywide response gaps.

Federal Programs for Terrorism Preparedness:
Time frame of grants. By the time we get through lower levels of Gov't, we have 2 or 3 months to finalize Grants. We need more time.
State Programs for Terrorism Preparedness:
The WMD Task Force has no street level Fire or EMS providers on it. Appear out of touch with our needs.

Federal Programs for Terrorism Preparedness:
Federal programs must get to the State.
State Programs for Terrorism Preparedness:
State programs must get to the local level.
Organization's Experiences or Lessons Learned:
Other lessons learned: Ability to work with other local (Police), County Depts, State Agencies and Feds.

Federal Programs for Terrorism Preparedness:
Regional teams funded & trained in specific response situations and available to local jurisdictions.
State Programs for Terrorism Preparedness:
Same as above.

Federal Programs for Terrorism Preparedness:
More funding for state and local planning, training, and equipment. A lot of promises, but little follow through.
State Programs for Terrorism Preparedness:
State programs are very good – Funding is coming to local responders based on needs priority. Very pleased with state response to our needs.
Organization's Experiences or Lessons Learned:
Just that promises are just that—promises. The Federal Government has promised first responders they would be taken care of informationally, financially, and in equipment. This has not happened at this point. The Federal Gov't. has reneged on its promises to State & Local Govts to assist us to upgrade training, equipment and information.

State Programs for Terrorism Preparedness:
The State and other Police have received a disproportionate share of equipment resulting in local Fire Depts., who will be primarily first in, closest and provide the most aid to the citizens, being shorted.

Federal Programs for Terrorism Preparedness:
Need more info passed onto locals.
State Programs for Terrorism Preparedness:
Same as above

Federal Programs for Terrorism Preparedness:
Fed[eral] programs should serve to coordinate state and local efforts. There are too many different organizations duplicating each other's efforts. Too many surveys. Too many meetings. Too much planning and too little action. These activities interfere with normal operations with small results.
State Programs for Terrorism Preparedness:
Same as above. Interagency communications frequencies and equipment should be mandated by law. ICS training should be required for selected officials and failure to observe an incident commander's instruction during an emergency response should be a punishable offense.

Organization's Experiences or Lessons Learned:
Decisions by heads of the largest public safety agencies in a local area can have negative effects on surrounding area agencies, i.e., communications system changes.

Federal Programs for Terrorism Preparedness:
The state is not the best agency to provide/pass funding to the local agencies. They decide where to use the dollars.
State Programs for Terrorism Preparedness:
See above. The areas where terrorist attacks are not treated with a higher level of support. The most rural and least likely areas of the state receive the same funding. The State receives the money and does not seek local input. If they do, it is lip service only.
Organization's Experiences or Lessons Learned:
Yes, the amount and length of surveys has increased.

Federal Programs for Terrorism Preparedness:
Have Federal programs offered at more regional locations.
State Programs for Terrorism Preparedness:
Have state programs offered at more regional locations.
Organization's Experiences or Lessons Learned:
Information from State/Federal level was very slow in coming on specific details of a infrastructure threat (critical). Took two to three days to get specific info.

Federal Programs for Terrorism Preparedness:
Our department is not financially able to maintain equipment and vehicles used to provide fire protection as well as we should. Funding for domestic terrorism is non-existent from any local funds.

Federal Programs for Terrorism Preparedness:
Feds give the money to the State which keeps 25 percent and gives the rest to the Counties, which disperse it according to political preference. Terrorist attacks are much more likely to happen in major metropolitan areas and that is where the funding should be concentrated. The U.S. Fire Administration lists 23 Fire Depts. in our State that got funding – every one of them is a volunteer fire dept. that will never have a connection with terrorism.

Federal Programs for Terrorism Preparedness:
We know the focus is on more populated areas, i.e., big cities, but if people leave the cities where are they going? – Small Town, USA. We do need to be better prepared to handle these folks and the problems they will bring that will overtax our system.

Federal Programs for Terrorism Preparedness:
Yes, many of the grants associated with domestic terrorism are not available to volunteer agencies. All agencies should have a basic level of protection and/or detection.

Federal Programs for Terrorism Preparedness:
I believe that terrorism preparedness needs to be a part of your organizations, all hazards planning and preparedness. The Federal government can best help by improving inter-agency communication at emergency scenes.

Federal Programs for Terrorism Preparedness:
Our Department is, as many departments, small with very little funding. I feel more funding and training should be developed to help Small Town USA. Mainly, volunteer departments.

Federal Programs for Terrorism Preparedness:
Federal programs should go farther than providing funds without any definitive criteria for fund/equipment distribution to the local jurisdictions. The local fire depts. and police depts. are the first responders who will suffer the initial consequences for the political games played at the Federal and state levels. The consequences include those responders' lives. Providing money at the Federal level does not make the country safe.
State Programs for Terrorism Preparedness:
See above. If possible, the political entanglements and mismanagement at the state level are even worse.
Organization's Experiences or Lessons Learned:
As noted, the political considerations – hurdles, corruption, mismanagement, etc.—are the biggest challenge. For someone who has spent lives protecting the citizenry of a jurisdiction, the political games which delay or stop the

distribution of the money, equipment, and training needed at the local level is at least incompetent and at most criminal.

Federal Programs for Terrorism Preparedness:
Provide funding for more local/regional training and support.
State Programs for Terrorism Preparedness:
Keep the State programs as support for training, but pass the financial support to the local jurisdictions rather than to the states—then down. The trickle down isn't happening. The finances never get out of the capital.
Organization's Experiences or Lessons Learned:
We respond to emergencies every day. We are trained for that. The Federal Gov. is trying to re-invent the wheel by creating this different dept. to handle terrorism. Equip the first responders better & you will meet the need rather than take funding away from us.

Federal Programs for Terrorism Preparedness:
Not at this time. Basic plans need funding to the local levels of Gov't.

Federal Programs for Terrorism Preparedness:
Funds seem to go to politically connected jurisdictions and communities. Police seem to get more funding than Fire Depts. Too much money is wasted on salaries and evaluations instead of needed equipment. The public is very misinformed of how much money actually gets to local responders.
State Programs for Terrorism Preparedness:
Same as above.
Organization's Experiences or Lessons Learned:
Public opinion of how much money local fire depts.get for WMD preparedness.

Federal Programs for Terrorism Preparedness:
Leave Fire Grant alone. Work on making things more regionally doable for New Englanders (who are reluctant to change).
State Programs for Terrorism Preparedness:
Bring it to the locals, don't try to have locals come to you.
Organization's Experiences or Lessons Learned:
No money for any programs and as stated earlier – reluctant to change.

Federal Programs for Terrorism Preparedness:
Information needs to be shared.
State Programs for Terrorism Preparedness:
Information and equipment need to be shared equally.
Organization's Experiences or Lessons Learned:
Preparing for domestic terrorism strengthen accidental emergencies and disaster.

Federal Programs for Terrorism Preparedness:
Making sure that the Federal money passed on to state govt's gets to the local responders.
State Programs for Terrorism Preparedness:
Making sure that they do not hold the Federal money and pass it on to the local responders
Federal Programs for Terrorism Preparedness:
Structural needs from personnel, to training, to building and grounds and equipment. Stop building more parks. Our local park district has more money, more grants, better equipment, better buildings than both fire and police combined. Turn over Fire & Police protection to the Park Districts; they have more money.

Federal Programs for Terrorism Preparedness:
Funds, equipment and training must go to local First Responders, not to agency that respond after the fact. Local fire, police and EMS are the front line vs. Hazard terrorist acts.
State Programs for Terrorism Preparedness:
Same as above.

Federal Programs for Terrorism Preparedness:
Please institute a Federal sponsorship program that assist with a degree program in counter-terrorism operations. Also consolidate FEMA, NFA, EMI, ODP, and OJP training for Unified command training. Provide bi-annual technology symposiums for organization preparing or improving WMD operations.
State Programs for Terrorism Preparedness:
Exercise the states' emergency operation centers with the joint terrorism task forces.
Organization's Experiences or Lessons Learned:
Yes, our political leaders do not understand the standards for WMD response. The community needs CBRNE information to begin preparation efforts related to the high target areas near residence. Fire organizations require "combat" approach to offensive counter-measures.

Federal Programs for Terrorism Preparedness:
The Federal government should provide emergency response equipment to financially strapped local fire departments to better provide terrorism preparedness as well as better communications to regions known to have a serious terrorism threat. Too much terrorism information is being concealed by the Federal government. Not enough terrorist information getting to local levels.
State Programs for Terrorism Preparedness:
Same as above.

Federal Programs for Terrorism Preparedness:
More guidance.
State Programs for Terrorism Preparedness:
More guidance. An awareness of what could happen.

Federal Programs for Terrorism Preparedness:
Funding is our largest problem; it causes an inability to receive proper training and to equip our department with proper gear and equipment.

Federal Programs for Terrorism Preparedness:
Continue DHS coordination, use existing personnel of L-S-F level, limit funding to consultants (especially those with limited or military only).
State Programs for Terrorism Preparedness:
Consider our large metropolitan area as a state – passing [Federal support] through the state government just adds another layer.

Federal Programs for Terrorism Preparedness:
Not at this time.
State Programs for Terrorism Preparedness:
Get money to the local jurisdiction sooner.

Federal Programs for Terrorism Preparedness:
Provide training courses either locally, or regional that combines law enforcement, fire/EMS and public works response.

Federal Programs for Terrorism Preparedness:
More money.
State Programs for Terrorism Preparedness:
More money.
Organization's Experiences or Lessons Learned:
Less money.

Federal Programs for Terrorism Preparedness:
We need to see a quicker pass through of funding from Fed's to state to local jurisdiction! Organized regional response teams, will be needed.

Federal Programs for Terrorism Preparedness:
As stated, there is a multitude of programs, organizations, guidelines mandates, etc., so much so that confusion is becoming a problem, especially who does what, who can, etc. Also large scale chem/bio will probably affect metro

areas – conventional still most probable- no need for a rural/suburb with unlikely targeting to have same preparedness/resources mandate.
Organization's Experiences or Lessons Learned:
Yes – standardize equipment and resources – in the event of a large scale terrorism event you should know outside responding agencies are all on the same page and similarly equipped and trained, ready to assume duties and positions that are already in motion.

Federal Programs for Terrorism Preparedness:
They should assess if small cities are at risk. If so, then fund and train at that risk. If not, then regionalize response teams from large cities if needed.
State Programs for Terrorism Preparedness:
State government should focus on what happens after an incident. Or stabilizing local needs after the emergency.
Organization's Experiences or Lessons Learned:
Information flows through too many agencies. Some through fire, EMS, law enforcement, emergency management. Need one collecting agency per county/city.

Federal Programs for Terrorism Preparedness:
Yes, set up a policy agency for inept chief who doesn't know how or want to evolve.

State Programs for Terrorism Preparedness:
The state should pay for the equipment that is ordered on the WMD grant form instead of having the county or city purchase it and them reimburse them after they turn in the receipts.

Federal Programs for Terrorism Preparedness:
Do more to combine local resources. In many cases there is a duplication of resources from municipality to municipality. People will apply for grants for equipment a neighboring town already has. We need to work together. We end up with more equipment than we need and not enough trained personnel. Bring training to local levels, especially existing police departments. Stop creating more agencies.
State Programs for Terrorism Preparedness:
Same as above.

Federal Programs for Terrorism Preparedness:
Do not funnel money for response programs, training etc. through the state systems.
State Programs for Terrorism Preparedness:
Develop funding systems that improve the flow of resources.

Federal Programs for Terrorism Preparedness:
Need better study on local needs. Insurance that money goes to the local level – not state, not county.
State Programs for Terrorism Preparedness:
Same as above.

Federal Programs for Terrorism Preparedness:
Make it easier to attain funding for training, equipment exercises and overtime (back-fill positions).
State Programs for Terrorism Preparedness:
The same as for fed's.
Organization's Experiences or Lessons Learned:
After 9/11, our city created an internal Task Force to review any deficiencies in our EMP-Plans. We found 321 deficiencies and have addressed all of them in a work plan I developed myself. All of our EMP plans have been updated, a brochure was developed (recently doing a reprint with new info) to be mailed to all of our community, and have developed many relationships with other communities, county, civic groups and private sector. If you would like a copy, please call me.

Federal Programs for Terrorism Preparedness:
This response concerns both questions #103 and #104. We have a concern about grant equipment that we have received from the State that was purchased with Federal dollars, not being what we needed. Instead it ended up being equipment that a committee at the State level decided we should have. As it result, it is my estimate that half of the funds expended was for equipment we don't have a use for or is not compatible with equipment we currently have.

State Programs for Terrorism Preparedness:
(See above)
Organization's Experiences or Lessons Learned:
Yes – our organization has participated in three major drills, in three metropolitan cities and TOPOFF. We have learned that there is a major confusion in the fire service in differentiating between standard HAZMAT incidents and WMD incidents. Please feel free to contact me about these "lessons learned."

Federal Programs for Terrorism Preparedness:
The monies should go to small cities and towns, not just the larger cities and towns.

Federal Programs for Terrorism Preparedness:
More coordination from the Feds through the state to the county and local levels.

Federal Programs for Terrorism Preparedness:
Yes, the big towns get the grants and for some reason we don't! Grants should be on <u>needs</u> and not on how good someone talks on paper.

Federal Programs for Terrorism Preparedness:
Information sharing is a definite problem. There is a lack of information dissemination by law enforcement agencies to fire departments. Everything is a big secret. Where fire departments are the first-responders in most incidents, it would be helpful to know that there is a threat before and not after the incident.
State Programs for Terrorism Preparedness:
Quicker dissemination of funding to the smaller, local agencies. The smaller agencies are going to be the primary recipients of the exodus of the larger impacted cities. Placing all the funding, or the majority of the funding in the cities that may be destroyed seems sort of unrealistic.

Federal Programs for Terrorism Preparedness:
As with most programs the most important factor is funding. With most fire departments facing budget cuts and reduction in manpower, it is of the utmost importance that funding for programs of those related to terrorist attacks or weapons of mass destruction be forthcoming. The fire departments in this country have been neglected for too long. In order for them to continue to respond in a safe and effective manner to an incident they need to receive funding at the federal level. This fund should go directly to the fire department and not through federal or state agencies.

Federal Programs for Terrorism Preparedness:
Establish a tiered response plan with local, regional, state and national levels of reinforced response and support. The concept of quick action by local agencies reinforced by adjacent agencies/counties within region, then a more sustained response by state/federal agencies.
State Programs for Terrorism Preparedness:
Establish regional multi-jurisdictional response teams for: hazmat, explosive detection/disposal, USAR-resive, mass casualty/care, biological-health department. Fund: equipment, training and personnel costs for these.
Organization's Experiences or Lessons Learned:
The Federal effort to assist local government with this issue has resulted in a poorly coordinated money grab. The process is not results oriented and will not ensure a meaningful improvement in local, regional and state response capability unless corrected.

Federal Programs for Terrorism Preparedness:
More funding for volunteer agencies.

Federal Programs for Terrorism Preparedness:
Yes. Enable/allow Federal contractors to apply and get grants and training. We are a career fire department surrounded by volunteer departments. We have highly trained but few personnel and extremely limited funding because we are a science site. The "vollies" have money, are eligible for grants, and have people (albeit not as well-trained). We could function as a resource to the mutual aid agencies around us if we had more people and/or money.
State Programs for Terrorism Preparedness:
See above. Same reasons.

State Programs for Terrorism Preparedness:
Have a state curriculum. There are too many courses coming from all different kinds of agencies. Should be streamlined like this: WMD awareness, operational, chief officer/command, logistics, HazMat Specialist.
Organization's Experiences or Lessons Learned:
That in some cases things/items have not been made or on the market.

State Programs for Terrorism Preparedness:
State should focus less on hurricanes and more on other items.
Organization's Experiences or Lessons Learned:
Yes, this survey is far too long and time consuming.

Federal Programs for Terrorism Preparedness:
More information needs to be available about how the old FEMA will be wrapped into the Department of Homeland Security. Local governments are waiting to know specifics of how the DHS will be operating.
State Programs for Terrorism Preparedness:
Our State also needs to clarify the merging roles of the Office of Emergency Services and our own Department of Homeland Security.

Federal Programs for Terrorism Preparedness:
We would like to see the FEMA Guidelines simplified but keep the funds coming from FEMA.

Federal Programs for Terrorism Preparedness:
We need funding for equipment.

Federal Programs for Terrorism Preparedness:
Having lived here for 30 years with the dam out my kitchen window, I am concerned with what would happen down stream if the dam broke. Flooding many cities and towns. Our Judge feared people in his county would be in danger. I agree.
State Programs for Terrorism Preparedness:
No one has contacted us about anything. If contacted we would do what ever we could. There is no one else out here to respond.

Federal Programs for Terrorism Preparedness:
Federal money channeled through local FEMA/EMA is not distributed properly. It becomes a popularity contest. Buying equipment for agencies other than first responders, police & fire.

Organization's Experiences or Lessons Learned:
We have started to work closely with the area Fire Departments. Including combined training and sharing of equipment and resources.

Federal Programs for Terrorism Preparedness:
The funding/training needs to be delivered directly to the local agencies. Too much funding is being caught up and diverted at state and local level.
State Programs for Terrorism Preparedness:
Same as above.
Organization's Experiences or Lessons Learned:
Yes, don't rock the boat when it comes to identifying deficiencies in operation or funding. If you do, your organization will be left out altogether.

Federal Programs for Terrorism Preparedness:
Whatever the Federal government mandates in the future, they will need to provide funding that reaches the local governments so they may implement what is needed locally.
State Programs for Terrorism Preparedness:
Again, if some program is mandated to the fire service the state government must make funding available to local government to implement the programs.
Organization's Experiences or Lessons Learned:
Yes other mutual aid and regional emergency response agencies depend upon my organization to fill gaps in preparedness/response capabilities.

Organization's Experiences or Lessons Learned:
Focus on IMS, awareness, and emergency management planning for all agencies. We must get everyone to a basic level before we waste money on anything advanced.

Organization's Experiences or Lessons Learned:
It would be nice if all the agencies who attend the WMD courses had a yearly schedule with the allotted slots per jurisdiction. This would help in the planning and selection of perspective participants; it would also quantify different agencies allotments.

State Programs for Terrorism Preparedness:
Funding and support for local departments are needed.

Local Offices of Emergency Management

Federal Programs for Terrorism Preparedness:
It is important to focus upon and provide direct support to county or regional consortia efforts. Counties and regional efforts are being short-circuited by the state and funds (controlled by the state) are being allocated without the counties/regions being involved in the decision making process.
State Programs for Terrorism Preparedness:
The state must involve the counties in strategic decision-making. How can they hope to achieve standardization of training and equipment for a combined mutual aid response if they do not involve the counties?
Organization's Experiences or Lessons Learned:
The 80%/20% fund allocations are much too high for the states to take (20%). The money needs to get to the real First Responders at the city, village, and township levels. That is where the rubber meets the road…not at the state capitol or state police agency.

Federal Programs for Terrorism Preparedness:
All of this terrorism stuff has really placed a burden on our operation. Our operation of 911/emergency mgmt was difficult to maintain even before the 9/11 terrorism. With the additional work, we can no longer excel or focus on any of our duties. We need more personnel to allow us to do the proper job!
State Programs for Terrorism Preparedness:
Better coordination and consolidation of programs.

Federal Programs for Terrorism Preparedness:
Fully fund WMD training, exercises, and equipment (including maintenance and calibration).

Federal Programs for Terrorism Preparedness:
No. I addressed the questions from the viewpoint of the Local Emergency Planning Committee which is also the emergency responders in our jurisdiction.
Organization's Experiences or Lessons Learned:
Small jurisdictions do not have the time to address the Risk and Treat assessment and grant writing. To hire someone to do the R&T assessment is impossible. You need background on what is in your jurisdiction; also, there wasn't enough time to do all the work.

Federal Programs for Terrorism Preparedness:
Current programs are not flexible enough to allow funds to be spent on specific local needs.

Federal Programs for Terrorism Preparedness:
A written developed plan on possible or feasible funding. By accomplishing this, the trickle down effect of local agencies would be enhanced.
State Programs for Terrorism Preparedness:
Have satellite offices spread elsewhere in the state to assist in completed federal/state mandated requirements (assessment–mitigation–grants).
Organization's Experiences or Lessons Learned:
Receipt of equipment that exceeds needs. No consideration of other agency participation in other federal programs such as MMRS or NLD.

Organization's Experiences or Lessons Learned:
One of the biggest hurdles we face is changing the laws and old ways we have done response and recovery, and, probably more so, planning and preparedness. Laws and procedures happen to block mentally and physically the transition to regionalization to planning and response. In our state, statutes mandate each jurisdiction plan and manage its own disasters essentially. Plans are written to support this philosophy. Incidents of a regional nature in our planning region should require commissioners and mayor from each jurisdiction to be in a regional EOC (if you use the regional approach). Each of our 18 counties has 3 commissioners. That means 51 commissioners would need to be involved, not counting mayors. Who would be in charge? Hopefully if regional planning and response and recovery are the goal, we'll find a way of getting there.

Federal Programs for Terrorism Preparedness:
We need and appreciate the support, but all funding comes with restrictions and limitations imposed by the state or the grant itself. It doesn't help when the equipment we have is listed as eligible and the equipment we need to add is not listed as eligible. Let the locals decide what is needed for situation.

Federal Programs for Terrorism Preparedness:
I would like to see the money that was supposed to go to First Responders get to the local level and not be given to the larger cities at the whim of a local director, who doesn't understand how the volunteer system works or how to treat volunteers. Most First Responders in this nation are volunteers and they deserve the funds.
State Programs for Terrorism Preparedness:
Provide enough funding and training for First Responders.

Federal Programs for Terrorism Preparedness:
Funds need to go directly to locals.
State Programs for Terrorism Preparedness:
States waste a lot of funding dollars.

Federal Programs for Terrorism Preparedness:
Cut the strings and bureaucracy with the grants! The Feds seem to be creating red tape so power is confirmed. They need to relinquish power.

Federal Programs for Terrorism Preparedness:
More funding to local level.
State Programs for Terrorism Preparedness:
Send the equipment procured from Homeland Security grants to local agencies quicker.

Federal Programs for Terrorism Preparedness:
Set national standards for local response capabilities. Give local govt's a choice of what response level they wish to achieve. Distribute funding to those jurisdictions that are in the most need.

Federal Programs for Terrorism Preparedness:
Monies sent down from the Federal side take approximately a year to reach the First Responders in our State. We at the local level are still waiting for the 2002 ODP dollars.

Federal Programs for Terrorism Preparedness:
Most local emergency management programs have one paid part or full time staff. We need staff support funding for local offices.

Federal Programs for Terrorism Preparedness:
If items are on an approved list to buy with current monies, why must they be re-approved before they can be purchased?

Federal Programs for Terrorism Preparedness:
The programs need to be geared toward the rural areas of the county. This is the area that relies on Volunteers for most responses as the local funding does not have the capability to fund full time EM - FDs – PDs and other emergency responders. Yes, NYC was a target, but what about the local Wal-Marts, etc., in small town America?

Federal Programs for Terrorism Preparedness:
Include the impact of crisis relocation/fleeing on host areas.
State Programs for Terrorism Preparedness:
Currently, the state has two separate terrorism preparedness offices which are not coordinating together or duplicating services and/or programs already existing in other law enforcement agencies.
Organization's Experiences or Lessons Learned:
The State Health and CDC must learn to work with the State and Local EMA and not reinvent the wheel.

Federal Programs for Terrorism Preparedness:
Be able to hire more people. Long-range plan as to what is going to be available in future.
State Programs for Terrorism Preparedness:
Cut down on the state cut of money.

Federal Programs for Terrorism Preparedness:
Decrease paperwork requirements. Send more money for staff to assist in the assessments.

Federal Programs for Terrorism Preparedness:
Get organized by getting the politicians out of the planning process except to appropriate funds.
State Programs for Terrorism Preparedness:
Small urban areas would benefit from state or regional programs such as a state telephone system that would allow county response groups to call the entire group with one call (on a pager system) – small urban areas can't afford such systems.
Organization's Experiences or Lessons Learned:
Yes, we're still more likely to have a severe weather event and need our systems to handle that also.

Federal Programs for Terrorism Preparedness:
More focus should be placed on small, frequent functional drills and tabletops than on large full-scale exercises.
State Programs for Terrorism Preparedness:
Give locals more latitude on what to implement and how to implement.
Organization's Experiences or Lessons Learned:
Politics and turf battles continue to impede progress. Incentives are needed to get some agencies to work together. In some cases, a city or dept. won't actively cooperate with a county because they know they can get funding through other mediums.

Federal Programs for Terrorism Preparedness:
The Federal money is starting to reach the small governments. This needs to be done sooner. Application process is too cumbersome and short turn around time from receiving application to return same. We have a very limited staff with normal day-to-day duties and other emergency issues. Give us more time!
State Programs for Terrorism Preparedness:
Same comments made above apply here also. We cannot do things overnight.
Organization's Experiences or Lessons Learned:
Local political people do not take the terrorism threat serious. The Federal/State need to reach out to them through State and Federal political people to address this issue.

Federal Programs for Terrorism Preparedness:
Programs need to get to us. Programs need more time to be responded to.

Federal Programs for Terrorism Preparedness:
Money for salary and equipment is needed.
State Programs for Terrorism Preparedness:
Funding needs to go to agencies, not to the state, then agencies - or at least not have the state take 20% off the top!

Federal Programs for Terrorism Preparedness:
1. Broaden the focus to all hazards planning—too much terrorism-specific effort that dilutes overall preparedness.
2. Improved coordination at Federal level—too many disparate programs from too many agencies
3. Improved operational focus on response and recovery—too many "one-shot" programs, especially in equipment, that don't build a comprehensive system.

State Programs for Terrorism Preparedness:
See above comment.
Organization's Experiences or Lessons Learned:
Need for operational plans
Need for broad perspective (see comment #3 above)

State Offices of Emergency Management

Federal Programs for Terrorism Preparedness:
1) Funding kept at zero match. 2) Freedom to use money as needed. 3) All Homeland Security money through one state Homeland Security Entity. 4) Notification of any related funds.

Federal Programs for Terrorism Preparedness:
No suggestions beyond answers previously discussed and answered in this survey.
State Programs for Terrorism Preparedness:
FEMA must make application packages easier.
Organization's Experiences or Lessons Learned:
A continued emphasis on the use of technology to overcome communication and other command system problems.

Federal Programs for Terrorism Preparedness:
Need to have funds for personnel to use training and equipment provided by current grants.
State Programs for Terrorism Preparedness:
Yes – more focus on all-hazards response.
Organization's Experiences or Lessons Learned:
Yes – the percentage of "other" hazards occurring far exceed the changes of domestic terrorism incidents. In rural America, the responders are few in number and will respond to all incidents, including terrorism. All efforts to be prepared should be focused on all-hazards.

Federal Programs for Terrorism Preparedness:
DHS/ODP reporting requirements/administrative approval of proposed equipment purchases needs to be streamlined.
Organization's Experiences or Lessons Learned:
Implementing on scene incident command/unified command during WMD exercises.

Federal Programs for Terrorism Preparedness:
This survey did not rate the performance of the current National Homeland Security effort of our agency.

Federal Programs for Terrorism Preparedness:
Merely a matrix of all Federal grants would be helpful. Especially if it was updated as grants are awarded, similar to Federal Fire Administration fire grants. We at the state level don't know all these grants that come to us. I suspect GAO can find out – but should be readily available to anyone on a website that consolidates all federal grants on one website.
Organization's Experiences or Lessons Learned:
Preparedness for terrorism incidents greatly enhances response capabilities statewide for all emergency response.

Federal Programs for Terrorism Preparedness:
Stop multiple assessments – one assessment – one standard! Stop multiple Exercise Programs (CDC, EPA, FEMA, DHS, DOJ, FBI) – one Homeland Security Exercise program!

Federal Programs for Terrorism Preparedness:
Size include contracted personnel.

LOCAL/REGIONAL EMS

Organization's Experiences or Lessons Learned:
The information given above reflects the EMS region's resources. There are 37 cities & towns with own law enforcement, fire and EMS departments. ESTIMATE!

Federal Programs for Terrorism Preparedness:
Make access easier and more widespread. Improve information sharing with EMS & Fire, seems very much law enforcement only.
State Programs for Terrorism Preparedness:
Same as above.
Organization's Experiences or Lessons Learned:
Public and EMS education is difficult. The "it won't happen here" mindset was overcome through education – specifically – we have a nuclear power plant and major tourist attractions that make good targets.

Federal Programs for Terrorism Preparedness:
Most Federal programs are not available for privately owned EMS organizations. Anything we have asked for has been turned down because we are not a non-profit organization at both the state and Federal levels. We are a large part of our county's MABA's program, but are treated as a "greedy private ambulance" by state and federal programs. We provide back up services and mutual aid to all departments in our county. We provide ambulances to most major fires and fire ground rehab free of charge at our own expense. When we have asked for Federal or state assistance in funding, we have consistently been turned down. We cannot afford to be more prepared for anything else at this time at our own expense.

Federal Programs for Terrorism Preparedness:
Faster access to funding and less cumbersome applications
State Programs for Terrorism Preparedness:
Faster access to funding and less cumbersome applications

Federal Programs for Terrorism Preparedness:
Please just provide some of the things you have asked about. For 3 yrs., we have answered these questions but no improvements, no funding, no training offered. Where are the things we need?
Organization's Experiences or Lessons Learned:
Funding

Federal Programs for Terrorism Preparedness:
Work to get the funding to the areas needed most!

Federal Programs for Terrorism Preparedness:
There is very little to no communication with those in the trenches. There are ICS systems that have been in effect in CT that are being ignored. I have had to go to independent agencies for programs and courses due to the lack of any programs at the federal and state levels. It appears that Homeland Security and DHS talk to who is politically expedient, not to those who are active in the field.
State Programs for Terrorism Preparedness:
The same comments as above. The one sad note is to watch the funding thrown away on projects we will most likely never use.
Organization's Experiences or Lessons Learned:
The only experiences that we have received is training from independent sources and the programs from agencies such as "American Red Cross: who had courses when the Homeland Security and DPN had nothing and still don't for EMS.

Federal Programs for Terrorism Preparedness:
Our organization is no more prepared for this than before Sept. 11, 2001.
State Programs for Terrorism Preparedness:
Same as above.
Organization's Experiences or Lessons Learned:
Same as above.

Federal Programs for Terrorism Preparedness:
Public health issues such as smallpox being addressed.

Federal Programs for Terrorism Preparedness:
Provide clear, understandable funding for training and antidotes to private healthcare organizations (hospital, ambulances, clinics).

State Programs for Terrorism Preparedness:
Send funding through EMS associations as opposed to through Emergency Management Coordinators.

Federal Programs for Terrorism Preparedness:
Many of the Federal training and equipment grant programs are being made available to EMS programs that are fire department-based. In our State, only 35% of the transport EMS service programs are fire based. That leaves 65% of our ambulance services ineligible for funding.

Federal Programs for Terrorism Preparedness:
We need funding help for general operations. We may not be here otherwise. Our vehicles are crap, our local funding sucks. Federal & state bureaucracies are killing us with oppressive rules and mandates.

Federal Programs for Terrorism Preparedness:
The primary focus seems to be on fire based EMS programs which leave out the majority of EMS providers.
State Programs for Terrorism Preparedness:
State Homeland Security Council does not include EMS and has to liaison with the Health Department member. Bioterrorism focus leaves out EMS which should have played the primary role in state terrorism planning and response to events.
Organization's Experiences or Lessons Learned:
Yes. Mostly that public health and others were re-inventing the wheel with plans and contact lists that were already in place and updated regularly.

Federal Programs for Terrorism Preparedness:
The biggest challenge we face is lack of interest of our employees regarding training. I would like to see mandated training with the funding available. By making it a requirement for re-certification would bring every employee up to date. If the Feds can mandate HIPPA training, they should be able to mandate WMD training.
State Programs for Terrorism Preparedness:
Same as above. We are faced with too much politics within the 4 county areas that we serve. I would suggest one lead agency (that being the State) to control protocol, training, and equipment.

Federal Programs for Terrorism Preparedness:
Funding!
State Programs for Terrorism Preparedness:
Funding!
Organization's Experiences or Lessons Learned:
Because we are a private company all grants go to local Fire Depts. only.

Federal Programs for Terrorism Preparedness:
Have a knowledgeable person/advocate that the little guys can call for help.

Federal Programs for Terrorism Preparedness:
Communications should be simple. Grants should be simple.
State Programs for Terrorism Preparedness:
Communications – Reddinet vs Rims. State is trying to impose Rims upon Reddinet system to report to the state. Reddinet is simple and easier to operate. I can go to Bank of America and process my account from any B/A site, but I cannot do that in emergency communication – that is terrible.

Federal Programs for Terrorism Preparedness:
As stated before, Federal programs have been helpful. Our primary problem is our state health division (OHS); while they clearly are making some effort, assistance and coordination and pass through funding has been slow. Some problems (including smallpox programs) they frankly have resisted. Direct funding to locals would be beneficial.
State Programs for Terrorism Preparedness:
Yes 1) There needs to be specific federal requirements on the type of response, stakeholders and organization. 2) Agreements should include evaluation of performance of state coordinators by local agency. State has not communicated well to date with its EMS agencies or hospitals.

Organization's Experiences or Lessons Learned:
Yes. Communications and intra operability was not directly addressed in this survey. Federal guidance of "surge capability" and methods communities can use is scarce. DHS (Homeland Security) organization and coordination is obviously early in its organization. Single stop shopping would help.

Federal Programs for Terrorism Preparedness:
More funding and programs at EMS/Health projects and training – not just fire.
State Programs for Terrorism Preparedness:
Get these programs together. Most are going in own direction. We still are not working together. If there is a need, we will still not be on the same track with each other.
Organization's Experiences or Lessons Learned:
Yes. 1) What we are able to do. 2) A Plan. 3) Local Response Teams

---

Federal Programs for Terrorism Preparedness:
The United States Fire Administration (USFA) National Fire Academy's EMS special operation, two-week course was excellent preparation for multi-agency, all-hazard preparedness and response. Unfortunately, core mission does not even involve EMS and there was an attempt to cancel these courses for budget reasons in the spring of 2003. We also make extensive use of National Wildfire Coordinating Group (NWCG) incident command courses.
State Programs for Terrorism Preparedness:
Our state programs barely recognize that EMS even exists.

State Programs for Terrorism Preparedness:
Duplication must be stopped. City and State levels of emergency preparedness are vying for the same funds and creating the same services.

Federal Programs for Terrorism Preparedness:
Direct funding to EMS
State Programs for Terrorism Preparedness:
Direct funding to EMS

Federal Programs for Terrorism Preparedness:
1) Easier application process. 2) More flexibility in spending/funding to meet local needs and enhance current capabilities.
State Programs for Terrorism Preparedness:
Same as above

Federal Programs for Terrorism Preparedness:
Give regional EMS councils direct resources and responsibilities.
State Programs for Terrorism Preparedness:
We worry that the State is beginning to view EMS as a Homeland Security program first, rather than address the day-to-day issues EMS faces. Regional EMS Councils are not included in any meaningful way by the State DPH and are not funded to increase staff to permit us to do what needs to be done to support our providers and towns. State "Centers of Excellence" do not include EMS Councils in EMS-related planning or activities.
Organization's Experiences or Lessons Learned:
I would need to survey our regional towns and provinces to respond to most of these questions and I simply don't have the staffing or time.

Federal Programs for Terrorism Preparedness:
We do fairly well in treating patients, but not so well in planning. We could use more information on planning and where best to spend our available money. Financial assistance would also be beneficial.
State Programs for Terrorism Preparedness:
Same as previous question.
Organization's Experiences or Lessons Learned:
Most were covered.

Federal Programs for Terrorism Preparedness:
Our EMS organization is a non-governmental organization (private). I believe we have roadblocks that restrict our access to funds for training, equipment, expertise and consulting resources.

Federal Programs for Terrorism Preparedness:
Individual EMS providers servicing the communities do not get first hands-on training due to staff shortage – personnel trained in areas of expertise.
State Programs for Terrorism Preparedness:
Same as above
Organization's Experiences or Lessons Learned:
Local counties are not prepared to handle an incident of great magnitude if needs be. Hospitals are not equipped as well for these types of incidents. Physician shortage – EMS vehicle and personnel shortage state-wide.

Federal Programs for Terrorism Preparedness:
Campus Law Enforcement – Security Issues

Federal Programs for Terrorism Preparedness:
Most important – one source for info/grants.

Federal Programs for Terrorism Preparedness:
They all should be computer based, compatible with email, since most grants require more than one person to fill them out.

Federal Programs for Terrorism Preparedness:
No. I believe that more programs, information, grants, etc., have originated at the federal level for states and local agencies in this past year.
State Programs for Terrorism Preparedness:
While we have done better this past year, states still need to be more aware of the needs of small volunteer departments. Training needs to be closer to "home" for people with jobs and families. Training on new protective equipment needs to follow more closely to the grants allowing local depts to purchase same. Templates for small depts. to use to set up training exercises - What is expected of us?

Federal Programs for Terrorism Preparedness:
Coordinate all efforts, training, funding through a single federal entity!
State Programs for Terrorism Preparedness:
Coordinate all efforts through one state agency

Federal Programs for Terrorism Preparedness:
Yes. Identify Opportunities, Training and Funding.

Federal Programs for Terrorism Preparedness:
See comments below for state programs.

State Programs for Terrorism Preparedness:
Equipment caches; funding for equipment; basic equipment lists for EMS providers
Organization's Experiences or Lessons Learned:
No challenges. Only experience is "WMD" being jammed down our throats, but there are no basic standards to follow – requirements for personnel, basic equipment needed for EMS units, standardized training.

State Programs for Terrorism Preparedness:
More money and assistance for training!
Radio frequency: too long to get one; poor coverage; poor multi-agency communication ability.

State Programs for Terrorism Preparedness:
The state needs to realize that when it comes to purchasing equipment for local governments "one size does not fit all." Local government is very diverse even though they reside in the same county or region. They should have a bit more autonomy in making purchasing decisions.

Federal Programs for Terrorism Preparedness:
The Federal resources for planning and coordinating the system do not pass down to regional and local levels.

Federal Programs for Terrorism Preparedness:
Not sure; we are very small - 30 trips/month service with no county involvement.

STATE EMERGENCY MEDICAL SERVICES

Federal Programs for Terrorism Preparedness:
Currently there are no federal grants focused primarily on EMS agencies but they are sorely needed.
Organization's Experiences or Lessons Learned:
1) Train with your fellow responders – police, fire, EM, management and hospitals. We list our joint training opportunities on a state website and all responders are welcome to attend. 2) Conduct tabletop exercises that involve all of the responders so that they get to know each other personally and to familiarize each other with the resources that each organization can (or can't) bring to mitigate a disaster.

State Programs for Terrorism Preparedness:
EMS is only based in fire departments in 33% of state's RMS agencies – fire based RMS is only in 34% of RMS agencies nationally. Fire does not equal EMS. Without RMS – incident response is flawed – will be unsuccessful.
Organization's Experiences or Lessons Learned:
Lessons learned thus far – nationally RMS is pretty unprepared because the funding stream is not set up to assist local, regional, or national RMS response preparation. State RMS Directors have been surveyed and can give figures of non-funding from almost all sources. Call 703-538-1299 or e-mail NASEMSD@aol.com for more information. If RAND really wants to make a difference – advise Congress and President that the response assistance program is extremely flawed.

Federal Programs for Terrorism Preparedness:
Need centralized coordination. EMS in all states is fragmented (i.e.: fire, hospital-based, private services). It is a part of the nation's health care infrastructure.
State Programs for Terrorism Preparedness:
Continue development of casualty surge capabilities, statewide triage, and patient tracking programs.
Organization's Experiences or Lessons Learned:
From a statewide perspective, many local responders do not feel counter terrorism is a high priority. Challenges exist with a system that is 55% volunteer based.

State Programs for Terrorism Preparedness:
Better communication and coordination.
Organization's Experiences or Lessons Learned:
Need for equipment.

Federal Programs for Terrorism Preparedness:
EMS Programs are not being adequately considered. When the assumption that addressing fire services takes care of EMS is made, MOST EMS is not included. Funding that flows through Emergency Management channels does not go to EMS. Federal grants, advisory boards, planning, etc., do not have EMS leaders involved. Every state has a STATE EMS DIRECTOR. The directors all belong to the National Association and regularly provide liaison and work with any who ask. Please address this problem.
State Programs for Terrorism Preparedness:
State programs MUST include State EMS directors. If they do not, the lead agency makes decisions that do not adequately factor medical, scope of practice, drug use limitations, protocols, etc., into plans, operations, and many other activities.
Organization's Experiences or Lessons Learned:
Yes: 1) CDC must include EMS environments when issuing patient care messages – some cannot be implemented. 2) Protective equipment is a very general term – situation/threat varies and impacts in many ways, e.g., SARS different from anthrax, different from smallpox, different from plague, etc. Complicated and so often NOT addressed. Needs to be.

Federal Programs for Terrorism Preparedness:
Make more specific request to FUND EMS programs in Grant application in the state.

Federal Programs for Terrorism Preparedness:
FEMA does not understand how EMS functions in much of this country. FEMA thinks that the fire service equates to EMS, but this is not there in much, if not most, of the U.S. There needs to be accurate, commonly understood definition of EMS system.
Organization's Experiences or Lessons Learned:
Our challenges arise from working in a state public health system that does not understand EMS.

Federal Programs for Terrorism Preparedness:
1) There are no Federal financial support programs for EMS. This part of the continuum of response, therefore, is not evolving at the same rate as other partners, even though EMS if the first provider responder.
2) Much better coordination at the policy level by the Federal government is needed, with the understanding that most of the activity is at the state and local level.

Federal Programs for Terrorism Preparedness:
Make programs and FUNDING specific enough for EMS that it is not gobbled up by State Health Agencies to fund project for local health departments that have minimal initial response responsibilities.
State Programs for Terrorism Preparedness:
As previously stated in above comment.

HOSPITALS

Federal Programs for Terrorism Preparedness:
Need to address the needs of small rural hospitals with limited funds. Most of the preparedness activities, programs, etc., focus on large hospitals with lots of resources. The government may want to break down hospitals into categories pertaining to size of hospital and population served and geographical area. Then develop or help develop standardized response plans for those categories.
State Programs for Terrorism Preparedness:
Same as above.
Organization's Experiences or Lessons Learned:
Rather than spend a lot of money we don't have, try to determine ways to respond using current resources or thinking "out of the box." If we have no decontamination equipment, use a pool, a hose, and a couple of tarps around a pt for decontamination, etc.

Federal Programs for Terrorism Preparedness:
Please let us know where funding and training can be sought.
State Programs for Terrorism Preparedness:
Assist small facilities especially the border facilities (Canadian border).

Federal Programs for Terrorism Preparedness:
Need consented and consistent training drills and exercises. The state and feds can coordinate the best system-wide.
State Programs for Terrorism Preparedness:
Same as above.

Federal Programs for Terrorism Preparedness:
In reference to questions 77 and 78 – if Homeland Security (DHS) is responsible for terrorism preparedness, then perhaps Public Health and HRSA should be managed by or work closely with them to ensure we have one plan to follow.
State Programs for Terrorism Preparedness:
Our state Department of Public Health is doing a fantastic job of managing HRSA funds and developing a hospital response plan by regions. If we received that same assistance from our Emergency Management and Homeland Security, the state would be better prepared.
Organization's Experiences or Lessons Learned:
How important it is for all entities to work together under one plan towards a common goal.

Federal Programs for Terrorism Preparedness:
Get the dollars to the local level – distribution to state ensures allocation to state levels with little to local hospitals.
State Programs for Terrorism Preparedness:
[Same as above.] Develop uniform realistic response protocols for implementation at local level.

Federal Programs for Terrorism Preparedness:
Federal money is being poorly used at the state level – guidelines on appropriate levels of equipment/training/personnel for each health care facility should be developed and then funded 100%.

Organization's Experiences or Lessons Learned:
Experience with SARS cases at nearby airport has strengthened our skill at dealing with all infectious diseases.

Federal Programs for Terrorism Preparedness:
I have seen absolutely no effect for any Aederal program. Anything that has been done, we have done ourselves.

Federal Programs for Terrorism Preparedness:
OSHA guidelines conflict with preparedness activities, things like fit testing, respiratory protection plan.

Federal Programs for Terrorism Preparedness:
Keep small rural hospitals involved and well prepared – we may be the first impacted because we aren't as well versed, drilled, etc., as major cities.
State Programs for Terrorism Preparedness:
Same as above.

Federal Programs for Terrorism Preparedness:
I believe the Federal government should be more involved with assisting hospital organization. There should be specific liaison access to address issues of preparation including technical and financial support. We are a rural hospital with limited resources.
State Programs for Terrorism Preparedness:
I believe most of the money the state has received has gone to own grandiose schemes and not to address local areas. The big boys in our State (our City) have gotten the bulk of the funding.
National/Professional Organizations Efforts in Terrorism Preparedness:
Greater technical support.
Organization's Experiences or Lessons Learned:
I believe there should be a center coordination body – one-stop shopping.

Federal Programs for Terrorism Preparedness:
There is so much training/equipment and seminars available to hospitals, but there is not adequate funding. Security, safety, and awareness are extremely expensive. Last year we (our hospital) received $9,000. We spent eight times that amount and we were conservative with expenditure.
Organization's Experiences or Lessons Learned:
Yes, hospitals need to share lessons learned in a more non-competitive arena.

Federal Programs for Terrorism Preparedness:
More information (if not capital) sharing to rural (vs. urban) facilities.
State Programs for Terrorism Preparedness:
Same as above.
National/Professional Organizations Efforts in Terrorism Preparedness:
Same as above.

Federal Programs for Terrorism Preparedness:
In the rural part of our State, the threat known is very small. Our greatest threat is being asked to assist others. Our traffic-way will cause us collateral more than direct involvement. Unless told we have a direct threat, I will continue to plan for conventional and industrial reactions more than tactical responses to a localized threat.
State Programs for Terrorism Preparedness:
Develop a communications system with at least one redundancy; Communicate more to health care locations what the support is in each area of responsibility being segregated; Set up an auto-e-mail information source (website), with or without access codes, to keep updated our state level threats or intelligence flow.

National/Professional Organizations Efforts in Terrorism Preparedness:
Additional training and updates are always needed.

Federal Programs for Terrorism Preparedness:
To standardize the program and standardize available equipment. This would allow state and Federal training to be the same – cost savings. Everybody is going in own direction, different equipment, different training, no continuity from one facility to the next, one agency to the next. Military equipment and training from one branch to the next comparable so people can work together, train together, speak the same language. List: this is the equipment available. Provide: training curriculum. Personnel from one hospital could be sent to another to assist in an emergency – typically can't be done now.
Organization's Experiences or Lessons Learned:
We strongly feel that the true impact that terrorists have had on the country is how successful they have been at getting us to divest our time, energy, money, etc., to this very nebulous effort and the stress that we have all endured.

State Programs for Terrorism Preparedness:
Assistance with field drills.

Federal Programs for Terrorism Preparedness:
A lot–most–of the money that was designated for bioterrorism went to fire/police departments. Of more than $63,000 earmarked for bioterrorism, only $5,000 went to hospitals.
State Programs for Terrorism Preparedness:
District-wide training.

Federal Programs for Terrorism Preparedness:
1) Get funding red tape under control and get funding availability down to the hospital level immediately (not local EMS/EMA agencies). 2) Standardize syndromic surveillance technology at national level – automate ASAP! 3) Provide for funding of ANFTE add-on to assist regional hospitals with dedicated terrorism staff expertise.
State Programs for Terrorism Preparedness:
1) Look at Georgia model for implementation.
2) Help states streamline funding channels.
3) Provide funding for FTE add-one for terrorism…regional HC systems.
4) Get ODP to recognize level A&B decon EQ's training needs in hospital – DO NOT CAP AT LEVEL C – no detection equipment or expertise – this seem like a…battle with EMS.
National/Professional Organizations Efforts in Terrorism Preparedness:
Create ANSI standardized for "second responders" – hospital WMD/hazmat PPE operations.
Organization's Experiences or Lessons Learned:
1) Weakness in the Public Health System.
2) Need to shift focus of terrorism from HHS to Homeland Security.

Federal Programs for Terrorism Preparedness:
Federal government should supply a standard plan and provide each hospital with the equipment and funds for compliance.
State Programs for Terrorism Preparedness:
Provide advances on grant funds to facilities.

Federal Programs for Terrorism Preparedness:
Best practices/Clearinghouse info/website would be helpful.

State Programs for Terrorism Preparedness:
Better coordination of training and funding for communication issues.

Federal Programs for Terrorism Preparedness:
Preparing training modules, helping develop and implement training exercises, and providing annual support for equipment and personnel should be primary functions of state agencies with the underlying funding supported by federal dollars. Direct Federal involvement should include manpower support for occurrences and more significant intelligence about threats.
National/Professional Organizations Efforts in Terrorism Preparedness:
Training modules for components of CBRNE should be developed by the federal government in conjunction with specific groups like NAEMSP, ACEP (American College of Emergency Physicians), ENA (Emergency Nurse Assoc.), etc.

LOCAL PUBLIC HEALTH

State Programs for Terrorism Preparedness:
Provide templates and recommended forms for plans, job descriptions (i.e. for staff at a mass immunization clinic).

Federal Programs for Terrorism Preparedness:
Small Health Departments need easy, accurate planning templates for response plans. We should all be doing relatively the same thing and responding the same way. Help!

State Programs for Terrorism Preparedness:
Coordination between State Emergency Management and State Health.
Organization's Experiences or Lessons Learned:
Yes. Locally, we are better coordinated with Public Safety/Hazmat/Fire/EMS Law Enforcement than the State Agencies are to one another and to the locals.

Federal Programs for Terrorism Preparedness:
Yes, 1) Responsible to all risk communication. 2) Liaison to police, fire, emergency management.
Organization's Experiences or Lessons Learned:
Management of media messages is key. Our residents get disease/terror info instantly on Web and CNN. Messages must be in real time. HAN is vital. Must be faster.

Federal Programs for Terrorism Preparedness:
Need Federal dialogue in appropriate response to actual smallpox case – i.e. ring or mass vaccination. How many cases, where, what circumstances would trigger mass vaccination?
State Programs for Terrorism Preparedness:
Would like additional help from state in designing and carrying out exercises.
Organization's Experiences or Lessons Learned:
Trying to overcome complacency of physicians.

State Programs for Terrorism Preparedness:
More exercises, funding to augment time away for training and exercises.

Federal Programs for Terrorism Preparedness:
Continue to closely monitor relationship between state and local agencies.

Federal Programs for Terrorism Preparedness:
Ensure uniformity/consistency nationwide (top-down).
State Programs for Terrorism Preparedness:
Same as above.
Organization's Experiences or Lessons Learned:
Tremendous staff time required sacrificing needed public health services.

Federal Programs for Terrorism Preparedness:
Need to integrate public safety and health agencies in research, training, planning, communications, operations and recovery efforts – still very insular.
Organization's Experiences or Lessons Learned:
Public service employees have important roles to play within public health but also in numerous support functions throughout government agencies and with community-based resources.

Federal Programs for Terrorism Preparedness:
Use resources wisely. Prevent duplication of service. Put in a days+ work. Take job seriously. Ask for local input prior to policy/law making – since the front lines have the experience and firsthand knowledge of what will work and what will muck up a working system.
State Programs for Terrorism Preparedness:
Be prepared to roll up sleeves and help. Merit input at local level. Don't put every city in a mold – big and small cities have major differences in resources and needs and risks. Listen/Work/Help!

Organization's Experiences or Lessons Learned:
Difficulty hiring for position for emergency response has on adding duties of emergency preparedness to other duties. Lack of background. Identified "turf" still exists.

Federal Programs for Terrorism Preparedness:
Far too much emphasis on smallpox.
State Programs for Terrorism Preparedness:
State programs are organized, planned and imposed on local health departments by people with little field experience and less common sense.

Federal Programs for Terrorism Preparedness:
Yes, criteria for allocation of grant funding should be determined jointly by Federal, state, and local agencies.
State Programs for Terrorism Preparedness:
Yes, priorities for funding allocations should be determined at the local level.

Federal Programs for Terrorism Preparedness:
The local public health system (non metro urban areas)/(rural) do not have the money, personnel, capacity to respond at the local level. Public health needs to be a system; not based on voluntary participation at the local level.
State Programs for Terrorism Preparedness:
States need to ensure that monies received for designated activities, are, indeed spent on that intended.

State Programs for Terrorism Preparedness:
Need more training in all areas WMD response planning etc.

Federal Programs for Terrorism Preparedness:
The guidance documents are very difficult to follow. Far better compliance would be achieved if information was transmitted clearly and concisely. Models with timelines and checklists seem to work best. While there is no interest in stifling local initiative, there are tremendous benefits to seeing that all jurisdictions achieve a solid foundation quickly.
State Programs for Terrorism Preparedness:
Yes. Our state has not regionalized its effort. The result is that we have 55 counties doing own thing without a cohesive, collaborative effort.
Organization's Experiences or Lessons Learned:
Tremendous teamwork has been developed at our agency.

Federal Programs for Terrorism Preparedness:
The smallpox vaccination program is hindered by the lack of workmen's compensation coverage at our regional hospitals.
State Programs for Terrorism Preparedness:
Same as above.

Federal Programs for Terrorism Preparedness:
Get more money to the local level where the work is being done. Fewer hurdles to get money, results at the local level.
State Programs for Terrorism Preparedness:
Private sector training exercises don't help the local level responses or provide a secure environment to the public.
Organization's Experiences or Lessons Learned:
Credentialing volunteer(s) properly is an issue that is not easy to accomplish. Getting volunteers to step up when not in imminent danger is also hard to accomplish. Local health departments have no money for PPE for biological so definite lack of equipment for chem., nuclear, incendiary incidents. Local public health departments also lack communication capability with other local emergency responders. (800 Mhz) tracking radios that are secure with HIPAA are quite costly, about 45,000 each.

State Programs for Terrorism Preparedness:
Yes, carry forward funding from fiscal year to fiscal year.

Federal Programs for Terrorism Preparedness:
Some of the areas do not take planned activities into account. Some programs, such as ours, are new and have not had enough time to accomplish specific items in the survey, but have them planned for the near future.

Organization's Experiences or Lessons Learned:
Our county has gaps in communication with our county hospital. This communication is badly needed.

Organization's Experiences or Lessons Learned:
Yes – the role of the health department in emergency operations is much diminished. Conventional first responders (law enforcement, fire service/EMS) are welcoming the new emphasis on countering bioterrorism and the resources being brought to bear on the issue.

Federal Programs for Terrorism Preparedness:
Adequate funding for local health departments in high-risk areas would be a tremendous help!

Federal Programs for Terrorism Preparedness:
Much of the Federal approach to funding (especially Department of Justice) is irrational. It is based on purchasing equipment/supplies without regard to either the existence of a plan or consideration of responders' roles in a WMD response. Funding would be better directed at system response standards (i.e. specific functional responses). Equipment, personnel and other resources could then be rationally determined.
State Programs for Terrorism Preparedness:
Our state has yet to develop a vision of what a successful response to terrorism or emergencies should look like. All work is buried in specific technical actions and details without a unifying framework. There needs to be emphasis on 1) the big picture of capacity and 2) the process for achieving that capacity.
Organization's Experiences or Lessons Learned:
Preparing for terrorism has helped us become more flexible organizationally. We are more fluent in negotiating organization al cultures outside of public health. We have also learned to implement actions at a scale and speed that we previously hadn't imagined.

Federal Programs for Terrorism Preparedness:
I believe there has been too much money given to too many organizations, state and county-wide. There is much duplication and not enough definition of the hierarchy of control (i.e., everyone believes his/her organization is in charge). If there ever was an incident, there would be mass confusion. In addition, perhaps the worst fiasco to come out of this preparedness issue has been the smallpox inoculations. This so called risk appeared out of nowhere. No one could even tell us satisfactorily who picked this disease as a risk to the nation. The information on this and other issues has been very slow to non-existent in coming to us in local public health. We are supposed to support the decisions that are made at higher levels and relate directly to the public. I have found this to be an impossible task.
State Programs for Terrorism Preparedness:
The state health department's deadline for submission of its grant was much too short! They were given virtually no time to put together a well conceived plan for terrorism preparedness.
Organization's Experiences or Lessons Learned:
No – but like most Americans, we only feel the axe of cutbacks in other important public health programs. Most, if not all, of my staff are not preoccupied on a daily basis with thoughts of domestic terrorism. They focus instead on areas of public health, most of which have been cut back due to the increases in the dollars given to terrorism preparedness. If anything, there is a great deal of resentment towards the preparedness programs.

Federal Programs for Terrorism Preparedness:
None that hasn't already been covered.
State Programs for Terrorism Preparedness:
Development of templates for plans and forms that can easily be adapted for locality specific situations.
Organization's Experiences or Lessons Learned:
The political, inter-agency and inter-jurisdictional issues which must be addressed to be successful.

Federal Programs for Terrorism Preparedness:
1) Plan for regionally trained staff to provide leadership in events. 2) Plan drills every 6 months for increased proficiency.

State Programs for Terrorism Preparedness:
Same as above.
Organization's Experiences or Lessons Learned:
Realization that, as trained staff leave, we experience huge loss of preparedness abilities.

Federal Programs for Terrorism Preparedness:
Yes: a local man was one of those infected with anthrax. NO special program to help him and family despite being unable to work! Better quality education ex. Smallpox. Too voluminous, information changed over time.
State Programs for Terrorism Preparedness:
Better mental health services for victims of terrorism.
Organization's Experiences or Lessons Learned:
That the victims can be forgotten despite great losses to personal lives and families.

Federal Programs for Terrorism Preparedness:
I believe the President is trying to protect this country from another attack, but we need better cooperation among the Federal, state, and local agencies. Due to budget cuts, the money is not filtering down to the local level. We feel left out of the loop.
State Programs for Terrorism Preparedness:
Better surveillance systems for chemical, biological, events.
Organization's Experiences or Lessons Learned:
People still worry about turf protection of individual entities instead of the good of all the people.

Federal Programs for Terrorism Preparedness:
Progress has clearly been made – funding needs to be flexible and based on local priorities and needs. To effectively respond to a bioterrorism incident, the entire public health system has to be rebuilt – plans without personnel are only "shelfware."
State Programs for Terrorism Preparedness:
Good effort at state level. Staffing is marginal, skill-levels are shakey. Leadership is excellent, however. Need dedicated, long-term, capacity building funding (not short-term crisis oriented).
Organization's Experiences or Lessons Learned:
Public Health system has woefully deteriorated in past 40 years – public and medical community awareness is very low.

Federal Programs for Terrorism Preparedness:
Communication with all levels.

Federal Programs for Terrorism Preparedness:
Federal agencies need to better understand the circumstances and constraints on local agencies. We appreciate the "guidances" that have been issued; but guidance that recommends/requires eight times the available staff is not helpful. Guidance that expects we can utilize non-existent professionals is also not helpful. And it is not realistic to expect local agencies to prepare a plan in two weeks to respond to a document the Federal agency spent 9 months – 1 year writing.

Federal Programs for Terrorism Preparedness:
We sponsor a DMAT team. There should be better information about appropriate use of DMAT teams. The federal government should train individuals/teams to manage the initial phase of SNS distribution.
State Programs for Terrorism Preparedness:
State should train individuals and help coordinate SNS distribution regionally (between counties).
Organization's Experiences or Lessons Learned:
We have competent, resilient staff who have good reason to believe they can respond appropriately if and when they are asked to do so.

Federal Programs for Terrorism Preparedness:
See comment below.
State Programs for Terrorism Preparedness:
1) Better cooperation and integration of plans/expectations from state level. 2) Plan based on ICS/IMS structure, not focus areas. 3) Less emphasis on information technology. It will fail in many emergencies. 4) Require less detail in plans. Plans must be general to allow adaptation during emergencies.

Organization's Experiences or Lessons Learned:
The strength of plans rests in the partnerships and trust formed at the local level. Partnership between local and state, as well as local/fed, level is in need of improvement. Multiple conflicting demands on local health departments are counterproductive.

Federal Programs for Terrorism Preparedness:
There is much technical assistance and information provided by CDC to bioterrorism-grantees that never trickles down to the front line, or local health departments. This information (e.g. HAN info, training guidelines, etc.) should be more available, meetings opened up to all levels of public health agencies, who would benefit from the information, even if they remain ineligible for direct funding.
State Programs for Terrorism Preparedness:
Much of the state's bioterrorism funding appears to be spent on NEDBS and other information systems/sources, with little demonstrable improvement in capacity to identify or investigate outbreaks. Additional staff should be hired, especially at district/local level, with better coordination and leadership centrally. Current state efforts suffer from lack of front-line contributions, like coordination with state EMA, political concerns overriding any intelligent or clear vision for true, statewide preparedness.

Federal Programs for Terrorism Preparedness:
Better inter-agency coordination and information sharing.
State Programs for Terrorism Preparedness:
Programs are too "stove-piped" – different CDC Focus Area programs are not well coordinated.
Organization's Experiences or Lessons Learned:
Incident command system and all "hazards planning" for local health departments, money for one-time and staff back-filling to allow for more training and exercises.

Federal Programs for Terrorism Preparedness:
Need direct contact with individual departments to assess specific needs.

Federal Programs for Terrorism Preparedness:
Continued support and planning.
State Programs for Terrorism Preparedness:
Rebuild public health infrastructure.

Federal Programs for Terrorism Preparedness:
Move training closer to local level.
State Programs for Terrorism Preparedness:
Fund locals based on population formula not base plus population. This latter formula is very poor with larger units. The smaller units tend to come to anyway.

Federal Programs for Terrorism Preparedness:
We work very closely with the city County HHS which retains a great deal of the personal resources to address the issues in this study.

Federal Programs for Terrorism Preparedness:
Local input into needs – no bureaucratic ladders. Thank you.
State Programs for Terrorism Preparedness:
The state has been receptive of our efforts at coordinating our metropolitan area's and statewide activities.
Organization's Experiences or Lessons Learned:
Helpful in preparing for West Nile and SARS.

Federal Programs for Terrorism Preparedness:
Looking back two years, this region/state has made tremendous progress. The time-lag on funding held up needed staff recruitment and training. This region is still in the recruitment and training of new bioterrorism (BT) staff. Older public health staff with Civil Defense training has given the support needed immediately (smallpox, community assessments, emergency response plans, etc.)

Organization's Experiences or Lessons Learned:
1) Need for closer working relationship with regional State Emergency management coordinators; law enforcement and emergency medical personnel. 2) Need for better emergency communication system locally and state wide. 3) Need to recruit/maintain younger people into public health.

Federal Programs for Terrorism Preparedness:
The money should all be saved in a fund for clean up and rebuilding a city! We are not stopping anyone with this training.

Federal Programs for Terrorism Preparedness:
On the local level classify the roles/responsibilities of staff response and involvement to incidents other than bioterrorism, i.e. chemical, radiological, nuclear, IED, cyber.
State Programs for Terrorism Preparedness:
The State Division of Mental Health in our state is dangerously ill-prepared, ill-equipped, and poorly trained to respond to even a minor incident. State and local mental health do not involve themselves in preparing or planning for any such events.

State Programs for Terrorism Preparedness:
Allow local health districts to carry over WMD funding from CDC into next budget year. The state is throwing monies at local health districts so fast that we are unable to effectively utilize the funds.
Organization's Experiences or Lessons Learned:
Intra- and inter-agency communication and coordination are still presenting problems. This will be a concern and should be addressed in greater detail.

Federal Programs for Terrorism Preparedness:
From the local level, it appears that the HRSA and CDC bioterrorism preparedness programs are not well integrated and operate in an overly compartmentalized manner. While local health departments (LHDs) do not receive HRSA hospital preparedness funds, we do receive CDC funds to support activities that require working with the same partners and issues addressed by the HRSA funds. At the local level, we integrate activities funded by both agencies, but do not see the same at the federal or state levels.
State Programs for Terrorism Preparedness:
Local health departments need to be seen as both state and Federal agencies' strongest partners for developing strong state and Federal public health preparedness programs. Deliberate efforts and practices by both state and federal agencies to work through local HDs and local public health preparedness programs is necessary to build these programs at local level and support LHDs' role as leaders in communities.
Organization's Experiences or Lessons Learned:
1) Local health departments are state and Federal government's best and strongest partners for developing state and national programs, and need to be recognized and supported as leaders in communities by working through them, not around them.
2) Over compartmentalization of programs inhibits development of an integrated approach at the local level.
3) Cannot under estimate or overlook the costs of infrastructure development, including time, money, personnel and capital equipment, and the need for a grants management infrastructure. Investments are needed at the local level to support both programmatic and administrative infrastructures to assure program success and integration with the local unified command structure.

Federal Programs for Terrorism Preparedness:
Standardized templates – I'm tired of recreating systems that could be the same across the nation.
State Programs for Terrorism Preparedness: Standardize templates.

STATE PUBLIC HEALTH

State Programs for Terrorism Preparedness:
Funding at state level.
Organization's Experiences or Lessons Learned:
Personnel issues continue to plague planning and preparedness.

Federal Programs for Terrorism Preparedness:
Federal programs should provide sustained, stable base funding for public health preparedness, basic public health and environmental protection programs, emergency medical services and trauma systems, and health care coverage,

so that basic public health and medical care and surge capacity are supported and sustained. Federal funding for chemical, radiological and nuclear response and preparedness is inadequate.
State Programs for Terrorism Preparedness:
Our State budget is under severe stress and is not able to provide additional support for counter-terrorism efforts. Basic public services are being severely reduced.
Organization's Experiences or Lessons Learned:
Counter-terrorism and preparedness for response to WMD need to be a high public health priority because the threat of a catastrophic biological attack or emerging infectious diseases is real. SARS, pandemic influenza, or rapid spread of diseases like West Nile Virus all represent real threats. With potential for catastrophic consequences, public health is cheap insurance, considering the magnitude of biological threat.

Federal Programs for Terrorism Preparedness:
More flexibility in use of funds. We find that we cannot utilize CDC and HRSA funds to complete parts of our emergency response plans (are not permitted to utilize funds for medications or certain equipment). Constant frustration working with CDC. HRSA much easier.

Federal Programs for Terrorism Preparedness:
More flexibility with funding uses. Focus on sustainable infrastructure building.

Federal Programs for Terrorism Preparedness:
We need clarification about what constitutes an adequate assessment and resultant response plan. Contingency planning is not part of the culture of public health, and so there is little experience to guide the development of response plans.

Federal Programs for Terrorism Preparedness:
Communication has not improved over last 1½ years, from Feds to state.
Organization's Experiences or Lessons Learned:
Challenge is building foundational elements while concerned about sustainment of funding.

Federal Programs for Terrorism Preparedness:
Coordinate the Federal terrorism-related grants.

Federal Programs for Terrorism Preparedness:
More converge w/in DHS. We (in Our State) are doing a great job of working with ODP Grantee and FEMA/DHS grantees – FEDERAL level still appears disjointed. NIMS – we were asked to comment on draft, but not invited to the session in D.C. – vulnerability and risk assessments are being funded by at least 3 Federal agencies. We don't have time!
Organization's Experiences or Lessons Learned:
Slow down – the smallpox program alienated many of our local health departments and over taxed the limited state staff. No progress was made in many of the more critical areas (Planning, Training, Exercising). Advocate using ODP money to fund all WMD exercises at all levels. It works for us.

Federal Programs for Terrorism Preparedness:
Centralized Federal surveillance and response for terrorism would be more efficient than repeating the exercise 50+ times.
State Programs for Terrorism Preparedness:
State government need to establish streamlined systems to administer the programs.

Federal Programs for Terrorism Preparedness:
Required integration of WMD-DHS funding for first responders and public health/hospitals.
Organization's Experiences or Lessons Learned:
The recent power blackout tested communication systems that are power based. Many patients are being discharged to home or are in ambulatory care (outpatient facilities), that rely on medical devices that require power. Hospitals are being asked to absorb these patients during power outages and this may be unrealistic.

Federal Programs for Terrorism Preparedness:
More flexibility in utilization of funds to meet particular circumstances of jurisdiction for preparedness.

Federal Programs for Terrorism Preparedness:
Our greatest difficulties are inability to hire staff even there is money (HR stalls) and inability to move money/contracts to assist in projects. Department infrastructure staff are angry that terrorism efforts are diverting resources and tend to throw up special "oversight" requirements – i.e., its bureaucratic red tape not imposed on other programs.
State Programs for Terrorism Preparedness:
Lack of coordination between CDC and HRSA grants is simply unacceptable. At this point, Department of Homeland Security provides us no benefit other than confusion and misuse of resources.
Organization's Experiences or Lessons Learned:
Improved all hazards approach.

Federal Programs for Terrorism Preparedness:
Need better coordination of funds coming from all the different Federal sources. Too many overlapping reports required. Expenditure tracking requirements across grants are not consistent and often very labor intensive. Need to be streamlined.

Federal Programs for Terrorism Preparedness:
Templates/training specific to cooperative agreement requirements. Coordination of reporting requirements to funding agencies and others. Enhanced biologic response tools/infrastructure (surveillance; planning; exercising; laboratory; communication; risk communication) has enhanced response to emerging infectious disease(s), (SARS, West Nile, Monkeypox, etc.)

Federal Programs for Terrorism Preparedness:
Clearly understand need for strong accountability of funding. However, need to evolve meaningful methods of undertaking this. Grants management activities and required fiscal tracking systems that frequently change, etc. are impinging upon/delaying ability to get actual preparedness task accomplished.
Organization's Experiences or Lessons Learned:
Importance of developing a good all hazards plan first before adapting to specific scenarios/diseases – smallpox, pandemic flu, SARS. Push for disease specific plans is too soon.

Federal Programs for Terrorism Preparedness:
1) Establish and fund a national laboratory response network that will assure adequate lab support for bio, chem., radiation and nuclear detection, response and assessment is available. 2) Require that USDA, FDA, EPA coordinate with and fund state capabilities to respond to food and environmental incidents much like CDC has done for biological incidents.

Federal Programs for Terrorism Preparedness:
Assistance with operational planning and development of medical and health incident management structures. Increased attention to special populations.
Organization's Experiences or Lessons Learned:
This survey is very comprehensive, but does not show qualitative measure of our progress. We are underway with many preparedness activities, but we still have a long way to go. Other areas that we may have answered "no" are in the planning stages.

Federal Programs for Terrorism Preparedness:
Too much reporting required on grants. The administrative burden is overwhelming and a barrier to program achievement.
State Programs for Terrorism Preparedness:
Get some templates developed and distributed.

APPENDIX E–CIVIL LIBERTIES IN A POST-9/11 WORLD*

The attacks of September 11, 2001, led to new laws, policies, and practices designed to enhance the nation's security against the terrorist threat. These security measures have prompted a debate about their impact on civil liberties. For its final report, the Advisory Panel seeks to contribute to the development of a long-term, sustainable approach to security that protects not just lives but also our way of life.

The Panel could advance this objective by reframing the terms of the civil liberties debate and emphasizing the importance of understanding the implications of the fundamentally altered environment in which individual counterterrorism initiatives need to be evaluated. Rather than the traditional portrayal of security and civil liberties as competing values that must be weighed on opposite ends of a balance, these values should be recognized as mutually reinforcing. Under this framework, counterterrorism initiatives would be evaluated in terms of how well they preserve all of the unalienable rights that the founders believed were essential to the strength and security of our nation: life, liberty, and the pursuit of happiness.

Moreover, an effective evaluation should focus not just on individual initiatives but on the way these initiatives fit into a fundamentally changed approach to counterterrorism overall. For example, we have moved from a largely law-enforcement approach in combating terrorism to a global war in which the continental United States is part of the battlefield. It is important to analyze the impact this may have on public reaction, judicial interpretation, and the applicable legal framework. Similarly, the FBI now has a broader mission that often eliminates the traditional requirement for a criminal predicate in order to justify intrusive investigative techniques. "Law enforcement" means something different than it did on September 10, 2001. These new paradigms must inform the evaluation of existing and proposed laws and policies.

Reframing the Debate

In times of crisis, when the pressure for dramatic change is most intense, it is helpful to return to the fundamental principles that have guided this nation since its inception. As Thomas Jefferson advised in his first Inaugural Address, "[t]he essential principles of our Government form the bright constellation which has gone before us and guided our steps through an age of revolution and reformation....[S]hould we wander from them in moments of error or of alarm, let us hasten to retrace our steps and to regain the road which alone leads to peace, liberty and safety."

The Declaration of Independence rests on the premise that there are certain "unalienable rights," to include "Life, Liberty and the pursuit of Happiness." The terrorists seek to destroy all three of these. A successful strategy to defeat the terrorists' objective, then, should seek to preserve not just life, but also liberty and our way of life.

Moreover, history teaches that the debate about finding the right "balance" between security and civil liberties is misleading. This traditional debate implies that security and liberty are competing values and are mutually exclusive. It assumes that our liberties make us vulnerable and if we will give up some of these liberties, at least temporarily, we will be more secure. Yet, consider the context in which civil liberties were first firmly established. The framers of the Constitution had just survived a truly existential threat and were acutely aware of the fragility of their nascent nation. In this uncertain and insecure environment, the framers chose not to consolidate power and restrict freedoms but to devolve power to

---

*** Suzanne Spaulding, J.D.**

the people and protect civil liberties from encroachment. They recognized that civil liberties and security are mutually reinforcing. Security clearly ensures the freedom to exercise our liberties, but it is also true that the exercise of civil liberties and our way of life contributes to our strength and security.

For example, no one individual or handful of people possesses the knowledge, wisdom, and skills to defeat the threat of terrorism. The solutions can only be derived through collective wisdom and innovation emerging from the marketplace of ideas that flourishes in a free society. The frequent admonition to "think outside the box" reflects the recognition that iconoclastic, nonconformist input maximizes the prospects for finding solutions. To meet today's threats, we need technological breakthroughs, such as the development of sensors to detect deadly chemicals or biological agents, and new ideas, such as ways of educating and assisting citizens to effectively protect themselves in the event of a terror attack. These developments are far less likely to emerge where "group think" dominates.

Yet many of the security measures added or expanded after 9/11 involve efforts to detect terrorists by looking for "outliers." Government officials at all levels, as well as the American public, have been instructed to watch for activity that is different or outside the norm. Combine this with the prospect of increased government surveillance over an ever-widening range of activities and individuals, and the pressure to conform grows.

Protection of civil liberties and our way of life also promotes the kind of relationship between the government and the governed that keeps the nation strong and secure. The framers understood that the strongest nation would be one in which the people viewed their government as "us" and not "them." The brave men and women who struggled on September 11 to keep their plane from being used to decapitate the government confirmed that the most effective antidote to threats inside our borders is an informed citizenry committed to preserving a nation in which they have a very real stake. Yet security restrictions can begin to drive a wedge between government and the people. Before the attacks of 9/11, an average of 10,000 to 20,000 visitors roamed the halls of the U.S. Capitol on busy days. Now, visitors are only allowed if they are on a tour, and the number is down to about 1,000. Similar limitations on access characterize Federal offices all across the country. A government that shuts off the halls of power inside jersey barriers and cloisters its public servants behind armed guards runs the risk of detaching itself from the governed.

Local police have learned how essential it is to become a more integral part of their communities.[63] Moreover, citizen support is strengthened by a sense that the system is just and fair. If that conviction begins to erode, so might vital citizen support. Thus, some police departments have expressed concern about some of the activities that Federal officials have asked them to undertake in their local communities, particularly with regard to enforcement of immigration laws. The concern is greatest with respect to the Arab American community, where support for government efforts could yield significant benefits but relations are often severely strained by policies perceived to be discriminatory.

Similarly, one of the greatest risks of the current plans for responding to bioterrorism, which are based primarily on compulsory measures such as quarantine or mandatory vaccinations, is that they may create an adversarial relationship between the government and the public. One of the most compelling advantages of adding the option of a measure such as Shielding, or "stay at home," is that it undermines the terrorist objective by building upon the strengths of democracy. Our system of government reflects the framers' faith in the wisdom of an informed citizenry to make decisions about what is best for themselves, their families, their communities, and their nation. Shielding reflects that same belief and

[63] See "Community Policing and Terrorism", Matthew C. Scheider and Robert Chapman, *Journal of Homeland Security*, April 2003, (http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=88) which emphasizes that "community policing philosophy is well positioned to play a central role in local law enforcement responses to terrorism" p.2.

takes advantage of the strengths of a democracy, empowering ordinary citizens through education and community-based decision-making.

The rights described in the Declaration of Independence and enshrined in the Constitution were not viewed as a luxury of peace and stability but as the best hope for a people embarking on the dangerous and daring endeavor of creating a new nation. They are no less essential to the nation's security today. Thus, proposed security measures should be evaluated on how well they frustrate the terrorists' targeting not just of life, but also liberty and the pursuit of happiness. The impact on these latter rights may be clear and direct, such as denial of due process, or subtler, such as chilling first amendment activity, creating pressure to conform, or otherwise deterring lawful activity. These more subtle effects are largely a result of the sense that government is casting a broad net that is more likely to "catch" non-terrorists—i.e., us.

Many of the security initiatives implemented since 9/11 have been challenged as possible violations of the Fourth Amendment prohibition against unreasonable search or seizure. Some of these challenges are currently pending in Federal courts. However, this paper focuses on the more subtle and potentially profound impact on the exercise of First Amendment rights and, more broadly, on the ability to pursue our way of life.

Evaluating an initiative's impact on "the pursuit of Happiness" can also yield a more accurate assessment of its cost. Overly burdensome financial reporting requirements, for example, may not infringe on core civil liberties, but they do raise transactional costs and will inhibit beneficial activity along with criminal activity. Similarly, the opportunity to fly may be viewed as a privilege rather than a right, but overly stringent and apparently arbitrary security hurdles can not only have an economic impact but also increase public skepticism about security measures generally.

A clearer assessment of the full costs of security measures should provide insights into more effective ways of achieving the desired impact on terrorist activity while minimizing the impact on our way of life. Narrowing the scope of new legal authorities, providing procedural or technological safeguards against abuse, or simply doing a better job of educating the public on implementation might significantly reduce the potential harm from new measures without significantly reducing their effectiveness against terrorism.

Possible Recommendation:

Efforts to combat terrorism should be evaluated in terms of how well they frustrate the terrorists' objective of destroying life, liberty, and the pursuit of happiness.

Understanding the Broader Context

The civil liberties debate often focuses on specific laws, policies, or practices. However, as this paper attempts to illustrate, these initiatives are implemented in the context of fundamental changes in our counterterrorism approach, which can have a significant consequences for their overall effectiveness and impact on the protection of life, liberty, and the pursuit of happiness. This is presents a significant challenge for evaluating civil liberties in the post-9/11 world.

The War on Terrorism

One of the most immediate and dramatic changes brought about on the morning of September 11, 2001, was the shift from viewing terrorist attacks as first and foremost a crime to viewing them as belligerent operations in an ongoing war. Americans are only now beginning to sort through the full implications of this shift. It was fairly straightforward as manifested in the combat operations in Afghanistan. However, the end of that conflict did not signal the end of the global war on terrorism. Thus, all actions taken to

protect Americans from terrorist attack occur in the context of this war; a war in which the enemy cannot be distinguished by uniforms, nationality, or location, with no defined battlefield, and with no discernable end point. This war has an impact on how courts and the Congress view the actions of the Executive branch, on what laws apply, and on how those laws are applied.

As Supreme Court Chief Justice William Rehnquist noted in his book on civil liberties in wartime, *All the Laws but One*, it is often said that law is silent during war (*Inter arma silent leges*). In part, this is because, as a matter of law, the government's authority to restrict civil liberty is greater during war than in peacetime. But Rehnquist also observes that "[q]uite apart from the added authority that the law itself may give the President in time of war, presidents may act in ways that push their legal authority to its outer limits, if not beyond." In addition, courts are reluctant to decide a case against the government on an issue of national security during a war. Rehnquist ultimately rejects the traditional maxim, concluding that the laws will not be entirely silent in time of war, but he does conclude that "they will speak with a somewhat different voice."

It becomes important, then, to understand the impact that this "somewhat different voice" may have on the legal framework for counterterrorism

Homeland Defense—Distinguishing between law enforcement and military operations

The attacks of September 11 brought home the reality that the continental US is part of the battlefield in this unconventional war. As those who live along the Potomac River just outside the nation's capital can attest, the US military patrols this battlefield regularly in an effort to detect and deter enemy combatants. As further testament to the importance of the domestic mission of the military, the Department of Defense established a new command, the Northern Command, whose responsibilities include homeland defense and support to civil authorities. Yet, these new domestic missions for the military have received relatively little public discussion and debate.

One consequence of the homeland defense mission is its potential impact on the application of Posse Comitatus. Questions have been raised as to whether the Posse Comitatus Act[64] provided DOD with sufficient flexibility to perform its domestic missions. What has been missed in much of that discussion, however, is that posse comitatus only applies when soldiers are asked to perform law enforcement functions. It does not apply to military operations. In today's environment, activities or situations that look very much like law enforcement may turn out to be military operations or activities.[65]

Thus, if terrorists were known to be hiding inside a warehouse and the military arrived upon the scene, it might not be clear whether any action they took was part of a military operation against enemy combatants or a law enforcement activity against suspected criminals. The application of Posse Comitatus would be uncertain. Yet, some of the concerns that prompted the Posse Comitatus Act might also apply to the domestic use of the military in a combat operation.

---

[64] 18 USC sec 1385.

[65] Jose Padilla, the terrorist suspect arrested in O'Hare airport and subsequently designated an enemy combatant (*see "Enemy Combatants" section, below*), argued that his detention by the military violated the Posse Comitatus Act (PCA). The court found, however, that PCA did not apply: "Padilla is not being detained by the military in order to execute a civilian law or for violating a civilian law, notwithstanding that his alleged conduct may in fact violate one or more such laws. He is being detained in order to interrogate him about the unlawful organization with which he is said to be affiliated and with which the military is in active combat, and to prevent him from becoming reaffiliated with that organization. Therefore, his detention by the military does not violate the Posse Comitatus Act." Order of Judge Michael Mukasey, US District Court, SDNY, December 4, 2002, at 47.

Guidance on the use of force by the military is usually provided by "rules of engagement" (ROEs). Yet there are reportedly no clearly articulated rules of engagement or "use of force" rules to govern the military's actions inside the United States in a situation like that described above. It is hard to imagine how troops could have been adequately trained to respond appropriately to such a contingency without the development of such guidelines.

Possible Recommendations:

The potential for serious infringement of liberties stemming from the domestic deployment of troops could be significantly reduced by the development of ROEs for the Continental United States (CONUS), rigorous training, and publicly articulated standards and procedures for determining when the military is conducting a military operation in its homeland defense role and when it is conducting law enforcement activities. These issues need to be fully discussed in the public arena so that the American people understand and are prepared for the military's intervention, should that become necessary.

DOD Intelligence Collection

Another consequence of the homeland defense mission is the enhanced collection of intelligence by the military inside the United States. Just as the military undertook intensive intelligence collection in Afghanistan prior to and during the war in order to support its combat operations, the military is collecting intelligence on the battlefield here in the US. Thus, the Defense Advanced Research Projects Agency (DARPA) has funded research into advanced data mining technology that would gather information from US companies, though not about US persons. In addition, the *New York Times* reported that the DOD, along with the CIA, was seeking authority similar to that currently exercised by the FBI to compel US businesses to provide records on targeted individuals.[66] And the National Imagery and Mapping Agency, which is responsible for analyzing images from satellites, has significantly increased its interest in targets inside the United States.

Yet, our system of laws and safeguards did not anticipate the homeland defense mission. For example, domestic intelligence collection by DOD has generally been viewed as a law enforcement activity governed by Posse Comitatus and related policies. However, as discussed above, today domestic intelligence collection is presumably being undertaken for military purposes, something the current legal framework did not contemplate.

It is not entirely clear how the courts will view intrusive intelligence collection, such as satellite imagery, undertaken inside the United States for military purposes during a time of war. As we have seen in the cases involving electronic surveillance, the courts have allowed some distinction between purely domestic situations and those involving a foreign power or an agent of a foreign power. In that situation, however, Congress chose to step in and articulate clear procedures to govern electronic surveillance for intelligence purposes inside the United States, enacting the Foreign Intelligence Surveillance Act in 1978.[67] This new context may warrant similar clarification.

Even with respect to actions overseas, the global war on terrorism may render certain laws inapplicable. For example, Congress and the Executive branch developed an extensive system of safeguards with respect to covert actions. However, the relevant statute notes that the requirements to do not apply to "traditional military activities."[68] Thus, not only are actions that might look like law enforcement susceptible to being labeled military operations, activities that might otherwise be considered covert actions are likely to be viewed as military operations if undertaken by DOD. To the extent that this

[66] *See* "http://www.cbsnews.com/stories/2003/05/02/attack/main552014.shtml"
[67] 50 USC 1801 et seq.
[68] 50 USC 413b.

complicates oversight by Congress and the Executive branch, it may also frustrate efforts to fully understand the civil liberties implications of the war on terrorism.

Possible Recommendations:

Congress should consider working with the Administration to develop, in statute and/or Executive Order, new guidelines and procedures for domestic intelligence collection by the military. Definitions may need to be revisited, or additional safeguards added, in order to address the challenges of this unconventional war.

Enemy Combatants

The war on terrorism brings with it the legal framework of the law of armed conflict. Yet this body of law was developed to govern the actions of nation states. Attempts to apply it to non-state actors in non-traditional global conflict present unique challenges. This is most clearly evidenced in the legal issues surrounding the detention of suspected terrorists as "enemy combatants."

The courts are currently considering *habeas corpus* cases involving the detention as enemy combatants of two American citizens, Yasser Esam Hamdi and Jose Padilla. Hamdi was taken into custody in Afghanistan during the armed conflict there, while Jose Padilla was initially taken into custody by law enforcement officers in O'Hare airport and detained under the material witness statute. A few days before a hearing on the legality of his detention, Padilla was removed from the criminal justice system, designated as an enemy combatant, and transferred to military custody.

The US Court of Appeals for the Fourth Circuit, in Richmond, Virginia, has held in the Hamdi case that the President has the authority to designate US citizens as enemy combatants and detain them without access to a lawyer. However, the court has noted that Hamdi was apprehended in a "zone of active combat" and "during a military campaign on foreign soil." Thus, it is not clear that the court would reach the same conclusion in the case of someone captured inside the US, such as Jose Padilla.

US District Judge Michael B. Mukasey in New York is hearing Padilla's case. While he has agreed with the 4th Circuit that the President has the authority to detain a US citizen as an enemy combatant, he has ruled that Padilla "must have the opportunity to present evidence that undermines the reliability of the [government's] declaration." Unlike the 4th Circuit, Judge Mukasey ruled that "the only practical way" to give Padilla that opportunity was for Padilla to have access to his attorneys. The government argues that access to attorneys will defeat efforts to gather intelligence from these detainees that could prevent another terrorist attack. The government is appealing this decision and oral arguments are expected in the fall. To date, Padilla has been held in solitary confinement for over a year with no access to his attorneys. Under international law, prisoners of war can be detained for the duration of the conflict. No one has yet speculated on when the war on terrorism might end.

These cases have raised concerns about the potentially indefinite detention of Americans with no formal charges and no right to challenge the basis for their designation as enemy combatants. When individuals are detained outside a zone of combat, the risk of error is significantly heightened. Moreover, there is some concern that the threat to remove a criminal defendant from the civilian court into the indefinite status of an enemy combatant may introduce a level of coercion into our criminal justice system that threatens its fairness.

The government is pursuing policies that seek to preserve maximum flexibility to meet the unique and potentially unforeseeable challenges inherent in this new approach to terrorism as an ongoing war. Thus, it is reluctant to articulate hard and fast rules or make categorical statements that might wind up limiting options in the future. Yet, in addition to the direct impact on those detained, this approach risks

undermining public support over time by raising concerns of arbitrariness. Moreover, the uncertainty about the scope of this approach can have a chilling effect, just as with vague or over-broad criminal statutes.

Possible recommendations:

If the current enemy combatant policy is evaluated in terms of how well it protects life, liberty, and the pursuit of happiness, some changes might be recommended. Such recommendations might include establishing guidelines that define, at least in general terms, the circumstances under which an individual might be designated as an enemy combatant and the length of time an individual so designated could be held incommunicado for purposes of intelligence interrogation, as well as providing access to an attorney at the end of that period of time for those detainees taken into custody somewhere other than in a zone of active combat or foreign military campaign. Clearer guidance on the circumstances that might lead to eventual release or the filing of criminal charges against detainees would also reduce the sense that the designation is a legal "black hole."

Similar clarifications on the policies regarding non-US citizens detained in Guantanamo Bay, Cuba, might also serve to sustain national and international support over the long haul.

More broadly, given the significant implications of the legal status that this war, unlike the war on drugs, appears to have, it may be appropriate for the Administration, Congress, and the courts to consider distinguishing between the war against Al Qaeda and its affiliates, and broader counterterrorism efforts aimed at the phenomenon of terrorism generally or at other terrorist groups or individuals. Legal justification for this distinction, and for drawing some lines around the scope of the "enemy" could be found in the Congressional authorization for the use of force after September 11, which has been cited by the Executive Branch as part of the legal basis for the actions such as the detention of enemy combatants.

The resolution authorized the President to "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons." It is not clear that the "global war on terrorism" is limited to those covered by this authorization. While efforts to combat terrorism may well need to be broader than just those responsible for 9/11 and their helpers, and include those who have never targeted the US or Americans, it may be worth considering whether all of those efforts should have the legal status of a traditional war.

The Changing Role of Law Enforcement

Another significant change in the overall environment in which security initiatives should be evaluated is in the roles and mission of the FBI and local law enforcement. Where the Bureau's mission had been to investigate criminal activity with the objective of bringing a successful prosecution, the primary mission today is to prevent a terrorist attack. Criminal prosecution is simply one possible avenue for achieving this objective. Intelligence collection and disruption, neither of which requires any criminal predicate, are now equally important roles for FBI agents. The move away from the traditional requirement for a criminal predicate to justify law enforcement activity has potentially far reaching implications. Not only has this change prompted some concomitant changes laws and policies it also affects the application of laws that were already on the books. The full impact of these changes on the nation's ability to protect life, liberty, and our way of life may not be known for years.

A fundamental principle of our democracy is that law-abiding citizens should be able to go about their lives without fear of government detention or interference. Law enforcement authority was, by definition, to be used to enforce the laws. Interference by law enforcement was to be limited to those situations involving a violation of the law, usually criminal laws. Thus, we require crimes to be clearly defined so

that people can know when they are violating the law. Law enforcement may mistakenly target an innocent person, but such mistakes should be rare and the system should operate to detect those mistakes as promptly as possible.

When law enforcement officials start looking for "suspicious" activity rather than criminal activity, this clarity is lost. People are left to speculate about whether their activity might be viewed as suspicious. While it may still be unlikely that a law-abiding citizen will be convicted for terrorism, they may well come under heightened scrutiny. This can have several consequences. The mere prospect that the government may be watching is sufficient to deter some people from engaging in otherwise lawful activity, including protected activity like exercise of religion or free speech. Moreover, enhanced surveillance raises the prospect that the government will detect non-terrorism violations, such as failure to pay child support or problems with income taxes. Just as Al Capone was locked up for tax fraud, Attorney General John Ashcroft has said the government will go after suspected terrorists for "spitting on the sidewalk." Thus, violations that might not otherwise be detected or rise to a level warranting prosecution may result in liability because "suspicious" activity led to heightened scrutiny. While few would object to using whatever laws are applicable to lock up terrorists, this approach also places non-terrorists at greater risk of prosecution if they engage in behavior the government has labeled as "suspicious." Aside from its chilling effect, this can eventually impugn the perceived credibility and fairness of the system, undermining vital citizen support.

Law-abiding individuals may also be at greater risk of other kinds of government interference, short of criminal prosecution, because of the Bureau's increasing reliance on "disruption" techniques. The intelligence community has traditionally used disruption overseas when there is information indicating a possible attack but either inadequate information or insufficient capability to move directly against the terrorists. In those situation, intelligence officials, usually working with cooperative foreign governments, will generate activity designed primarily to intimidate the terrorists into delaying or canceling the attack. "Rounding up the usual suspects"—detaining members of the communities of which the terrorists are thought to be a part-- is a classic form of disruption. Authorities may get lucky and actually take into custody someone who is necessary for the attack but, at a minimum, they put the terrorists on notice that the government knows something is up. The Attorney General and FBI Director have made it clear that disruption is now part of the strategy inside the United States, raising issues not present in the overseas context. To some extent, at least, the large-scale detentions and questioning of immigrants after September 11 was part of a disruption campaign. Other kinds of government disruption that falls short of criminal prosecution might include IRS audits, denying permission to board an airplane, or extensive questioning or searches each time you try to board a plane. These activities do not require any criminal predicate for justification and often are not governed by the safeguards the system usually imposes to prevent abuses of government authority. Typically, the targeted individuals have little recourse to challenge the basis for the government action, unlike the protections built into the criminal justice system.

Concern about being caught up in anti-terrorism actions because you have engaged in "suspicious," rather than criminal, activity is heightened by technology designed to enhance the government's surveillance capability. Broad search capabilities designed to find terrorists based on a "profile" raise the greatest concern. These might include some proposals for data mining, as well as physical surveillance technologies such as facial recognition and gait analysis. Underlying this heightened concern is skepticism about the government's ability to create a profile that is sufficiently accurate to detect all terrorist activity and only terrorist activity. Instead, many fear that the profile will miss some terrorists and "catch" too many non-terrorists. Similar concerns underlie the controversy over technologies that would access databases of questionable accuracy in programs like CAPPS II. These concerns might be alleviated, then, if the public were assured of the accuracy and effectiveness of the data and the profile, and if the "cost" to non-terrorists of being mistakenly profiled were relatively low. A more accurate system for "profiling" terrorists, if one could be developed, might actually enhance civil liberties and

reduce the fear of unwarranted government interference by reducing the likelihood that law abiding individuals would be targeted.

Proposals for a national ID card also raise the prospect of heightened government surveillance. The idea of a card that can be a more reliable form of identification through the use of biometrics, for example, would address a number of security concerns. However, in order for the biometrics to be an identifier, presumably the government will have to have some way of matching the data. For example, if the biometric identifier were fingerprints or DNA, the government would need to have everyone's fingerprints or DNA on file in order to match the card with the name. This is personal information the government currently does not have for most Americans. Moreover, as more and more businesses, employers, locations, and others begin to require these ID cards, they will form records of our every action. These records will be susceptible to government access.

Many of the challenges to various surveillance and search techniques are based on the Fourth Amendment prohibition of unreasonable searches and seizures. However, evaluations of these techniques should also include consideration of their potential chilling affect on protected activity. In counterterrorism efforts, particularly, Fourth Amendment and First Amendment rights are often closely connected. As Supreme Court Justice Lewis Powell noted in a decision on electronic surveillance, "[n]ational security cases…often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Thought the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech."[69] This is particularly pronounced in investigations targeting politically or religiously motivated terrorism.

Possible Recommendations:

Efforts to detect possible terrorists living in our midst could more effectively preserve life, liberty, and the ability to pursue happiness if safeguards could be developed to maximize the fairness and effectiveness of the methods utilized.

For example, concerns about government surveillance and use of profiling might be alleviated by the development technologies and methodologies to maximize the effectiveness of terrorist "profiles" and strengthen the accuracy of data. Moreover, privacy concerns could be eased by ensuring that data remains "anonymous"--allowing computers to do "blind" matches so that no person has access to the names--until a court, magistrate, or other independent authority determines that the investigator has met an appropriate threshold for allowing names to be matched with data.

The costs of a "false positive" should also be reduced, perhaps by establishing mechanisms that would allow individuals to get off watch lists, developing more timely mechanisms for verifying information leading to a "hit", and placing limits on the type of action that can be taken on the basis of such a hit.

Accountability could be enhanced by using technology to build in rigorous audit controls to detect unauthorized activity such as improper storage of information on protected activity, or inappropriate searches of databases or uses of surveillance technology.[70]

[69] United States v. United States District Court (Keith), 407 U.S. 297 (1972).

[70] These kinds of safeguards might also be applicable to privacy concerns regarding health records. Developing appropriate mechanisms for preventing the abuse of access to health information might ease concerns about sharing that information with law enforcement or others who may need it to prevent or mitigate a bioterrorism attack, for example.

Law Enforcement and Intelligence

As FBI and local cops focus on prevention, it becomes harder to distinguish between law enforcement and intelligence. According to the revised Attorney General Guidelines issued in May, 2002, law enforcement activity includes activities related to counterterrorism and foreign intelligence. (*AG Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations*, Section VI(C).) FBI activity is defined as "law enforcement activity" even if it involves actions designed to collect intelligence rather than to investigate criminal activity.

Traditionally, as FBI Director Robert Meuller has told the Advisory Panel, criminal investigators brought a certain discipline to the collection and analysis of information because that information might eventually be evidence in a criminal prosecution. Law enforcement officers at the local, State, and Federal level knew that if information was not collected in a manner consistent with the Fourth Amendment, for example, it could not be used at trial. This served as a safeguard against the potential abuse of law enforcement powers. However, since prosecution is no longer the primary objective, this safeguard may no longer be effective. Indeed, it has been reported that many of those detained after September 11 were not read their *Miranda* rights or given access to counsel because the objective of the detention was to collect intelligence information rather than to use that information in a prosecution. Most were detained under the material witness statute and, while this is probably not unconstitutional[71], it is a different way of doing business for the FBI and it may be appropriate for Congress to consider whether new safeguards are needed.

Other investigative techniques have also been broadened to apply even when there is no indication of criminal activity. For example, online searches for information about individuals or groups prior to September 11 could not be conducted in the absence of some showing of possible criminal activity. Law enforcement actions that touched upon First Amendment activity, particularly the exercise of religion, were subject to particular scrutiny. Many agents in the field interpreted this policy as a virtual ban on such actions and important opportunities to detect terrorist recruitment efforts, for example, may have been lost.

The revised AG Guidelines authorize FBI agents to visit any place and attend any event that is open to the public, and conduct online search activity or access online sites and forums, on the same terms and conditions as members of the public generally, for the purpose of detecting or preventing terrorist activities. Section 411 broadly defines "terrorist activities" and again makes it clear that criminal activity is not required.

The most significant concern with allowing the monitoring of First Amendment activities such as exercise of religion and freedom of speech is that it will have a chilling effect. This concern is exacerbated if those doing the monitoring are allowed to keep files on individuals they observe.

The AG guidelines attempt to address this concern by stating that:

> The law enforcement activities authorized by this Part do not include maintaining files on individuals solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of any other rights secured by the

[71] Courts have upheld the use of the material witness statute in this context and the Supreme Court has recently held—though in a fractured opinion that left some questions open-- that coercive interrogation without criminal prosecution does not violate the Constitution, at least where the interrogation does not "shock the conscience." (Chavez v. Martinez, No. 01–1444, Decided May 27, 2003.)

> Constitution or laws of the United States. Rather, all such law enforcement activities must have a valid law enforcement purpose as described in this part.

This apparent safeguard is not as strong as it might at first appear. First, files could be maintained if they were for another purpose *in addition to* monitoring constitutionally protected activity. Moreover, the activities permitted must have a valid law enforcement purpose but, as discussed above, that term is now very broadly defined.

Possible Recommendation:

The potential chilling effect of broadened surveillance authority could also be reduced if, in addition to baring the collection or storage of information *solely* for monitoring protected activity, a more rigorous standard was imposed for any targeting that involved protected activity. The key would be to ensure that the higher threshold was not interpreted in the field as effectively a prohibition against such collection or storage, as happened in the past.[72]

Changes in FISA

The blurred distinction between law enforcement and intelligence has been most clearly evidenced in the application of the Foreign Intelligence Surveillance Act (FISA). Pursuant to FISA, FBI can apply for orders from the Foreign Intelligence Surveillance Court (FISC) authorizing electronic surveillance or physical searches where there is *probable cause* to believe that the target is a foreign power or an agent of a foreign power, as opposed to the traditional Title III wiretap authority used in criminal cases, which requires probable cause to believe the target is involved in criminal activity. Unlike surveillance or searches authorized under the criminal code, FISA activities can be undertaken without ever notifying the target.

The definition of a foreign power includes "a group engaged in international terrorism or in preparation therefore." "Agent of a foreign power" includes a non-US person who is a member of an international terrorism group or any person, including a US person, who knowingly engages in sabotage or international terrorism, or activities that are in preparation therefore, for or on behalf of a foreign power; or knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or knowingly aids and abets persons engaged in such activities.

Long interpreted by some elements of the intelligence community as applying only where the "primary purpose" of the surveillance was foreign intelligence rather than law enforcement, the statute was amended as part of the USA PATRIOT Act to allow its use when foreign intelligence was merely a "significant purpose." Subsequently, the Foreign Intelligence Court of Review concluded that there was never any constitutional requirement for distinguishing between a law enforcement and foreign intelligence purpose where the two overlap, as they do with regard to international terrorism. The court tore down the wall that had been erected over a period of 25 years between these two communities.

One immediate impact of this is to allow criminal investigators to receive information collected pursuant to FISA. However, it also allows those investigators to assist in identifying targets. For all practical purposes, FISA has now replaced the traditional criminal wiretap authority for all international terrorism investigations. Again, one significant impact of this change is to effectively remove the requirement for a criminal predicate for electronic surveillance of international terrorism suspects.

[72] Again, there are parallels in the health arena, where misunderstandings about the application of HIPPA have unnecessarily restricted information sharing.

In addition, the potential scope of the FISA authority may have been significantly expanded by other changes in the law. The statute prohibiting material support to terrorists, for example, was also broadened in the USA PATRIOT Act and is now being challenged in court as unconstitutionally vague and overbroad. If "material support" as broadly defined in that statute informs the FISA threshold that allows targeting of individuals who "knowingly aid and abet" individuals engaged in international terrorism, the scope of potential FISA targets has grown correspondingly. If constitutional challenges to the material support statute are upheld, they may call into question the legitimacy of the related FISA collection.

Possible Recommendation:

Congress should carefully monitor the application of FISA as amended, particularly in light of the decision of the Foreign Intelligence Court of Review and changes in other laws, to ensure that the powers authorized still meet constitutional requirements and do not chill legitimate activity.

Section 215 – Library Records

Another change to FISA contained in the USA PATRIOT Act that has been of particular concern to civil liberties advocates is the expanded authority to compel libraries, bookstores, schools, Internet service providers, retailers, and others to turn over information to the government. Section 215 of the PATRIOT Act amended FISA to give FBI the authority to seek an order from a FISA judge or magistrate requiring anyone served with such an order to turn over "any tangible things (including books, records papers, documents, and other items)." Prior to this amendment, this authority was limited to business records held by common carriers, hotels, storage facilities, or car rental companies. The provision as amended is not limited to businesses or business records but would apparently apply to tangible things held by any individual or entity. Its potential application to libraries and bookstores is what has prompted the greatest concern.

The amendment makes several other changes to the provision. The original provision required that the information was being sought pursuant to an FBI investigation and that there were "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." Neither of these requirements was carried over to the amended version. Applications seeking information on non-US persons need only be "to obtain foreign intelligence information."

However, if the information sought involves a US person, the amended provision can only be used if its purpose is to protect against international terrorism or clandestine intelligence activities (espionage) and only if it is not conducted *solely* upon the basis of activities protected by the First Amendment to the Constitution. Thus, a request to a library to turn over records indicating what books were checked out by a US person presumably would be justified if it were *related* to an international terrorism investigation—generally a fairly relaxed standard. Moreover, as with the AG Guidelines on maintaining files, the bar on inquiries based "solely" upon protected activity—without a more definitive requirement for showing a connection to terrorism—provides limited protection.

The records covered by Section 215 could have been sought prior to the USA PATRIOT Act by getting a subpoena from a grand jury. However, convening a grand jury requires a criminal predicate. Moreover, grand jury subpoenas would not necessarily enjoy the same level of secrecy imposed by Section 215.

Possible Recommendations:

As suggested above, concerns about the application of Section 215 might be alleviated if a higher threshold were imposed to collect information directly related to First Amendment activity, in addition to barring collection based solely on protected activity. For example, we know that some of the 9/11

highjackers used library computers prior to the attacks. If investigators pick up Internet activity that they reasonably believe is related to terrorism and can identify that it came from a computer in a library during a certain time period on a certain day, it makes sense to give them authority to find out who used the library's computers at that time. However, a significantly higher threshold, such as that required to monitor voice communications, should be required to give the government access to information on the content of that activity or what books someone checked out.

More fundamentally, having a separate domestic intelligence collection agency might allow the FBI to return to a context in which a criminal predicate is once again a pre-requisite for law enforcement activity. It could also provide a clearer context in which to evaluate and address concerns that relate specifically to the collection of intelligence inside the Unites States, separate and apart from the issues related to what actions the government can take based on that information. Clarifying the distinction between intelligence collection authority and law enforcement power could also clarify oversight responsibility.

Treatment of Immigrants

Because the terrorists involved in the attacks of September 11, like many of those involved in the first bombing of the World Trade Center, were non-citizens, terrorism prevention efforts have had a particular focus on the immigrant community. It is important to improve the nation's ability to know who has entered or is attempting to enter this country. However, because enforcement of our immigration laws and policies has been so lax for so many years, there is an "enforcement deficit" that invites potential discrimination, or at least the perception of discriminatory treatment. Moreover, the complexity of immigration requirements and delays in processing paperwork means many people are unwittingly or unavoidably out of status at any given time.

For example, in an effort to get a better understanding of foreigners already present in the country, the government has initiated a registration program. The numbers are too great to register all foreigners at once. Since the highjackers came from the Middle East and that is the ideological home of Al Qaeda, the decision was made to register visitors from those countries first. What has exacerbated concern over this disparate treatment is that a significant number of those showing up to register wound up being charged with immigration violations and, often, deported. As with the heightened scrutiny for suspicious activity described above, the immigration violations were only detected because of the registration requirement. Thus, young Arab men were more likely to be caught and deported because of the decision to require them, as opposed to young men from other countries, to register.

The opportunity to visit this country is a privilege rather than a right. Moreover, the ability of a country to control who enters and lives in their country is a fundamental sovereign right. Thus, countries have wide latitude in setting immigration policies. Once an individual has entered the country, however, more rights begin to attach. The Supreme Court has said that virtually all of the constitutional protections apply to immigrants who have "substantial contacts" with this country.

Moreover, as noted at the outset of this paper, because community relations can be an important element in preserving security, policies that pass constitutional muster may nevertheless have a negative impact on security if they undermine the sense that the system is fair and just. The objections of some in local law enforcement to suggestions that they should take a more active role in enforcing immigration laws, for example, reflect, in part, this concern about disrupting important community relations.

Possible Recommendations:

One possible way to evaluate the rights of immigrants is to distinguish between the fundamental rights accorded to all people—what the founders referred to as unalienable rights—and the whole panoply of specific rights that are granted by virtue of the social compact between a government and those it governs.

In the enemy combatants' situation, for example, you might conclude that all detainees have basic rights against arbitrary detention or torture. Thus, the government must explain the basis for their detention. However, non-citizen/resident detainees may not have a right to challenge their detention in US courts. That right could be viewed as deriving from the social compact and therefore only available to US citizens or permanent residents. This is consistent with the way the Supreme Court has generally viewed these issues.

As noted, however, security may actually be enhanced by adopting policies that are sensitive not just to the legal rights of immigrants but also to the impact of those policies on the immigrants' way of life, and thus on community relations. The "enforcement deficit" is difficult to address short of an overhaul of our immigration policies and enforcement resources. However, at a minimum, evaluations of the actions taken against immigrants as part of the effort to prevent another terrorist attack should include the security costs of infringing on immigrant liberties and way of life.

Conclusion

As Justice Louis Brandeis observed, "Those who won our independence believed that the final end of the state was to make men free to develop their faculties….They valued liberty both as an end and as a means. They believed liberty to be the secret of happiness and courage to be the secret of liberty."

If this nation can maintain the courage to preserve liberty in the face of terror, it will succeed in sustaining a long-term strategy that defeats the terrorists' objectives.

TAB—SUMMARY OF KEY PROVISIONS OF THE USA PATRIOT ACT OF 2001

TAB—SUMMARY OF KEY PROVISIONS OF USA PATRIOT ACT OF 2001

(Reprinted from the National Security Law Reporter of the American Bar Association Standing Committee on Law and National Security. Prepared by Dale Bosley, Stephen Kroll, Gordon Lederman, Joshua Levy, Michael Smith, and Suzanne Spaulding.)

Title I – Enhancing Domestic Security Against Terrorism

- Establishes a Counterterrorism Fund to reimburse DOJ for costs incurred in counterterrorism efforts.
- Authorizes $600 million over three years for the FBI's Technical Support Center.
- Sense of the Congress condemning discrimination against Arab and Muslim Americans.
- Directs Secret Service to develop a national network of electronic crime task forces.
- Provides for military support to law enforcement under certain emergency circumstances where required to enforce prohibition on use of chemical or biological weapons.
- Expands President's authority under IEPA to include any property subject to US jurisdiction, allow orders to block assets during an investigation, and provide for the confiscation of property of foreign persons, organizations, or countries determined to be involved in armed hostilities or attacks against the US.

Title II -- Enhanced Surveillance Procedures

- Seeks to significantly enhance the government's ability to collect, analyze and share intelligence information concerning international terrorism.
- Amends Title III of the Omnibus Crime Control and Safe Streets Act (18 U.S.C. 2501 et seq.) (Title III) to:
  -provide new criminal statute predicates that would support an application for a warrant;
  -permit seizure of voice mail pursuant to a warrant;
  -permit the results of surveillances to be shared with intelligence agencies, subject to Attorney General procedures if the information concerns a United States person; and
  -expand authority to intercept computer trespasser communications.
- Amends the Foreign Intelligence Surveillance Act (50 U.S.C. 1801 et seq.) (FISA) to:
  -enable surveillances to be implemented against targets who attempt to thwart surveillance, e.g., by switching phones, without going back to the Foreign Surveillance Court;
  -lengthen, in certain cases, the duration of initial surveillances and renewals;
  -broaden the use of pen registers and trap and trace devices "to protect against international terrorism or clandestine intelligence activities"; this authority may not be used against USP's solely on the basis of activities that are protected by the First Amendment. A similar change is made to the FISA provision that permits access to records and other items; and
  -permit surveillance under FISA when foreign intelligence is "a significant purpose" rather than "the purpose".
- Amends the Electronic Communications Privacy Act (18 U.S.C. 2701 et seq) to:
  -broaden the scope of subpoenas for records of electronic communications to cover internet sessions but not the content of those sessions;
  -permit emergency disclosure of electronic communications to protect life and limb; and
  -permit nationwide service of warrants for electronic surveillance.
- Modifies the Federal Rules of Criminal Procedure (FCRP) to:
  - permit delayed notification of the execution of a warrant when the warrant prohibits a seizure and disclosure may have an adverse result on the investigation ("sneak and peek"):
  -expand the scope of court orders for pen registers and trap and trace devices to collect information on internet sessions but not including the content of those sessions; and
  -give nationwide effect to search warrants issued in terrorism investigations.
- Enhances sharing of information between the intelligence and law enforcement communities through the change to Title III noted above and through a modification to Rule 6 (e) of FRCP to permit the passage of information obtained by a grand jury to any intelligence or national defense official provided it is "foreign intelligence information" (a defined term).
- Permits "aggrieved persons" to seek money damages in a civil action against the United States for improper disclosure of information obtained pursuant to FISA, ECPA and Title III.
- Contains a sunset provision (December 31, 2005) for most of the changes to FISA and certain changes to ECPA and Title III.

Title III - International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001

- Seeks to increase significantly the strength of U.S. measures to prevent, detect, and prosecute international money laundering and the financing of terrorism, and to facilitate dissemination of financial information to the intelligence community in connection with efforts to fight international terrorism.

- Amends the Bank Secrecy Act (12 U.S.C. 1951-59 and 1829b, 31 U.S.C. 5311-5332) in a number of ways, most importantly to:
  -give the Secretary of the Treasury, in consultation with other senior government officials, authority to impose one or more of five new "special" recordkeeping, reporting, and account restriction "measures" against foreign jurisdictions, financial institutions, transactions or types of accounts that the Secretary, after consultation with Secretary of State and the Attorney General, determines to be of a "primary money laundering concern" to the United States.
  -require a U.S. financial institution that maintains a correspondent account or private banking account for a non-United States person to establish appropriate, specific, and, where necessary, enhanced due diligence procedures that are reasonably designed to detect and report instances of money laundering.
  -mandate additional, more specific controls and monitoring for accounts opened by offshore banks or banks from countries with substandard money laundering controls and for private banking accounts, especially those potentially owned by foreign political figures.
  -bar any depository institution or registered broker-dealer operating in the United States from establishing, maintaining, administering, or managing a correspondent account in the United States for a foreign "shell" or "brass plate" bank, i.e., a bank that does not have "a physical presence in any country."
  -require foreign banks with U.S. accounts to appoint U.S. agents for service of process in connection with records relating to U.S. account transactions, and require the closing of any such account upon notice from the Department of Justice or Treasury that a subpoena served on such agent has not been either complied with or challenged.
  -require issuance within one year of regulations for uniform identity verification requirements for U.S. nationals opening financial institution accounts, and ask Treasury to recommend within six months similar requirements (and perhaps a uniform identification number system) for non-United States nationals opening such accounts.
  -require financial institutions in the U.S. to set up anti-money laundering programs.
  -require issuance by July 1, 2002, of regulations requiring reporting by securities broker-dealers of suspicious transactions.
  -clarify application of the Bank Secrecy Act to underground banking and money transmission systems.
- Amends Title 18 in a number of ways, most importantly to:
  -add a number of "specified unlawful activities," including corruption directed at foreign governments, support for designated terrorist organizations, and criminal export control violations, to the criminal money laundering statutes.
  -mandate a "law of the U.S." solution to disputes involving forfeitures of funds in interbank accounts.
  -make banks that do not operate in the U.S. subject to the extraterritorial jurisdiction provisions of the criminal money laundering statutes.
- Amends the purpose and disclosure provisions of the Bank Secrecy Act to include as a statutory purpose the preservation of records and dissemination of required reports "for use in the conduct of intelligence and counter-intelligence activities, including analysis, to protect against international terrorism."
- Amends the Right to Financial Privacy Act (12 U.S.C. 3401 et seq.)(the "RFPA"):
  - to permit records obtained pursuant to the RFPA's terms by one agency (e.g., a law enforcement agency) to be transferred to another agency if the records are relevant to an "intelligence or counterintelligence activity, investigation or analysis related to international terrorism," as well as to a law enforcement inquiry (as under existing law).
  -to extend existing special RFPA procedures for requesting records relevant to counter-intelligence or foreign-positive intelligence inquiries, and protective function inquiries, to requests from "a government authority authorized to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism" for the purpose thereof.
  -to permit records obtained by grand jury subpoena to be used for one of the purposes for which RFPA contains such special procedures.
- Amends the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) to require consumer reporting agencies to furnish information to "a government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism," upon receipt of an appropriate certification from that agency.
- Requires the Secretary of the Treasury to issue regulations, within 120 days of the date of enactment, to encourage cooperation among financial institutions, financial regulators and law enforcement officials, and to permit the sharing of information by law enforcement and regulatory authorities with such institutions regarding persons reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities.

- Allows (with notice to the Secretary of the Treasury) the sharing of information among banks involving possible terrorist or money laundering

Title IV – Protecting the Border

- For the Canadian border, triples INS-personnel, increases facilities supporting them, and improves monitoring technology.
- Requires DOJ to provide INS and State access to data on visa-applicants' criminal histories.
- Requires Attorney General and the Secretary of State to create identity-confirming technology for aliens, within two years.
- Requires the Attorney General to report to Congress on the feasibility of enhancing the fingerprinting system used for those aliens entering or exiting the U.S.
- Bars admission of aliens who endorsed or espoused terrorist activities, persuaded others to support terrorist activities or terrorist organizations, or are influential members of groups whose public endorsement of terrorism has undermined the U.S.-effort to fight terrorism.
- Broadens definition of "engaged in terrorist activity" to include providing material support or encouragement to groups that the individual knew or should have known were terrorist organizations.
- Mandates detention of aliens that the AG certifies as threats to national security, but must charge with criminal or immigration offenses within seven days, in which case detention may continue for six months unless found removable, in which case detention continues until removed or no longer a threat; allows limited judicial review in DC Circuit.
- Gives the Secretary of State discretion to share visa lookout database information and other records on aliens with reciprocating countries.
- Authorizes appropriations for AG's rapid and full implementation of integrated exit and entry data system for airports, seaports, and land ports of entry.
- Authorizes AG to collect information from flight schools, language schools, and other vocational schools on alien students in the same manner in which AG can collect information on alien students in higher educational institutions.
- Requires SecState to monitor checking of passports and issuing of consular visas.
- Creates special immigrant status for certain aliens, whose relatives have lived in the U.S. before September 11, 2001 and whose same relatives died as a result of a terrorist attack. Neither this status nor any other government benefit shall be conferred to relatives of the terrorists.

Title V – Removing Obstacles to Investigating Terrorism

- Authorizes the Attorney General, and broadens the Secretary of State's authority, to pay rewards to combat terrorism.
- Authorizes officials engaged in FISA surveillance to consult with Federal law enforcement officers to coordinate efforts to investigate or protect against specified threats from a foreign power or an agent of a foreign power, such as an actual or potential attack, sabotage or international terrorism, or clandestine intelligence activities.
- Gives the Secret Service concurrent authority with FBI to investigate cyber-terrorism crimes against government computers.
- Authorizes an Assistant Attorney General to obtain a court order for the purpose of collecting educational records that are relevant to the investigation or prosecution of a grave felony or terrorism.
- Allows FBI Deputy Assistant Director or higher (or Special Agent in Charge) to issue National Security Letters for telephone toll and transaction records, financial records, and consumer reports.

Title VI – Providing for Victims of Terrorism, Public Safety Officers, and Families

- Expedites government payments to beneficiaries of public safety workers who were catastrophically injured or killed in connection with the prevention, investigation, rescue, or recovery effort related to a terrorist attack.
- Increases death benefits for such workers' beneficiaries from $100,000 to $250,000.
- Enlarges the fund for victims of terrorist acts and their beneficiaries. Creates fund to compensate response to September 11, 2001 events.

Title VII – Increased Information Sharing for Critical Infrastructure Protection

- Authorizes $150 million over the next two years for DOJ to establish secure information sharing systems with state and local law enforcement entities to enhance investigation and prosecution of multi-jurisdictional terrorist conspiracies and activities.

Title VIII—Strengthening the Criminal Laws Against Terrorism

- Expands criminal sanctions to include possession of biological agents, toxins, or delivery systems for other than, or of a type or quantity not justified for, peaceful purposes.

- Adds special penalties for criminal possession of biological materials by “restricted persons” defined to include fugitives, illegal aliens, felons, and others.
- Expands definition of domestic terrorism to include “mass destruction” ands requires intent to intimidate or coerce civilian populace or to influence government policy or conduct.
- Adds a list of specified crimes to definition of ``federal crime of terrorism'' in 18 U.S.C. 2332b(g)(5)(B) (which already contains a requirement that the activity “is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct”).
- Adds terrorism crimes listed in 18 U.S.C. 2332b(g)(5)(B) as predicates under RICO.
- Makes it a crime to engage in terrorist attacks on mass transportation systems.
- Adds special penalties for harboring or concealing persons known or reasonably believed to be terrorists.
- Expands authority to go against all assets used to support, plan, conduct or conceal acts of domestic or international terrorism.
- Extends statute of limitations to bring indictments in noncapital terrorist offenses (8 years) and capital terrorist offenses (no time limit).
- Increases maximum penalties for terrorism offenses including “for any term of years or for life” in capital cases.
- Provides that parties to a conspiracy to commit certain terrorism offenses may be punished to the same extent as actual perpetrators.
- Defines threshold damages for acts of *cyberterrorism* as $5000, physical injury, threat to public health or safety, or damage of any kind to a government computer system used in administration of justice, national defense or national security.
- Authorizes $50 million annually to enable the Attorney General to establish regional computer forensic laboratories to assist in defense against cyberterrorism.

Title IX – Improved Intelligence

- Gives DCI explicit authority to establish requirements and priorities for foreign intelligence (FI) collection under FISA and work with the AG to ensure dissemination.
- Requires AG, in consultation with DCI, to develop guidelines to ensure (1) prompt disclosure to the DCI of FI acquired during a criminal investigation and (2) timely notice to DCI of decision whether to commence a criminal investigation based on information provided by the DCI to DOJ regarding possible criminal activity by a current or potential FI source.
- Directs AG and DCI to develop a program to train appropriate federal, state, and local officials to identify FI that may be encountered in the course of their official duties.
- Requires a report from the AG, DCI, and Secretary of Treasury on feasibility and desirability of reconfiguring current foreign asset tracking and control entities so as to improve analysis and dissemination of FI related to terrorist financing.
- Requires a report on the establishment of a virtual translation center within the intelligence community.
- Expresses Sense of Congress encouraging intelligence relationships with terrorists.

Title X—Miscellaneous

- Requires the DOJ Inspector General to designate an official to receive complaints alleging abuses of civil rights and liberties by DOJ employees and submit reports to Congress.
- Defines ``electronic surveillance'' in FISA to exclude the acquisition of computer trespassers' communications.
- Endeavors to enhance states and local governments' ability to respond to and prevent terrorism through various DOJ grant programs.
- Requires FBI to report to Congress on feasibility of providing airlines with names of passengers who are suspected to be terrorists.
- Enhances statutes making it unlawful to fraudulently solicit charitable contributions.
- Requires determination by Transportation Secretary that licensee poses no security risk before states can issue licenses to transport hazardous materials.
- Establishes National Infrastructure Simulation and Analysis Center in DOD to protect United States' critical infrastructure from terrorist attacks.

APPENDIX F–BURDEN SHARING*

Background

For a number of years the Federal government has been concerned with the ability of states and localities to adequately deal with terrorist incidents involving chemical, biological, and radiological weapons. This concern over weapons of mass destruction (WMD) prompted the U.S. Congress and the President in 1998 to establish the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (the "Gilmore Commission").[73] One of the Gilmore Commission's specific charges is to "assess Federal agency efforts to enhance domestic preparedness for incidents involving weapons of mass destruction."

Grant programs are frequently used as Federal tools for improving State and local response capabilities for WMD incidents. Some programs target specific local-responder groups (e.g., law enforcement, emergency medical services, public health agencies) or specific categories of need (e.g., equipment, training, overtime). Other programs fund activities that span multiple areas. Regardless of their scope, grant programs provide State and local jurisdictions with tangible incentives and assistance to undertake actions to increase preparedness.

But Federal grant programs can be structured in various ways. For example, some programs use competitive project grants, where applicants compete against one another for funding, while others use formula grants, where agencies allocate predetermined amounts of funding to jurisdictions. Some grant programs require matching funds while others do not. And some grant programs distribute money directly to localities while others pass funding to localities through the states. How these Federal programs are structured, or alternatively how these programs share responsibilities between Federal, State, and local authorities, can affect how successful they are at achieving Federal goals for national WMD preparedness.

Objectives

In support of the Gilmore Commission's work, this paper provides a cursory examination of issues involving burden sharing between the Federal, State, and local governments for WMD preparedness. This research draws on the theoretical literature in economics and political science, the applied literature in public policy, and on interviews conducted with Federal and State program administrators. The paper attempts to inform the following question: If the Federal government provides financial grants to states and localities to enhance specific aspects of local-responder capabilities, how might elements of the program's design support or hinder the Federal government's efforts?[74]

Specifically, we looked at the three major elements that vary across Federal grant programs generally. These include:

- the flow of funds from the Federal government to local responders (i.e., whether or not funds pass through the States);
- how funds are allocated (i.e., through formula grants or project grants); and

[73] Established in section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105-261.

[74] This report defines local responders broadly as law enforcement, firefighters, emergency medical services, emergency management operations, hospitals, and public health agencies. However, the report only considers grant programs for local responders generically. That is, it does not address differences in the ways that different local-responder communities have traditionally been funded.

*** Justin Adams, Ph.D.**

- the requirements for State or local funding funds, particularly State and local matching funds and maintenance of effort;

And we examined the main ways in which they affect achievement of Federal goals for WMD preparedness:

- the level and/or quality of preparedness activities provided by local-responder jurisdictions;
- the strength of coordination across the different levels of government;
- the geographic distribution of funds across local-responder jurisdictions;
- the administration of the program;
- and, innovation in States and localities.

Insights gained from this research can help the Federal government design more efficient and effective local-responder grant programs. Given the disparity between the funding available for improving WMD response capabilities and the nationwide need, this is particularly important. The Council on Foreign Relations (2003), for example, estimates that the U.S. will fall approximately $98.4 billion short of meeting critical emergency responder needs under current Federal, State, and local funding levels. Consequently, it is imperative that the Federal government stretches every dollar for local responders to the greatest extent possible.

Review Of Studies

There are a number of reasons why the Federal government might be motivated to provide funds to local responders for WMD preparedness rather than rely solely on State and local efforts:[75] The Federal government has access to a wider range of revenue sources; as Zycher (2003) points out, the Federal government has relatively greater taxing power over businesses and individuals than the States and localities and it can borrow money to finance consumption rather than investment. The Federal government can help facilitate preparedness for and responses to terrorist incidents with adverse impacts that spill across neighboring communities and neighboring States. Additionally, the Federal government might have a greater interest in ensuring equal levels of preparedness (or instead minimal levels) across the country. And, the Federal government might want to regulate State or local preparedness efforts; Federal funds provide it a substantial amount of leverage over recipients.

In light of these possible motives for Federal funding, this report addresses the question of how the structure of grant programs might support Federal efforts to enhance WMD preparedness. That is, it examines the design elements of Federal programs for local responders and the mechanisms by which they impact local preparedness.

With respect to design elements, we examined the three major elements that vary across Federal grant programs:[76]

- ***Flow of Federal funds.*** Program funds can flow directly from the Federal government to local jurisdictions. In this case the Federal government maintains responsibility for selecting recipients and allocating funds. Alternatively, program funds can flow first to State governments who then pass this money through to local jurisdictions. Here, States have the

[75] There are also reasons why the Federal government might not rely solely on the private sector to provide sufficient levels of WMD preparedness nationwide. WMD preparedness activities are collective goods, meaning that their benefits go to society as a whole rather than to particular individuals. As such, these preparedness activities are likely to be underprovided by the free market relative to an economically efficient level, since individuals are less likely to pay for activities that provide benefits from which they cannot be excluded. And one way of mitigating these problems is through Federal subsidies. For a more complete discussion see Zycher (1993).

[76] Other related analyses have looked at these elements as well. See Canada (July 8, 2003), for example.

responsibility for selecting recipients and allocating funds subject to Federal guidelines.

- ***Allocation of Federal funds.*** Program funds can be allocated to local responders through competitive project grants or instead allocated on the basis of formulas. Under programs with competitive grants, eligible local responders apply to a Federal agency for funds, and money is awarded on the strength of their applications. Under programs with formula grants, the responsible Federal or State agency allocates funding based on factors such as population or need (however need is defined); formulas could be specified in statute or determined by the appropriate agency.

- ***Requirements for State or local funding.*** As a condition of receiving funds, Federal programs sometimes require that State or local jurisdictions spend some amount of their own money on the desired activity. One type of requirement is for State or local matching funds, which are predetermined recipient contributions. A fire department that uses Federal funds to purchase equipment, for example, might be required to match 30 percent of the Federal award. A second type of requirement is for State or local maintenance of effort, which requires that recipients maintain a specified level of State or local expenditure as a condition of a grant award. In cases where Federal programs provide funding to help recipient jurisdictions augment their existing and locally funded activities, maintenance-of-effort requirements prevent recipients from simply supplanting local funds with Federal funds.

Federal efforts at enhancing WMD preparedness are broad and wide-ranging. They include facilitating the purchase of equipment for local responders, providing resources for education and training, fostering improved communication between local-responder communities, and assisting State and local planning efforts. In this report, we considered five general goals that Federal programs might focus on to enhance WMD preparedness:

- ***Enhancing the level and/or quality of preparedness activities by local responders.*** Federal programs might have the goal of enhancing the WMD preparedness activities of State and local governments by providing them with new or additional resources. Programs then can utilize design elements to ensure that States and localities employ these resources to increase the amount or types of preparedness activities undertaken, or improve the quality of their activities. For example, if the Federal government is interested in getting local governments to do more of a locally funded activity, it could incorporate a maintenance-of-effort requirement that prohibits the redirection of funds.

- ***Strengthening coordination across different levels of government.*** Given the multitude of local-responder communities and the central planning capabilities of the States and the Federal government, the Federal government might want to improve WMD preparedness by strengthening the degree of coordination across levels of government. In this case, the Federal government can structure a particular grant program to encourage or require coordination and cooperation by recipients. For example, a program could have funds flow through the States rather than directly to localities to ensure that local efforts are consistent with statewide needs.

- ***Improving the geographic distribution of funds across local-responder jurisdictions.*** Depending on its intended purpose, a Federal program targets one or more local-responder groups to help them address some need, such as building the capability to handle a specific threat. The Federal government then could have a goal of improving the distribution of funds by better targeting relevant jurisdictions. For example, if the Federal government wanted to provide a base level of funding to all communities with a particular need, the grant program could employ a formula to allocate funding appropriately.

- ***Improving the administration of Federal grant programs.*** The Federal government might have as a goal improving WMD preparedness by ensuring that Federal grant programs are administered effectively and efficiently. Federal officials, for example, may desire to have local jurisdictions receive funds as quickly as possible. They may also want assurances that programs are managed well, with a minimum of administrative costs and where localities spend funding only on eligible activities that are part of a coherent plan.

- ***Encouraging innovation in States and localities.*** Because local-responder communities are closer to WMD threats and in many cases know their own needs better than the Federal and State governments, the Federal government might have as a goal to increase the flexibility and innovation of local jurisdictions. As such, the Federal government could design Federal programs to limit restrictions on the acceptable uses of funds, for example by utilizing block grants.

This discussion of possible Federal preparedness goals is not to suggest that this set of goals is exhaustive. There could be others, although the five listed appear to be the most relevant for enhancing State and local WMD preparedness efforts. Nor is this discussion to suggest that Federal programs support preparedness efforts in each of the five ways. Some of these goals conflict might with one another; a program that encourages strong coordination between the States and localities, for example, could limit local flexibility and innovation. But this list of ways that Federal goals could *potentially* influence State and local behavior conveniently frames the discussion for the reviews of studies on intergovernmental aid and the three Federal programs that follow.

Enhancing The Level And Quality Of Local Efforts

Discerning the impact of program design elements (i.e., the flow of funds, the allocation of funds, and State and local funding requirements) on the ability of the Federal government to help enhance the level and/or quality of local-responder preparedness efforts requires the examination of two issues. The first is whether the Federal government can influence State and local jurisdictions in a meaningful way so that they take action to enhance their response capabilities. That is, do Federal local-responder programs designed to achieve specific objectives actually serve as inducements for these communities to undertake activities that they may not have otherwise? The second is the magnitude of this impact on State and local behavior and how it changes over time. These issues are addressed in turn.

Incentives for Higher State and Local Spending

Unlike legislative mandates that require specific behavior by States and localities, Federal grants simply provide incentives to communities and expand their resources. Certainly it is true that States and locals must undertake specified actions on the condition of accepting Federal money. But they could decide not to participate in these programs, and recipients always retain the ability to opt out of Federal programs should they choose to do so. Given that Federal grants serve only as inducements, it is conceivable then that Federal influence over State and local actions could be minor, especially when Federal funding levels are low.

Anecdotal evidence suggests that the Federal government is in fact able to exert sizeable influence over States and localities, however. And some studies on State and local responses to Federal spending generally support this notion as well. Welch and Thompson (1980), for example, examined 57 State public policies to see how Federal incentives impacted the spread of new policies across the States. Specifically, they analyzed whether State public policies that were exposed to "positive" Federal incentives (i.e., the provision of funding) or "negative" Federal incentives (i.e., the threat of depriving States of existing funding) hastened their adoption in all 50 States. They found that Federal incentives

stimulate policy diffusion significantly regardless of the policy area, and that direct fiscal aid stimulates causes more States to adopt policies earlier.[77]

Hofferbert and Urice (1985) examined Federal funding for the arts. They showed how the creation of the National Endowment for the Arts (NEA) in 1965, and its subsequent formula and competitive grants to the States, spurred State spending on the arts: In 1967, the States other than New York appropriated a combined $505,000 to their respective arts agencies, but by 1974 this figure (including New York) totaled $33 million and by 1980 it reached $96 million. This nationwide investment came despite the fact that the arts represented only a minor policy area with a small constituency.

Nathan and Doolittle (1985) studied the growth and decline in Federal aid from the 1960s to the early 1980s. They found that as Federal aid to the States and locals was cut under President Reagan, local jurisdictions were generally much less likely than the States to replace these programs with local ones. Although local jurisdictions occasionally lobbied the States to create replacement programs, this nevertheless suggests that outside funding can cause localities to undertake activities that they would not otherwise.

These studies suggest that Federal local-responder programs can affect State and local decisions, but an important issue is the magnitude of this impact over time. Public choice theory suggests that the impact of Federal programs on State and local behavior could be small: Communities can provide different levels of public services, and voters have some choice over the community in which to reside and the level of public services provided by their community, so one would expect that over time the public programs provided by a locality would coincide with local preferences for those programs. If this is the case, Federal grants (in particular unrestricted lump-sum grants) might have little impact on States and localities; local officials, following the desires of their taxpaying constituents, could return a similar amount of non-Federal revenue back to them.[78]

In contrast with this theory, a substantial literature on intergovernmental grants shows that Federal aid has significant and large stimulative effects on local spending (see Gramlich, 1977). These effects occur whether the Federal funding comes as categorical grants or instead as unrestricted lump-sum grants. For unrestricted lump-sum grants in particular, the stimulative effects are often referred to as 'flypaper effects', meaning that money seems to stick to wherever it hits. Studies by Logan (1986), Aronson and Munley (1994), and Hines and Thaler (1995), all attempted to explain away the empirical findings of higher State and local spending as an artifact, but they were unable to do so.

Stein (1984) found that flypaper effects exist not just with respect to local spending, but also with respect to municipal public employment. He found that municipalities take a "wait and see" approach with Federal aid, where cities initially resist hiring new employees because they see this assistance as temporary and because it is typically difficult to eliminate government positions once they have been filled. Over time, however, municipalities eventually give in as they begin to consider Federal aid as a permanent source of revenue.

Thus, the literature indicates that Federal grant programs can stimulate State and local spending significantly, and that this is the case even when Federal funding has no restrictions. This suggests that if the Federal government added restrictions to its grant programs such as State and local matching requirements, maintenance-of-effort requirements, and categorical grants, it could stimulate State and local behavior even further. Matching requirements and maintenance-of-effort requirements would help

[77] However, they also found that the speed of diffusion still remains lengthy. Federally affected policies took an average of 13.7 years to diffuse across 50% of the States and 29.7 years to diffuse across 100 percent of the States. For policies not impacted by Federal incentives, the averages were 23.5 years and 50.1 years, respectively. It should be noted, however, that Welch and Thomson's dataset encompassed policies that dated only to the 1970s.

[78] This assumes, of course, that local bureaucrats do not have their own individual motivations, such as to maximize local agency expenditures regardless of whether the money is Federal or non-Federal.

ensure that the States and localities maintain at least some minimum level of contributions, and categorical grants would tend to limit the ability of States and localities to redirect funds.

However, there is a potential downside to the stimulative effects of Federal programs. State and local jurisdictions can become dependent on Federal aid while at the same time having no control over it. So when grants for activities terminate, States and localities are faced with having to cut services or assume local responsibility for these programs. Levine and Posner (1981) also point out that during revenue downturns, States and localities are more likely to cut or eliminate entirely local programs in order to maintain matching funds in the federally subsidized programs. As a result, this dependence could skew the portfolio of services provided at the State and local level. Thus, locally-supported responder programs not subsidized by the Federal government might be cut over time, and the portfolio of preparedness programs could be distorted and overall preparedness could even be adversely impacted.

Supplanting State and Local Funding

An issue opposite to that of flypaper effects is supplantation. Supplantation occurs when the States and localities use new Federal money simply to replace their own funding for existing activities, thereby freeing up State and local funds for other things including tax reduction. Supplantation is particularly relevant when a Federal program comes in the form of a block grant, where recipients receive large amounts of funding that have few restrictions as to their use. So two natural questions are how much supplantation typically occurs with Federal programs, and how can Federal programs be structured to mitigate it?

Ellwood and Boyd (2000) saw relatively little evidence of supplantation from their investigation of the Temporary Assistance to Needy Families (TANF) program in the aftermath of welfare reform. In looking at whether the States in their study (California, Georgia, Missouri, and Wisconsin) spent more Federal money and less State money on social services than they did prior to welfare reform, Ellwood and Boyd generally found that this was not the case although they did find some instances of supplantation in specific areas.

The GAO (1996, 2003) noted in their reports on Federal grants and homeland security that, with respect to the studies they examined, every additional Federal grant dollar resulted in about 60 cents of supplantation on average. In other words every Federal dollar generated only about 40 cents more in combined (Federal, State and local) spending. This finding was especially true with respect to block grants received by public programs with prior State and local involvement.

The GAO discussed how a number of program characteristics could help to mitigate supplantation. It noted that restrictive Federal programs such as categorical grants could limit the ability to redirect funds relative to unrestrictive programs such as block grants, since recipients could only supplant funds within the specific category. Second, it pointed out that providing Federal matching funds also helps maintain State and local spending, because in these cases Federal funds act to effectively reduce the price of an activity to the citizens of the States and thereby encourage States and localities to "purchase" more of it; here Federal matches could be capped at a specified total dollar amount or instead remain open ended. And it noted that maintenance-of-effort requirements could help to maintain State and local spending. But with respect to homeland security, the GAO asserted that maintenance-of-effort requirements could potentially penalize the communities that took the initiative after September 11, 2001 to increase their own preparedness spending; these communities would be required to maintain a higher level of spending than communities that did nothing.

Over the longer term, an issue is whether State and local spending for preparedness can be sustained. Generally, sustainment refers to whether the States and localities take "ownership" of programs so that they do not terminate if Federal funding ends. To address this, the GAO (2003) and Posner (The Nelson A. Rockefeller Institute of Government, 2003) raised the possibility of a Federal "seed money" approach.

Here, the Federal government would encourage sustained State and local spending by offering an initial Federal match and lowering the match over time. This would allow State and local governments to gradually adjust their budgets over time to accommodate spending on preparedness activities.

Improving Coordination Among Levels of Government

Many describe local communities as being on the front lines for responding to terrorist incidents involving WMD. At the same time, the Federal government has significant resources, and both the Federal and State governments have substantial central planning capabilities. Consequently, many studies on homeland security conclude that strong coordination and collaboration between Federal, State, and local governments are needed.

Some studies advocate that the States play a key role in resolving the needs of local jurisdictions with the desires of the Federal government. Kettl (The Nelson A. Rockefeller Institute of Government, 2003), for example, argued that coordination of local-responder efforts is unlikely to happen on its own, and that State governments could promote and nurture this coordination. Given that the types of problems faced vary from State to State as well as the responses needed, he argued that coordination at the State level would be preferable to coordination by the Federal government. Accordingly, he concluded that intergovernmental aid for homeland security should come in the form of Federal block grants to the States, where the Federal government sets minimum national standards for preparedness and the States have wide discretion to allocate funding to local governments.

One way to strengthen intergovernmental coordination and cooperation is to require that funding from Federal grant programs flow through the States to the localities. The Gilmore Commission in its third report (2001) and again in its fourth report (2002) recommended that all Federal funding and grant programs be coordinated through the States. It asserted that scarce Federal money that is used to improve local capabilities should be used to complement State plans and requirements and, importantly, should be subject to a level of prioritization that the States can provide.

However, passing Federal funds through the States can potentially have some negative consequences for WMD preparedness. Delegating Federal responsibility for the allocation of funding to the States could result in the States choosing recipients that are more consistent with State prerogatives than Federal goals. It could also result in funding being disbursed to local jurisdictions in a less than timely fashion or being withheld entirely. To help mitigate these consequences, the Gilmore Commission (2002) concluded that as a general rule of thumb, States should not withhold more than 25 percent of Federal funds that are intended to improve State and/or local response capabilities. The Commission also concluded that activities where funding is available for joint State and local efforts, the States should withhold no more funding than the percentage of State effort.

The U.S. Conference of Mayors (2003) argued against passing Federal funds through the States for similar reasons. It asserted that States traditionally (and mistakenly) viewed counties as the focal points of emergency and disaster response rather than cities. Moreover, it asserted that States receiving Federal pass-through funds would dilute and delay funding intended for local responders.

But it should be noted that the flow of funding is not the only mechanism by which the Federal government can facilitate increased coordination and cooperation. The Federal government could, for example, allocate funds to localities itself but mandate that the States and localities engage in particular behavior such as having States sign off on local projects. Or the Federal government could develop standards to promote cooperation. As Thomas (1979) pointed out, coordination describes both a process and a goal. It requires that the various participants develop a consensus over the objectives to be obtained and the means to use.

Improving the Geographic Distribution of Funds

The next issue pertains to whether a Federal program can be structured so that it better targets local jurisdictions in need, however need is determined by the program.[79] That is, can program design elements improve the ability of Federal funding to make its way to the local-responder communities that need it most to better stretch scarce Federal dollars?

There are two approaches to answering this question. The first examines the responsiveness of the Federal government in trying to allocate funding to where the need exists (supply side of Federal programs). The second examines whether needy communities seek out Federal funding (demand side of Federal programs).

Pushing Funding to Needy Communities

Depending on the specific WMD preparedness goals the Federal government is trying to achieve, it might want to selectively target communities in need. Such programs might draw on the Federal government's private information or on its unique analytical skills (e.g., threat assessments) to push money where it is needed the most.

One issue in pushing funding to needy communities is that determining a community's actual "need" in the face of a given threat can be difficult. There are often a number of possible objective and subjective metrics that Federal agencies can use to measure a community's level of preparedness. For example, in the context of prioritizing funds for WMD preparedness in urban areas, a community's need could be measured by its population, its population density, its number of special sites, its economic importance, or by other metrics. Using one metric (or more) over another could result in a different ranking of need, and determining which metric(s) is most appropriate to use for a given threat is not always straightforward. This remains problematic whether an agency is devising a funding formula for a program or instead deciding how to rank applications for competitively funded awards.

Once communities have been ranked according to some measure of need, a second issue that emerges is whether funds actually get allocated to the communities with the greatest needs or are spread more broadly. Political pressures can influence which jurisdictions receive funding under formula allocations, whether the formulas are determined by agencies or are specified in statute, so that some less needy communities obtain funding. Similarly, communities with lesser needs can attempt to lobby agencies over the awarding of competitive grants.

The studies reviewed show a decidedly mixed picture with respect to the Federal government's ability to design programs that effectively allocate funding according to need. In other words, these studies tend to show weak correlations between the jurisdictions that needed funding under programs and the jurisdictions that got it. Importantly, even in instances where the Federal government appeared responsive to local needs, the States appeared to be more responsive. This might suggest a benefit from having Federal funds flow through the States. However, it should be stressed that in these studies researchers often developed their own ways in which to measure need. So conclusions about the effectiveness of Federal programs are in essence statements of how well these programs measured up against researchers' estimates of need.

In one study, Dye and Hurley (1978) examined total Federal outlays (primarily for housing, economic opportunity, and health, education and welfare) during the late 1960s and early 1970s to 243 central cities

[79] Depending on the grant program, need could be defined narrowly or broadly. A program to enhance port security, for example, might define needy communities as only those coastal jurisdictions immediately adjacent to water, resulting in a limited set of eligible applicants. On the other hand, a firefighter preparedness program might encompass all jurisdictions with paid or volunteer firefighters and result in a far larger set of eligible applicants.

with populations of at least 50,000. They found that differences in city demographic measures could explain only about 15 to 22 percent of the variation in Federal per capita funding to these cities, so they concluded that Federal outlays were generally unrelated to urban needs and resources. In comparing Federal grants-in-aid to State grants-in-aid for these same cities, they found higher correlations between State funding and city demographic measures, and thus concluded that State grants-in-aid generally were more responsive than Federal grants-in-aid to the needs of the cities.[80]

Dye and Hurley's study was criticized on methodological grounds, particularly because they used per capita funding figures rather than total allocations; some argued that using per capita figures is inappropriate because legislators do not make decisions over funding allocations in this way. Pelissero (1984) attempted to test some of Dye and Hurley's conclusions taking these critiques into account. Pelissero analyzed the total intergovernmental funding from the States to the 47 largest cities (with 1970 populations of at least 300,000) for the years 1962 and 1976 after controlling for city population. He still found consistent correlations between State aid and common city demographic measures, and concluded that States were responsive to the needs of cities.

In the area of education, Pelissero and Morgan (1992) examined 1982 data for over 13,500 independent school districts to determine whether the Federal or State governments were better at targeting aid to local schools with social, economic, or fiscal hardships. Pelissero and Morgan saw little evidence that either the Federal or State government targets school aid according to socioeconomic need, finding little correlation between aid and demographic measures of need. They instead found some evidence that intergovernmental aid is driven mostly by enrollment, particularly at the State level.

And in the area of homeland security, the GAO (October 2, 1998; November 1998) commented on the inefficiencies in the Nunn-Lugar-Domenici Domestic Preparedness Program that resulted from poorly specified Federal funding formulas. The Domestic Preparedness Program was intended to enhance domestic response capabilities for incidents involving WMD, and the Department of Defense (DoD) as the lead agency chose to allocate funding to cities based on core city populations. Because the DoD used population measures rather than assessments of city preparedness, financial ability, and threats, the GAO concluded that the DoD was potentially wasting program funds by insufficiently tying funding to local needs. For example, it could be replicating training in nearby cities that might be part of the same response system or mutual aid area, or providing assistance to communities with a smaller threat risk over those with a larger threat risk.

Although this last example illustrated a problem with funding formulas, it is not to suggest that using competitive grants is necessarily better at targeting communities in need. Just as a Federal (or possibly State) agency would have to define a specific formula under a formula funding program, it would have to define specific eligibility and application criteria under a competitive grant program. Thus inefficiencies could arise under either setting.

Encouraging Communities to Apply for Funding

The general literature on intergovernmental aid suggests that Federal assistance does not just find its way to communities in need. Instead, localities typically must demonstrate both entrepreneurial spirit as well as a strong capacity for planning in order to obtain Federal aid. These can be beneficial qualities for local jurisdictions to have, since they help to ensure that grant awards are used effectively.

Saltzstein (1977) studied whether differences in the amounts of financial aid received by cities are best explained by social and economic need or by the attitudes and practices of local decision makers. He

[80] The State funding they examined typically included Federal funding that passed through the States that could affect the level of State responsiveness, but they also noted that this should not necessarily make the State more responsive than Federal direct grants.

analyzed Federal assistance from the Department of Housing and Urban Development (HUD) and the Law Enforcement Assistance Administration (LEAA) to cities in Texas with populations from 50,000 to 300,000 and a council-manager form of government between 1971 and 1973 (20 cities). He found no support for the notion that communities with more social and economic need received more funding, but he did find that funding by the LEAA was highly correlated with the effort exerted by the city manager to receive funds.

Stein (1979) analyzed the factors that drive communities to apply for Federal grants. Looking at 145 communities in southeastern Wisconsin, he found that communities with clear need and significant planning resources tended to seek Federal assistance, but that communities with low levels of fiscal capacity and little support for planning activities tend not to apply, despite the fact that they are often the intended beneficiaries of the Federal programs. He concluded that, given the importance of the application process, Federal attempts to correct inequities in the allocation of Federal funds should focus on areas like administrative technical assistance to communities rather than on altering funding formulas.

Rich (1989) studied six Federal programs on community and economic development to determine to what extent political influence, community needs, and local demand and administrative capacity affected the distribution of Federal grants. In the presence of significant political and community effects over time, he found that local demand for Federal aid and the extent of participation in prior project grant programs were important factors in the allocation of funding.

Rich's study provides additional insights because the six Federal programs he studied involved both formula and project grants, sometimes managed by the same agency. He found that programs with formula grants tended to yield wide, almost universalistic geographic coverage (although not necessarily with equal per capita allocations). On the other hand, programs with project grants had a more limited distribution that was sometimes influenced by political factors such as maintaining the support of key legislators. He also found that while formula grant programs tended to provide funding to more jurisdictions with little or no need than categorical grant programs, administrators still managed to direct money in both types of programs toward the neediest communities.

Not mentioned by these studies is the fact that the Federal government can entice local communities to apply for funds by using tools such as Federal matching funds or online application and grant management processes. By providing Federal matching funds for State or local spending on particular activities, the Federal government effectively reduces the price the State or locality faces for the activities, so undertaking the activities becomes more attractive. By using online application and grant management processes, the Federal government can make it easier for jurisdictions to apply for funds and for recipients to administer them. But these tools are only inducements; they do not obligate State or local participation in Federal programs.

Together, these studies on the geographic distribution of Federal grants raise the issue of whether formula funding or a competitive grant better targets communities in need. They suggest that if the Federal government intends to distribute funds widely under a specific WMD preparedness program, perhaps to spur State and local spending on a new activity, a formula allocation might be more beneficial. Rich (1989) in particular showed that formulas allocations tend to be more universalistic than competitive grant allocations. A competitive grant, on the other hand, might be more consistent with a narrow WMD preparedness program.

These studies also demonstrate that how need is defined (e.g., population, threats, fiscal capacity) matters importantly with respect to which communities receive funding. This fact was particularly evident in the GAO critique of the funding formula used in the Nunn-Lugar-Domenici program. However, the definition of need also matters with respect to competitive grant programs, since need is often used to determine the pool of eligible applicants. A significant problem is that the most appropriate measure for a given program is not always clear. And, as suggested in the studies by Dye and Hurley (1978), Pelissero

(1984), and Pelissero and Morgan (1992), targeting funds exclusively to the neediest communities might still be difficult.

Improving Program Management

The Federal government might have as a goal improving WMD preparedness by ensuring that Federal grant programs are well administered. This could involve concern over a number of areas, including whether local-responder funds reach their recipients in a timely fashion; how well compliance with program requirements is monitored and regulated; and how political influences affect program operation over time.

Timely Allocation of Funds

With respect to Federal funds flowing through the States, the U.S. Conference of Mayors (2003) issued a report presenting the results of a survey on the status of ten Federal grants for homeland security for FY 2003. In the report, many of the responding 168 cities complained that their parent States often failed to disburse pass-through funds on time (sometimes in violation of statutory deadlines). States also often failed to notify cities in a timely manner if they would be receiving funds, and failed to consult them in the use of funds.

As mentioned earlier, the Gilmore Commission (2002) recommended some steps to help mitigate these consequences. It advocated that States not withhold more than 25 percent of Federal funds that are intended to improve State and/or local response capabilities, and that the States should withhold no more funding than their percentage of joint State and local efforts.

Regulating and Monitoring Compliance

Another issue is how well the Federal government does at regulating and monitoring program compliance by grant recipients. The Federal government must ensure, for example, that grant recipients expend funds only on eligible activities, and that they comply with State and local funding requirements, if any. More importantly, though, if a Federal program passes funds through the States, the States then assume some level of responsibility for regulation and enforcement as well. So an interesting question is, what happens when some responsibility for regulation or enforcement is devolved to State or even local authorities?

The literature surveyed indicates that Federal and State regulators become subject to pressures from all political levels. Wood (1992), for example, analyzed enforcement of the Clean Air Act by the Environmental Protection Agency (EPA) and the 50 States from 1977 to 1985. He found that the top tier of environmental oversight, the EPA, was influenced mostly by national policymakers (e.g., the President, the Congress). On the other hand the lower tier of enforcement, the States, was subjected to a wider range of influences from the Federal level (i.e., the EPA) as well as the State level (e.g., governor, legislature).

Hedge and Scicchitano (1994) studied the issue of Federal oversight as it pertained to environmental regulation where responsibility for enforcement of Federal standards was transferred to the State. They analyzed Federal oversight behavior at the Office of Surface Mining (Department of the Interior) during 1985-1989 with an eye to how Federal regulators acted. They found that oversight actions were influenced not only from the top by national policymakers but also from the bottom by State actors such as governors, legislators, and interest groups. As they noted, Federal regulation is often justified on the basis that it is less subject to capture by political interests, so as a result their research calls into question whether regulation by the Federal government is necessarily any better than regulation by State governments.

Political Influence on Program Operations

Some studies also suggest that political pressures by the Congress or Federal administrators to "universalize" Federal programs could lead to waste and inefficiency over time. Hamman (1993), for instance, studied the evolution of mass transportation programs operated by the Urban Mass Transportation Administration (UTMA) from the 1960s to the 1980s. He concluded that Federal administrators in the UTMA used their discretion in funding to broaden the reach of their mass transportation program, and advocated that it be bundled with additional programs during congressional reauthorization. In this way the UTMA was able to steadily increase the number of jurisdictions and constituencies it served and, in turn, steadily increase its base of congressional support.

One possible way of countering political pressures from the Federal, State, and local levels is by using performance measures in program management. Performance measures provide objective assessments of local needs and how well they are being met and allow for a rational distribution of funding. Consistent with this view, the Gilmore Commission (2002) advocated the development and use of an integrated system of metrics to ensure that the Federal government could measure the level of preparedness across the country and that dollars were being spent effectively.

Encouraging Innovation in States and Localities

Local-responder communities are closer to WMD threats than the Federal government, and in many cases they know their own needs better than the Federal and State governments. Consequently, a desirable goal of the Federal government regarding programs that target domestic response capabilities could be to encourage innovation at the State and local level.

In the context of Federal grant programs, State and local flexibility essentially equates to having few Federal requirements or restrictions placed on them. These include things like maintenance-of-effort requirements, but they also include more basic things such as financial performance reporting and eligible activities. Although the surveyed literature shows that greater flexibility and autonomy can lead to more innovation, it also shows that there are barriers to providing it at the local level tradeoffs with planning and accountability.

With respect to the benefits of flexibility, Marcus (1998) for example looked at how 24 nuclear power plants implemented safety review innovations in 1981 and 1982 that were introduced by the Nuclear Regulatory Commission (NRC) after the Three Mile Island reactor accident. Although causality is difficult to demonstrate, he tested for a mutually reinforcing relationship between having autonomy and being a plant with good safety performance and found some evidence to support this assertion. Similarly, he found some evidence to support the notion of a mutually reinforcing relationship between having little autonomy and being a plant with poor safety performance. He concluded that poor performing plants would likely improve their safety with more autonomy, but that given their past performance they would be unlikely to receive it.

But some studies suggest that the States have been unwilling to provide local governments the same authority and flexibility that they sought from the Federal government in the 1990s. Kelly and Ransom (2000) explored the relationship between three cities and their parent States (Richmond, Virginia; Trenton, New Jersey; and Tallahassee, Florida) and noted similarities in their interactions. They found that most State-city contacts were initiated by the cities, and that the communications channels used by the cities are hampered by, among other things, the lack of structural ties with State leaders and the tendency for States to look on local jurisdictions as lobbying groups. Thus, the flow of funds through the States potentially could adversely impact local flexibility.

Other obstacles to innovation stem from the nature of the homeland security threat. Posner (The Nelson A. Rockefeller Institute of Government, 2003) advocated a model with performance partnerships or

contracts between the Federal, State and local jurisdictions, partially because it allows for local experimentation and innovation. He noted that this type of collaboration works best when the stakes are lower, when there is limited national consensus, and when there is limited knowledge of how best to meet objectives. In the case of homeland security, however, he concluded that knowledge is limited but the stakes are high and there is general agreement that the preparedness and response system is interdependent and only as strong as its weakest link.

Also, having greater flexibility and autonomy conflicts to some extent with accountability. The GAO (1998) looked at grant program design in education and other areas and created a typology of programs. The GAO noted that accountability for performance to the Federal government tends to be greatest in programs with national performance objectives and with few major activities; these programs easily allow program dollars spent across the country to be tracked and compared with respect to outcomes. But at the same time these types of programs provide little flexibility to the States and localities. On the other hand, expenditures for larger block grants that incorporate State and local flexibility often cannot be measured against national goals because every State's implementation can differ.

Summary

The reviewed literature on intergovernmental aid yields a number of insights relevant to the design of Federal grant programs. The important points are summarized below:

- **Federal grant programs can stimulate State and local effort in significant and desirable ways, however sustained effort might require a sustained Federal commitment.** The selected literature showed that State and local governments respond positively to Federal financial incentives by more than one would expect. This is true even when unrestricted lump-sum grants are used, and it is likely that the effects are greater when restrictions are imposed such as maintenance-of-effort requirements and categorical grant requirements. But the States and localities will likely take a "wait and see" approach before they agree to commit their resources to fund a new activity over the long term.

- **Studies find that, on average, the States and localities supplant 60 cents on every Federal dollar of grants, but this can be mitigated to some extent by State and local fund requirements.** This supplantation estimate by the GAO is especially true with respect to block grants and activities that have had previous State and local involvement. Matching fund requirements and maintenance-of-effort requirements can help preserve local commitment, but the Federal government must be careful to not penalize jurisdictions that undertook homeland security investments on their own initiative.

- **Studies suggest that State involvement with Federal funding for local jurisdictions could improve coordination between levels of government, but State involvement is not a necessity and has disadvantages.** Many of the reviewed studies indicate that passing Federal funds through the States to localities can help to translate and focus Federal goals into local activities that are relevant to their specific geographic regions. States can also help to ensure that local jurisdictions collaborate with one another and take actions that are regionally coherent and consistent with State plans. However, States can at times be unresponsive to the needs of local communities with respect to the distribution of funds. This can be mitigated to some extent by Federal requirements limiting how much funding States can withhold and for how long. Moreover, mechanisms other than the flow of funding can help to facilitate coordination.

- **Studies suggest some evidence that Federal and State governments have had difficulties in targeting aid to the communities where it is needed the most, but that States sometimes do slightly better.** The surveyed literature showed little correlation between measures of community need and actual allocations. It is unclear, however, whether these results arise from

programs poorly targeting needy communities, or from programs having other objectives, or from researchers poorly measuring community need. Moreover, the grant type can also have an effect: one study showed that formula grants tend to lead to situations with universalistic funding whereas competitive grants are sometimes influenced by political persuasion.

- **Studies indicate that the allocation of competitive grants often coincides more with local administrative capacity rather than local needs.** The surveyed literature suggests that the local communities with the strongest planning and administrative functions and the greatest entrepreneurial spirit tended to apply for grants. This can be mitigated to some extent by programs that provide administrative technical assistance to applicants.

- **Studies suggest that the effectiveness of Federal programs can get diluted over time because of political pressures on regulatory activity and funding decisions.** The studies reviewed on the management of Federal grant programs showed examples of Federal and State influence on regulatory enforcement actions. They also showed attempts by Federal agencies to broaden the coverage of grant programs to increase Congressional support rather than to fulfill unmet local needs.

- **Studies indicate that greater program flexibility can likely increase local innovation, but there can be tradeoffs with accountability and possibly preparedness.** The studies reviewed on State and local innovation illustrated that block grants provide local jurisdictions the flexibility to direct funds to activities they deem the most critical because they have the fewest Federal restrictions. At the same time, however, they suggested that flexibility can make it harder to track where dollars are spent relative to when targeted project grants are used. Also, some studies indicated that fostering innovation might make less sense in a homeland security setting, since experimentation could possibly result in weak links in national preparedness in the form of one or more poorly prepared local jurisdictions or responder communities.

Program Reviews

Our research includes reviews of three current Federal grant programs to provide some real-world context for the studies discussed in the literature review. The three grant programs examined relate to fire protection and emergency preparedness. They include: the Assistance to Firefighters Grant Program (AFGP), the Emergency Management Performance Grants (EMPG) program, and the Urban Areas Security Initiative (UASI).

Grant Program	Flow of Funds	Type of Funds	Matching Requirement	Maintenance-of-Effort ?
Assistance to Firefighters Grant Program	Direct to locals	Competitive	10 to 30 percent, depending on population	Yes
Emergency Management Performance Grants	To States for allocation to locals	Formula	Trend to 50/50 Fed/State cost share	No
Urban Areas Security Initiative	Direct/pass-through to locals and States	Formula	None	No

Source: RAND **Table 3.1: Design Elements of Selected Grant Programs**

Although a number of local-responder programs exist, these three were selected because they present an interesting diversity of program design elements. As shown in Table 3.1, the AFGP, EMPG, and UASI use among them a mix of competitive and formula grants. Two programs allocate some funding directly

to local jurisdictions; one program employs pass-through funding for localities; and one program allocates funding to the States, which may then reallocate it as they see fit. Two programs have matching or cost-share requirements, and one has a maintenance-of-effort requirement. Together, these programs can provide insight into how different design elements interact to achieve different Federal goals.

Assistance To Firefighters Grant Program[81]

The Assistance to Firefighters Grant Program (AFGP) contains the following design elements: It provides competitive grants directly to local jurisdictions. It has a local matching requirement of 10 to 30 percent depending on the population of the local jurisdiction. It also has a local maintenance-of-effort requirement allowing no supplantation.

Administered by the U.S. Fire Administration (USFA) in the Federal Emergency Management Agency (FEMA), the AFGP provides funding to support those local fire departments that lack the tools and resources necessary to protect the health and safety of the public as well as that of firefighting personnel. Congress created the AFGP in 2000 (Public Law 106-398) out of a concern that local firefighters were facing greater risks in their jobs but with fewer resources.[82] The AFGP derives its authority specifically from the Federal Fire Protection and Control Act of 1974 (15 U.S.C. 2201 et seq.), as amended. Congress appropriated $360 million in FY 2002 and another $750 million in FY 2003 and again in FY 2004 to fund the program.

Eligibility for the AFGP is limited to fire departments of a State that provide fire suppression to a population within a fixed geographical area. Each year, local fire departments may apply for grants to fund one or more eligible activities in a programmatic or functional area. This approach, in use since FY 2002, has heretofore used four program operations: fire operations and firefighter safety; fire prevention; emergency medical services; and firefighting vehicles acquisition. The eligible activities in a given programmatic or functional area are multiple and intended to be comprehensive for that area.[83]

The AFGP provides one-year grants on a competitive basis, and awards are made directly to local fire departments. The competition has two phases. In the first phase, applications are ranked based on how well they meet established program funding priorities for the type of community served (i.e., urban, suburban, and rural). The applications that best address the program funding priorities will be considered to be in the "competitive range" and will undergo the second phase of competition. In the second phase, applications are assessed according to the clarity and completeness of the project description, the demonstration of the financial need of the applicant, and a description of cost and benefit.

The AFGP contain a matching requirement. Applicants who protect a population of 50,000 or less are required to provide a non-Federal cost-share of at least 10 percent of the total award; those protecting a population greater than 50,000 are required to provide a non-Federal match of at least 30 percent. The AFGP also has a maintenance-of-effort requirement to ensure that the Federal funds are used to supplement, not supplant, existing resources. Grant awards tend to be rather uncomplicated: they are

[81] This description is based on Federal Emergency Management Agency documents (March 11, 2003; March 14, 2003) and on a phone interview with Brian Cowan, Director of the Assistance to Firefighters Grant Program, U.S. Fire Administration, Federal Emergency Management Agency, Department of Homeland Security.

[82] For example, see testimony to the House Subcommittee on Oversight, Investigations, and Emergency Management on HR 1168, the Firefighter Investment and Response Enhancement Act (Congressional Record, April 12, 2000). Kenneth Burris, Chief Operating Officer of the United States Fire Administration, noted in his remarks that 100 firefighters died in 1999 (where 16 deaths occurred in December alone) with an average of 90,000 firefighters being injured on the job each year. He also mentioned that "now fire departments are being called on to provide an ever expanding and more complex array of services including hazardous materials, search and rescue, emergency medical, disaster response, and counter-terrorism [while] at the same time local governments and fire departments are encountering severe budget challenges."

[83] For example, eligible activities under the fire operations and firefighter safety program fall under training; wellness and fitness; firefighting equipment acquisition; personal protective equipment acquisition; and modifications to fire stations and facilities.

relatively small (the average award size is $70,000) and typically are used for basic firefighter activities and equipment.

The program as structured seemingly tends to result in wide and balanced geographic coverage, which from the literature review is more typical of formula grant programs than competitive grant programs. This results, however, because of the AFGP's small average award size and large number of awards: The AFGP has received 19,000 to 21,000 applications a year, and under its FY 2003 appropriation anticipates that it will award grants to about 9,000 fire departments nationwide.[84] (It distributed about 5,300 grants in 2002, and about 1,850 grants in 2001.) These fire departments are spread across every region, every type of community (e.g., urban, rural), and every type of department (e.g., paid, volunteer).

But the wide and balanced geographic coverage might also occur because the AFGP has made applying for funding simple and straightforward. The Director of the AFGP noted that an important focus of the program is "getting needed resources to local fire departments as quickly as possible." To this end, the AFGP utilizes online application and grant management systems to help funding get disbursed and obligated in a timely manner.

It should also be stressed that resources in the AFGP are not necessarily targeted towards the most "needy," as need is defined here; proposed funding uses first must be consistent with program priorities and secondarily based on need and cost-benefit analyses. But on the margin, the Director of AFGP has some discretion to direct funding towards particular types of communities and particular regions. And the Director has anecdotal evidence that suggests that grants often go to regional areas that are supportive of urban centers.

With respect to coordination between the different levels of government, interactions under the AFGP occur mostly between FEMA and the localities. Direct funding to local fire departments means that the States are bypassed. Consequently, State fire marshals and emergency management centers have complained about their lack of input in to the program, so the Director of AFGP feels that there is some room for increased coordination with the States. That said, the AFGP is intended primarily as a local fire department program, however, and as such there tends to be less need for coordination with the States; the level of detail from the program's decisions (e.g., numbers of self-contained breathing apparatuses, lengths of hose) is beyond normal State-level coordination activities. Moreover, as mentioned there is at least some evidence that local jurisdictions already do collaborate on their own initiative.

Local innovation is not a particular concern of the AFGP. The Director notes that the program determines the eligible activities (which tend to focus on "meeting basic firefighter needs") and it funds fire departments according to how well local requests mesh with program priorities. That said, the AFGP does try to allow for local flexibility by presenting a comprehensive list of eligible activities in its program areas.

In essence, the AFGP has as its primary goal to increase the level and/or quality of preparedness activities, with a secondary goal of improving the geographic distribution of funds. It provides an example of a narrowly tailored Federal program that focuses on helping to provide basic equipment and training to resource-constrained fire departments across the country. The requirement for local matching funds for these one-time competitive grants provides an incentive for fire departments to acquire only necessities. The maintenance-of-effort requirement ensures that over time fire departments increase their level of preparedness. And because the AFGP fills basic needs such as vehicles and hoses, funding bypasses State governments and goes directly to localities.

[84] It also has a statutory grant limit of $750,000 to any one fire department.

Emergency Management Performance Grants[85]

The Emergency Management Performance Grants (EMPG) program contains the following program design elements: It provides formula funding that passes through the States to localities. It has a matching funds requirement and no maintenance-of-effort requirement.

Administered by FEMA, the EMPG assists the development, maintenance, and improvement of State and local emergency management capabilities. EMPG funds help to meet State and local needs in disaster mitigation, preparedness, response, and recovery. The EMPG is a consolidation of former planning program activities, and as such it receives its authority from a number of statutes: The Departments of Veterans Affairs, Housing and Urban Development, and Independent Agencies Appropriations Act, 2000, Public Law 106-74; 38 U.S.C. 301; Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, Title II, Section 201(d), Title VI, Sections 611 and 613, 42 U.S.C. 5196 and 5196(b); Public Law 93-288, as amended; 42 U.S.C. 5121 et seq.; and, 42 U.S.C. 5195 et seq. Congress appropriated $165 million for the EMPG for FY 2003 and $181 million for FY 2004.

Eligible applicants for EMPG funding are all 50 States plus the District of Columbia and all territories and possessions. EMPG funding is used to help the States achieve the goals set out in their five-year operations plans by supporting a variety of functional areas of emergency management.

EMPG funding is allocated to the States by formula, although the specific formula is not in statute. For each State, FEMA derives a target allocation for the year by calculating the percentage of available EMPG funds that the State received in the prior year. A matching requirement is calculated for each State, where each recipient's cost share percentage will increase by one percent over the prior year's match until the 50 percent Federal/50 percent State level is reached. There is no maintenance-of-effort requirement, although the structure of the matching requirement effectively maintains or increases State spending for EMPG activities over time.

The States can then distribute EMPG funding across their localities as they see fit to support emergency management activities. According to the FEMA Region IX Emergency Management Specialist, States often differ as to their statewide response structures, so they often differ in terms of how they implement the program. Many States allocate funds by formula across their local jurisdictions after first adding additional State goals and performance requirements for locals to meet.

Take California as an example. FEMA Region IX (California's FEMA liaison) considers California to be a "model" State given its sophistication in planning and training and its utilization of regional offices. California allocates 75 percent of its EMPG funds to all of its county operational areas. Here, a county operational area is a body comprising all of the political jurisdictions and responder groups in a county where all members are treated equally. The State Office of Emergency Services (OES), which administers the EMPG in California, provides each operational area a baseline amount of money and allocates the rest according to population.

Each operational area then decides which constituent jurisdictions get EMPG funds in order to best meet Federal and State guidelines and requirements. The OES Planning Branch Chief responsible for the EMPG believes that such a distribution mechanism makes it likely that funds ultimately get spread geographically according to need. This is because the jurisdictions in each operational area have to decide how to distribute limited funds among themselves; these compromises are made at the lowest level, or the "impact area." These compromises, of course, can be adversely affected to the extent that FEMA and OES guidelines interfere with the distribution of funds according to actual needs.

[85] This description is based on the Catalog of Federal Domestic Assistance (2003) and on phone interviews with Jane Hindmarsh, Planning and Technological Assistance Branch Chief, Governor's Office of Emergency Services, State of California; and Barbara Kambouris, Emergency Management Specialist, FEMA Region IX, Department of Homeland Security.

Coordination between levels of government is supported under the EMPG because FEMA allocates funding to the States rather than to local emergency management centers. As the FEMA Region IX Specialist points out, relying on the States is good because the States are "the leader of the band," and because dealing with the locals requires a lot of effort and the States are better positioned than the Federal government to do this. Additionally, the States have the opportunity to add their own guidelines to local allocations, thereby adding coherence to the use of EMPG grants by the localities. California also uses its six regional OES offices to foster collaboration between operational areas in a region as well as with other State agencies.

Given the small size of the grant awards (the average State award in FY 2001 was $2.4 million) and the narrow purpose of the program, local jurisdictions tend to complain more about insufficient funding than about insufficient flexibility or inefficient program management. Local innovation can happen in the EMPG, though. In California's case it is fostered by the collaboration required for the operational areas to function effectively.

Consequently, as a program to enhance emergency management planning at the State and local level, the EMPG has a primary goal of increasing the level and/or quality of preparedness activities and a secondary goal of improving the coordination between levels of government. The EMPG represents an example of a Federal program that funds a narrow set of activities on an ongoing basis. Its small average award allocated by formula means that recipient funding is relatively predictable from one year to the next. There is no maintenance-of-effort requirement, but the 50/50 Federal/State cost share helps to minimize the supplantation of recipient funds. And the allocation of funding to the States with the subsequent reallocation to localities (with added State requirements) helps to facilitate coordination.

Urban Areas Security Initiative[86]

The Urban Areas Security Initiative (UASI) Grant Program contains the following design elements: It provides one set of formula grants directly to local jurisdictions; it provides a second set of formula grants through the States to local jurisdictions. There are no local matching fund requirements or maintenance-of-effort requirements.

Administered by the Office for Domestic Preparedness (ODP) in the U.S. Department of Homeland Security (DHS), the UASI provides funds to enhance the ability of State and local governments to prepare for and respond to terrorist threats or incidents. The stated purpose of the UASI is to address the unique needs of large urban areas, and to assist them in building an enhanced and sustainable capacity. The intent behind the program is to provide localities in the short term needed resources to address new and significant terrorist threats, and to develop sustainable models in the long term that other urban areas across the nation can look to and learn from. The UASI consists of two separate parts, Grant Program (GP) I and GP II. The UASI GP I is authorized by the Omnibus Appropriations Act of 2003 (Public Law 108-7), with appropriations of $100 million for FY 2003; the UASI GP II is authorized by the Emergency Wartime Supplemental Appropriations Act of 2003 (Public Law 108-11), with appropriations of $700 million for FY 2003.

Seven selected jurisdictions are eligible to receive UASI GP I funding,[87] and 30 jurisdictions (including the original 7) are eligible to receive GP II funding.[88] These urban areas are regions, typically consisting

[86] This description is based on documents from the Office of Domestic Preparedness (2003a, 2003b) and on a phone interview with Darrell Darnell, Director of the Urban Areas Security Initiative, Office for Domestic Preparedness, U.S. Department of Homeland Security.
[87] They are New York City, the National Capital Region, Los Angeles, Seattle, Chicago, San Francisco, and Houston.

of a county with a core city. They were chosen by DHS based on an assessment of three key factors: existing critical infrastructure in a core city and region; an analysis of current threat estimates produced by the DHS Information Analysis and Infrastructure Protection Division for a core city and region; and population density in a core city and region. Eligible jurisdictions may use UASI GP I and GP II funding for a wide variety of needs, including planning, equipment, training, and exercises.

The formula that determined eligible jurisdictions is also used to allocate funding amounts to the urban areas. Under UASI GP I, funding is being distributed directly from DHS to the localities. Under UASI GP II, however, funding is being passed through the States. States must pass through at least 80 percent of the funds to their eligible urban areas. States may use up to 20 percent of grant award to complement State assets that will provide direct assistance to the urban areas for terrorist threats or incidents. There are no State or local matching requirements, but there is a requirement that UASI funding not supplant funds appropriated for the same purpose.

According to the Director of the UASI, the program emphasizes the importance of building "sustainable anti-terrorism programs" at the local level. The focus on regions rather than on individual cities is to facilitate local partnerships and complementary capabilities that will enhance the regions' overall capability to prevent, deter, or respond to a terrorist incident. A key component of the program is the development of metrics and an evaluation process to measure how well regions are prepared.

The program also emphasizes effectiveness and flexibility. The UASI is designed to get funding to localities to start meeting their needs as soon as possible; funding either goes directly to the locals or must be released by the States within 45 days. And only 3 percent of grant awards may be used for program management and administration purposes. Flexibility comes through the variety of eligible uses.

The UASI also stresses the importance of attempting to target areas with the highest need. The allocation formula used (based on critical infrastructure, threat estimates, and population density) was a direct attempt to measure need in an objective fashion with the most pertinent information. Of course, as discussed in the literature review, it can be difficult to accurately define an area's "need" for any program. That said, though, it is not readily apparent that there are necessarily better measures of need than those currently employed in the UASI.

An interesting insight regarding the UASI comes from the transition from GP I to GP II. The original program (GP I) allocates funding directly to the 7 urban areas. The urban areas under GP I have immense flexibility considering that, aside from reporting requirements, they are only required to submit their plans to a designated State agency for administrative review (if applicable). But as a result of lessons learned from other Federal programs and a desire to facilitate State and local collaboration, ODP amended the distribution procedures for UASI GP II such that the States now are critical actors and have much greater responsibilities to ensure collaboration and coordination.

Under UASI GP II, a State administrative agency for an urban area must specifically define the geographic boundaries of that urban area consistent with the boundaries of the local responder communities. A State also must facilitate the development of an Urban Area Working Group, comprising the chief executive officers of all its constituent jurisdictions. This working group is then responsible for assessing the capabilities of the urban area and developing a homeland security strategy before the bulk of funds can be released.

Essentially, the UASI has as its primary goal increasing the level and/or quality of preparedness activities, with secondary goals of strengthening coordination across different levels of government and encouraging

[88] The remaining 23 urban areas are Buffalo, NY; Dallas, TX; San Diego, CA; Sacramento, CA; Long Beach, CA; Boston, MA; Denver, CO; Philadelphia, PA; Pittsburgh, PA; St. Louis, MO; Kansas City, MO; Miami, FL; Tampa, FL; Cincinnati, OH; Cleveland, OH; Detroit, MI; Newark, NJ; Phoenix, AZ; Baltimore, MD; Honolulu, HI; Portland, OR; New Orleans, LA; and Memphis, TN.

innovation. Having arisen in the aftermath of the terrorist attacks of September 11, 2001 out of concern that large urban areas were not adequately prepared to deal with their unique threats, the UASI provides an example of a Federal program designed to address a new and complex need. DHS developed a formula to determine which areas had the greatest needs, it selected a subset of these areas, and is allocating funding to them accordingly over a few years. In light of the substantial resources needed for localities to develop a sustained capability to deal with these threats, the UASI has no State or local funding requirements; large urban areas can begin developing their preparedness capacity immediately with Federal funds, and over time adjust their local finances to take ownership of their new responsibilities. The initial version of the UASI had funds flow directly to localities; the second version amended this to involve the States to help facilitate regional cooperation and stretch Federal resources.

Findings

The literature review on intergovernmental grants generally and the review of three Federal grant programs for fire protection and emergency preparedness have provided a number of relevant insights into burden sharing between the Federal, State, and local governments. The main findings, described below, can be used to help the Federal government design programs for WMD preparedness that effectively meet its desired goals:

- **If a goal of the Federal government were to enhance the level and/or quality of preparedness activities by local responders, then having categorical grants, local matching fund requirements, and maintenance-of-effort requirements will help augment State and local efforts.** Studies suggest that even unrestricted lump-sum grants stimulate State and local behavior. But adding additional conditions on Federal grants will make it more difficult for State and local governments to substitute Federal funding for their own funding.

- **If a goal of the Federal government were to strengthen coordination across different levels of government, then requiring Federal funds to flow through the States to local jurisdictions could be beneficial but is not necessary.** Some studies suggested that allocating funding through the States can help translate and focus Federal goals into local activities that are relevant to their specific geographic regions. States can also help to ensure that local jurisdictions collaborate with one another and take actions that are regionally coherent and consistent with State plans. However, the Federal government can conceivably impose standards or other requirements on States and localities to facilitate coordination.

- **If a goal of the Federal government were to improve the geographic distribution of funds across local-responder jurisdictions, formula grants and competitive grants can result in different outcomes.** Studies suggest that both Federal and State governments have had difficulties in targeting aid to the communities where it is needed the most. But formula grants tend to result in universalistic coverage, whereas competitive grants often depend on the planning capacity and entrepreneurial spirit of the applicants.

- **If a goal of the Federal government were to improve the administration of Federal grant programs, then limits on the States when pass-through funding is used would be beneficial.** The two reviewed Federal programs that allocated funding through the States limited the amount of funding that the States could withhold and set dates by which the States had to disburse money to local recipients.

- **If a goal of the Federal government were to encourage innovation in States and localities, then imposing few Federal grant requirements could be beneficial but there could be tradeoffs with accountability and possibly preparedness.** Studies suggested that block grants provide localities the flexibility to direct funds to activities they deem the most critical because they have the fewest Federal restrictions. At the same time, this flexibility can make it harder to

track where dollars are spent, and unsuccessful experimentation could result in weak links in national preparedness.

REFERENCES

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, "III. For Ray Downey: Third Annual Report to the President and the Congress," Santa Monica, CA: RAND, December 15, 2001.

-----, "IV. Implementing the National Strategy: Fourth Annual Report to the President and the Congress," Santa Monica, CA: RAND, December 15, 2002.

Aronson, Richard J., and Vincent G. Munley, "(Non)equivalence in a Federalism: Dual Tax Shares, Flypaper Effects and Leviathan," *Public Choice*, Vol. 89, 1996, pp. 53-62.

Bradford, David F., and Wallace E. Oates, "Towards a Predictive Theory of Intergovernmental Grants," *The American Economic Review*, Vol. 61, No.2, May 1971, pp. 440-448.

Canada, Ben, "Department of Homeland Security: State and Local Preparedness Issues," Washington, D.C.: Congressional Research Service, CRS Report RL31490, May 5, 2003.

-----, "First Responder Initiative: Policy Issues and Options," Washington, D.C.: Congressional Research Service, CRS Report RL31475, July 8, 2003.

Catalog of Federal Domestic Assistance, "97.042 Emergency Management Performance Grants," http://www.cdfa.gov/public/ viewprog.asp?progid=1738, 2003.

Council on Foreign Relations, "Emergency Responders: Drastically Underfunded, Dangerously Unprepared," Report of an Independent Task Force, 2003.

Dye, Thomas R., and Thomas L. Hurley, "The Responsiveness of Federal and State Governments to Urban Problems," *The Journal of Politics*, Vol. 40, No. 1, February 1978, pp. 196-207.

Ellwood, Deborah A., and Donald J. Boyd, "Changes in State Spending on Social Services Since the Implementation of Welfare Reform: A Preliminary Report," The Nelson A. Rockefeller Institute of Government, February 2000.

Federal Emergency Management Agency (FEMA), U.S. Department of Homeland Security, "2003 Program Guidance for the Assistance to Firefighters Grant Program," http://www.usfa.fema.gov/fire-service/grants/2003grants/03prgguide.pdf, March 11, 2003.

-----, "Assistance to Firefighters Grant Program; Final Rule and Notice," Federal Register, Vol. 68, No. 50, March 14, 2003, pp. 12544-12560.

Gramlich, Edward M., "Intergovernmental Grants: A Review of the Empirical Literature," in *The Political Economy of Fiscal Federalism*, edited by Wallace E. Oates, Lexington, MA: Lexington Books, 1977.

Hamman, John A., "Universalism, Program Development, and the Distribution of Federal Assistance," *Legislative Studies Quarterly*, Vol. 18, No. 4, November 1993, pp. 553-568.

Hedge, David M. and Michael J. Scicchitano, "Regulating in Space and Time: The Case of Regulatory Federalism," *The Journal of Politics*, Vol. 56, No. 1, February 1994, pp. 134-153.

Hines, James R., and Richard H. Thaler, "Anomalies: The Flypaper Effect," *The Journal of Economic Perspectives*, Vol. 9, No. 4, Autumn 1995, pp. 217-226.

Hofferbert, Richard I., and John K. Urice, "Small-Scale Policy: The Federal Stimulus versus Competing Explanations for State Funding of the Arts," American Journal of Political Science, Vol. 29, No. 2, May 1985, pp. 308-329.

Kelly, Janet, and Bruce Ransom, "State Urban Policy: 'New' Federalism in Virginia, New Jersey and Florida," *Policy Studies Review*, Vol. 17, No. 2/3, Summer/Autumn 2000, pp. 62-83.

Levine, Charles H., and Paul L. Posner, "The Centralizing Effects of Austerity on the Intergovernmental System," *Political Science Quarterly*, Vol. 96, No. 1, Spring 1981, pp. 67-85.

Logan, Robert R., "Fiscal Illusion and the Grantor Government," *The Journal of Political Economy*, Vol. 94, Issue 6, December 1986, pp. 1304-1318.

Marcus, Alfred A., "Implementing Externally Induced Innovations: A Comparison of Rule-Bound and Autonomous Approaches," *The Academy of Management Journal*, Vol. 31, No. 2, June 1988, pp. 235-256.

Nathan, Richard P., and Fred C. Doolittle, "Federal Grants: Giving and Taking Away," *Political Science Quarterly*, Vol. 100, No. 1, Spring 1985, pp. 53-74.

Oates, Wallace E., "An Essay on Fiscal Federalism," *Journal of Economic Literature*, Vol. 37, Issue 3, September 1999, pp. 1120-1149.

Office for Domestic Preparedness, U.S. Department of Homeland Security, "Fiscal Year 2003 Urban Areas Security Initiative Grant Program I: Program Guidelines and Application Kit," NCJ200848, 2003a.

-----, "Fiscal Year 2003 Urban Areas Security Initiative Grant Program II: Program Guidelines and Application Kit," NCJ200849, 2003b.

Pelissero, John P., "State Aid and City Needs: An Examination of Residual State Aid to Large Cities," *The Journal of Politics*, Vol. 46, No. 3. August 1984, pp. 916-935.

Pelissero, John P., and David R. Morgan, "Targeting Intergovernmental Aid to Local Schools: An Analysis of Federal and State Efforts," *The Western Political Quarterly*, Vol. 45, No. 4, December 1992, pp. 985-999.

Saltzstein, Alan L., "Federal Categorical Aid to Cities: Who Needs It versus Who Wants It," *The Western Political Quarterly*, Vol. 30, No. 3, September 1977, pp. 377-383.

Rich, Michael J., "Distributive Politics and the Allocation of Federal Grants," *The American Political Science Review*, Vol. 83, No. 1, March 1989, pp. 193-213.

Stein, Robert M., "Federal Categorical Aid: Equalization and the Application Process," *The Western Political Quarterly*, Vol. 32, No. 4, December 1979, pp. 396-408.

Stein, Robert M., "Municipal Public Employment: An Examination of Intergovernmental Influences," *American Journal of Political Science*, Vol. 28, No. 4, November 1984, pp. 636-653.

The Nelson A. Rockefeller Institute of Government, "The Role of 'Home' in Homeland Security: The Federalism Challenge," Albany, NY, March 24, 2003.

Thomas, Robert D., "Implementing Federal Programs at the Local Level," *Political Science Quarterly*, Vol. 94, No. 3, Autumn 1979, pp. 419-435.

U.S. Conference of Mayors Homeland Security Monitoring Center, "First Mayors' Report to the Nation: Tracking Federal Homeland Security Funds Sent to the 50 State Governments," September 2003.

U.S. General Accounting Office, "Federal Grants: Design Improvements Could Help Federal Resources Go Further," GAO/AIMD-97-7, December 1996.

-----, "Balancing Flexibility and Accountability: Grant Program Design in Education and Other Areas," GAO/T-GGD/HEHS-98-94, February 11, 1998.

-----, "Combating Terrorism: Observations on the Nunn-Lugar-Domenici Domestic Preparedness Program," GAO/T-NSIAD-99-16, October 2, 1998.

-----, "Combating Terrorism: Opportunities to Improve Domestic Preparedness Program Focus and Efficiency," GAO/T-NSIAD-99-3, November 1998.

-----, "National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts is Critical to an Effective National Strategy for Homeland Security," GAO-02-621T, April 11, 2002.

-----, "Homeland Security: Reforming Federal Grants to Better Meet Outstanding Needs," GAO-03-1146T, September 3, 2003.

Welch, Susan, and Kay Thompson, "The Impact of Federal Incentives on State Policy Innovation," *American Journal of Political Science*, Vol. 24, No. 4, November 1980, pp. 715-729.

Wood, B. Dan, "Modeling Federal Implementation as a System: The Clean Air Case," *American Journal of Political Science*, Vol. 36, No. 1, February 1992, pp. 40-67.

Zycher, Benjamin, "A Preliminary Benefit/Cost Framework for Counterterrorism Public Expenditures," Santa Monica, CA: RAND, MR-1693-RC, 2003.

APPENDIX G-CREATING THE DEPARTMENT OF HOMELAND SECURITY*

The process of creating the Department of Homeland Security (DHS) has been one of the most significant and challenging United States government restructuring efforts since World War II. The aim of establishing DHS and integrating a wide range of agencies and offices from the Coast Guard to FEMA was to increase the security of the U.S. homeland and to improve the government's ability to prevent and prepare for terrorist attacks and other major disasters. Indeed, the challenge of integrating 22 separate agencies into a single, effective department has been substantial.

Unfortunately, there has been little comprehensive and systematic examination of DHS's structure and strategy. This appendix assesses and evaluates DHS's efforts and challenges in four areas:

- Information analysis
- Emergency preparedness and response
- Science and technology
- Border and transportation security

These areas were chosen for two major reasons. First, they represent critical homeland security issue areas. Information analysis is important to understand the threats to the homeland, recognize vulnerabilities, and disseminate information to the American public and State, local, and private sector entities. Emergency preparedness and response is necessary to prepare for, and respond to, future attacks and other major disasters. Science and technology is critical to research and utilize relevant technologies and scientific talent in order to improve the security of the United States. And border and transportation security is important to protect points of entry such as seaports, land borders, coastlines, airports, highways, railroads, and waterways. Second, these areas correlate with the major directorates of DHS, which serve as the core functional departments in DHS. They include the Directorates of Information Analysis and Infrastructure Protection, Emergency Preparedness and Response, Science and Technology, and Border and Transportation Security.

Several important caveats are apropos. To begin with, there are significant hurdles in evaluating a department that has just been established. The Homeland Security Act was passed by Congress and signed by President George W. Bush in November 2002, and a number of related organizations such as the Terrorist Threat Information Center (TTIC) were established as recently as May 2003. This reality presents practical challenges because it takes time to hire staff, restructure agencies, and outline strategic objectives. Nonetheless, it is both possible and necessary to explore the logic of DHS's structure, examine and evaluate its strategies and priorities thus far, and analyze whether current efforts maximize the nation's security. Furthermore, this chapter does not pretend to offer a comprehensive evaluation of the strategy and structure of DHS. There are important functions of DHS that are not included in this analysis, such as infrastructure protection. Their absence should not be regarded as a statement of their relative importance or success, but rather are due to the limited scope of this effort. Rather, it focuses on several significant issues of homeland security that DHS has been tasked to address.

DHS Structure and Objectives

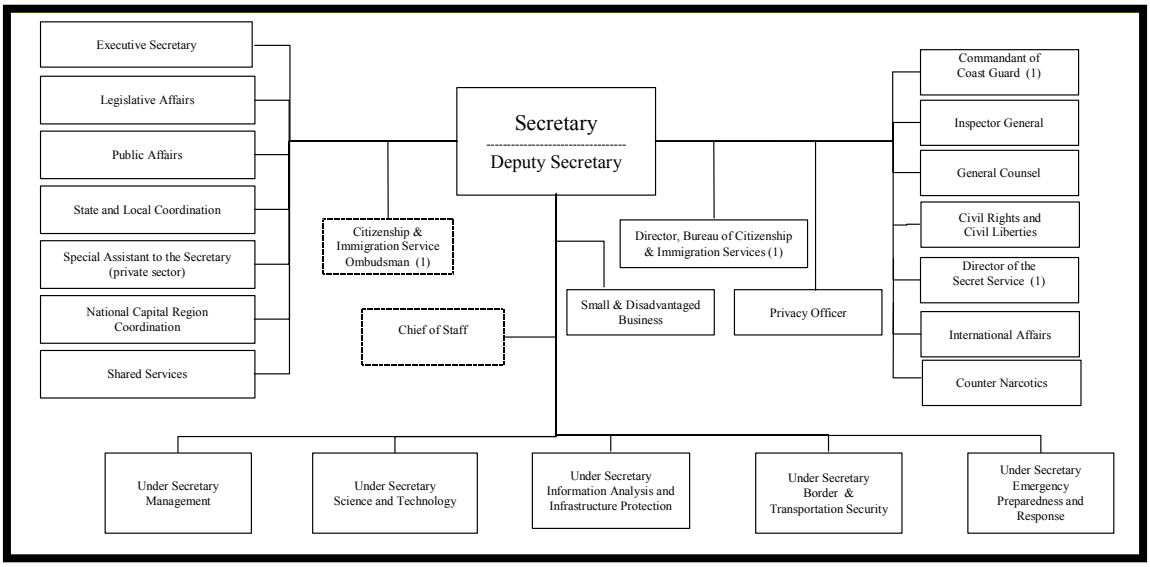
Since its inception in 1998, the Gilmore Commission has offered a number of homeland security recommendations that are now applicable to current DHS strategy and structure. First, it recommended the creation of a National Counter Terrorism Center (NCTC) as a "stand-alone" organization to consolidate the analysis of foreign-collected and domestically-collected intelligence and information on international terrorists and terrorist organizations that threaten attacks against the United States. It contended that the organization should be located outside of the CIA for legal, policy, perception, and

---

*** Seth G. Jones**

cultural reasons; outside of the FBI because of concern that it might focus too much on law enforcement at the expense of detection and prevention; and outside DHS because it would be viewed as more responsive to DHS activities at the expense of other agencies.[89] Second, the Gilmore Commission argued that terrorism-related threat assessments and intelligence should be disseminated to appropriate State and local agencies and response organizations.[90] Third, the Commission recommended preserving an all-hazards approach to emergency preparedness. It advised Federal agencies to coordinate training and equipment programs as part of all-hazards preparedness, including the incorporation of training for combating terrorism into existing all-hazards training.[91] Similarly, it suggested consolidating information about, and application procedures for, Federal terrorism preparedness grant programs into one office.[92] Fourth, it recommended the development of nationally recognized standards for equipment and training, with the ultimate objective of providing official certification.[93]

Figure 1: DHS Organizational Structure



In response to these and other recommendations – and particularly to the September 2001 attacks in New York City and Washington – the Department of Homeland Security was created. It has three broad objectives. As outlined in the White House's *National Strategy for Homeland Security*, they include preventing terrorist attacks within the United States, reducing America's vulnerability to terrorism, and responding to attacks and disasters that do occur.[94] As President George W. Bush noted upon signing the Homeland Security Act of 2002: "The new department will analyze threats, will guard our borders and airports, protect our critical infrastructure, and coordinate the response of our nation for future emergencies."[95] In order to meet these objectives, DHS is divided into five major directorates, as illustrated in Figure 1. The directorates include Border and Transportation Security, Emergency Preparedness and Response, Science and Technology, Information Analysis and Infrastructure Protection,

[89] *Implementing the National Strategy: 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* (Santa Monica, CA: RAND, December 2002), pp. iii-v, 42.
[90] *Fourth Annual* Report, p. iv; *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* (Santa Monica, CA: RAND, December 2001), p. 4.
[91] *Third Annual Report*, p. 10.
[92] *Third Annual Report*, pp. 8-9.
[93] *Toward a National Strategy for Combating Terrorism: Second Annual Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Santa Monica, CA: RAND, December 2000), p. xi.
[94] *National Strategy for Homeland Security*, p. vii. On DHS objectives also see the *Homeland Security Act of 2002*, p. 8; Bush, *The Department of Homeland Security*, p. 1.
[95] Remarks by the President at the Signing of H.R. 5005, the Homeland Security Act of 2002 (Washington, DC: Office of the Press Secretary, November 25, 2002).

and Management. Furthermore, DHS also includes several "stand-alone" agencies such as the Coast Guard, Secret Service, Bureau of Citizenship and Immigration Services, and Office of State and Local Government Coordination.

In addition to DHS, a number of other Federal departments and agencies have critical homeland security functions. For example, the Department of Defense established U.S. Northern Command in 2002 to conduct operations against threats aimed at the United States and its interests, as well as to provide military assistance to civil authorities through such components as the National Guard. The Central Intelligence Agency plays an important role in collecting intelligence abroad on terrorist threats to the United States and analyzing it in such bodies as the Counterterrorist Center (CTC). The Department of Justice has a number of important homeland security missions, ranging from the prosecution of terrorists to domestic counterterrorism and cyber security efforts by the FBI. In the Department of Health and Human Services, the Centers for Disease Control provide a system of health surveillance to monitor biological and radiological attacks, implement prevention strategies, and play a key role in protecting public health during and after an attack. Numerous other Federal agencies such as the Departments of Energy, Health and Human Services, and Agriculture, as well as State, local, and private sector entities, also have important homeland security functions. In short, this broad array of responsibilities makes it critical for DHS to coordinate homeland security strategies.

Analysis of DHS

This section examines four issue areas of DHS: information analysis, emergency preparedness and response, science and technology, and border and transportation security.

1. Information Analysis

One of the most important rationales for creating DHS was to help improve the coordination, analysis, and dissemination of intelligence information on terrorist threats and likely targets.[96] As numerous reports have pointed out, cooperation between departments of the Federal government, State and local government agencies, and private sector entities has clearly been inadequate.[97] For example, the *National Strategy for Homeland Security* argues: "Agencies at all levels of government have not always fully shared homeland security information due to real and perceived legal and cultural barriers, as well as the limitations of their information systems."[98] In response to this challenge and contrary to the Homeland Security Act, the Gilmore Commission's *Fourth Report* recommended that a stand-alone organization should be established outside of the FBI, CIA, or DHS to consolidate the analysis of information gathered in the U.S. and abroad on international terrorists and organizations threatening attacks against the United States.[99] This did not quite happen.

Instead, the Bush Administration created two major entities addressed here that involve DHS. The first is the Directorate of Information Analysis and Infrastructure Protection (IAIP) in DHS, which has a central

---

[96] As the Homeland Security Act of 2002 noted, the Directorate for Information Analysis and Infrastructure Protection has a stated mission "to access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal government, State and local government agencies, and private sector entities, and to integrate such information." *Homeland Security Act of 2002*, p. 12.

[97] *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001* (Washington, DC: U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, December 2002); Ivo H. Daalder et al, *Assessing the Department of Homeland Security* (Washington, DC: The Brookings Institution, July 2002), pp. 17-21; Gary Hart and Warren B. Rudman, *America – Still Unprepared, Still in Danger* (New York: Council on Foreign Relations, 2002), pp. 1-5; *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force* (New York: The Markle Foundation, October 2002), pp. 69-78.

[98] *National Strategy for Homeland Security*, p. 16.

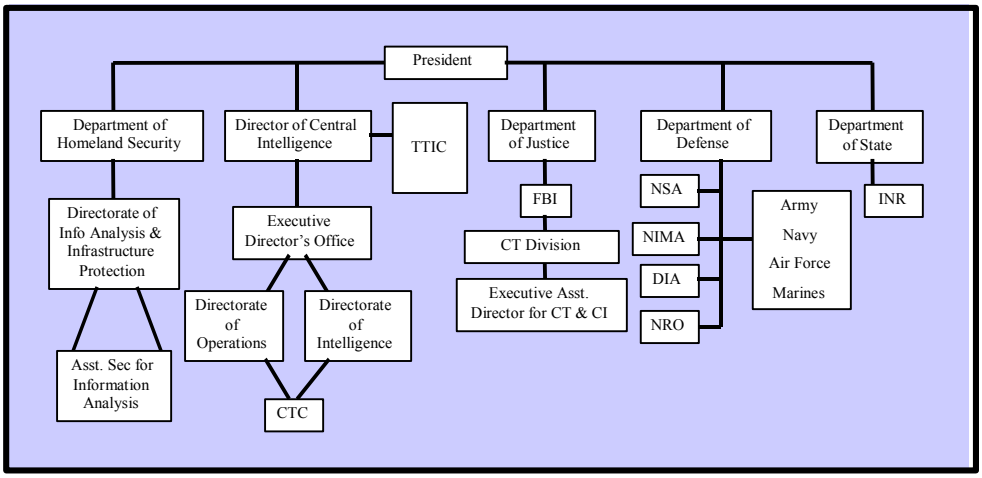
[99] *Implementing the National Strategy: The Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Santa Monica, CA: RAND, December 2002), pp. 41-50.

objective of coordinating and analyzing intelligence information about terrorist threats to the U.S., assessing vulnerabilities to U.S. infrastructure, and disseminating information to the private sector and relevant Federal, State, and local officials. It also includes providing terrorist threat warning through such formats as the color-coded Homeland Security Advisory System. The second entity is TTIC, which was created in May 2003 to coordinate and provide comprehensive terrorism-related threat analysis to the President, DHS, and other Federal agencies.[100] President Bush noted that TTIC was established to "integrate and analyze all terrorist threat information, collected domestically and abroad in a single location … When the center is fully operational, it will fully house a database of known and suspected terrorists that officials across the country will be able to access and act upon."[101] TTIC is staffed by representatives that have been assigned from the CIA, NSA, Federal Bureau of Investigation, and the Departments of Homeland Security, Defense, and State.

On a purely statutory level, the Director for Central Intelligence (DCI) oversees TTIC, though it is legally not part of the CIA. However, in practice the distinction is much less clear. The CIA wields a preponderant amount of influence in the center. TTIC is currently located at CIA Headquarters, though there have been some indications that it could move to the neighboring area of Tyson's Corner, VA, and it is funded through the CIA's budget.[102] Indeed, the logic for giving the DCI, rather than DHS or the Department of Justice, authority over TTIC was that the CIA is considered to have the most competent terrorism analysis capabilities. Some argued that it would be most efficient to have a single agency – the CIA – oversee offensive capabilities such as penetrating terrorist organizations and attacking them through preemptive strikes, as well as defensive capabilities such as analyzing threats and vulnerabilities to the U.S. homeland.[103] The need for a center capable of consolidating intelligence from across the intelligence community is critical for homeland security.

What are the main challenges with the current DHS and intelligence structures? Interagency intelligence cooperation has improved somewhat over the past two years. As Figure 2 illustrates, however, there are still a plethora of government departments and agencies that collect, analyze, and disseminate domestic and foreign intelligence information, and indeed there is a strong argument that there needs to be. However, this complicates coordination and has had a detrimental affect on DHS. There are several main challenges with the current structure.

Figure 2: Primary Agencies Analyzing Terrorist-Related Intelligence[104]



[100] On TTIC see *Fact Sheet: Strengthening Intelligence to Better Protect America* (Washington, DC: The White House, January 2003); John O. Brennan, "The Terrorist Threat Integration Center and Its Relationship with the Departments of Justice and Homeland Security," House of Representatives Committee on the Judiciary and the House of Representatives Select Committee on Homeland Security, July 22, 2003.
[101] George W. Bush, "New Terrorist Threat Integration Center," Speech at the FBI, February 14, 2003.
[102] William New, "Key House Chairman Backs Secret Anti-Terrorism Center," *GovExec.com*, October 8, 2003.
[103] Interview with senior intelligence officials, August 6, 2003 and August 13, 2003.

First, the Department of Homeland Security – and IAIP in particular – has largely been sidelined regarding the analysis and even dissemination of terrorism-related intelligence. DHS has a primary responsibility of protecting the U.S. homeland from terrorist attacks, but little power and capability to do this. To begin with, IAIP does not have significant analytical power. In theory, the *Homeland Security Act of 2002* gives DHS substantial responsibility "to access, receive, and analyze law enforcement information, intelligence information, and other information" collected at home and abroad to identify and assess terrorist threats to the homeland and potential domestic vulnerabilities.[105] In practice, however, the creation of TTIC gives the CIA the *de facto* responsibility for sifting through and analyzing raw terrorist intelligence information on threats to the homeland. This has largely sidelined DHS and left it with a paucity of competent intelligence analysts, while intelligence professionals have been much more willing to go to the CIA or Departments of Justice, Defense, or State.[106] Despite the existence of some analysts, DHS has also been crippled by a number of other problems such as installing secure SIPRNET lines to send and receive classified information.

Interviews with State and local officials have indicated that DHS has not effectively shared threat information with appropriate State and local entities. Indeed, DHS has had significant competition from other Federal agencies in disseminating information to State and local authorities, the private sector, and other areas, despite President Bush's July 2003 Executive Order giving the Secretary of Homeland Security primary authority for sharing homeland security information.[107] Some of these problems may be due to overlapping responsibilities. For example, the FBI is responsible for sharing intelligence information with State and local law enforcement through its Joint Terrorism Task Forces, but has also disseminated information to other actors such as State and local governments. Other problems may be the result of proactive efforts by State and local governments. Senior intelligence officials have told the Gilmore Commission that there has been some intelligence sharing between the CIA and State and local actors, often at the initiation of State and local entities.[108] These conclusions are supported by other studies. For example, a recent GAO study argued that while organizations such as DHS have initiatives under way to improve information-sharing, they have not been sufficient: "Information on threats, methods, and techniques of terrorists is not routinely shared; and the information that is shared is not perceived as timely, accurate, or relevant. Moreover, Federal officials have not yet established comprehensive processes and procedures to promote sharing."[109]

Second, there have been several problems with giving the CIA *de facto* authority over the TTIC. Perhaps the most significant is cultural. The CIA has developed an effective culture for collecting and analyzing intelligence information on terrorist threats, penetrating foreign organizations and governments, and conducting covert attacks. The CIA's *raison d'être* necessitates dealing with unsavory characters, protecting sources and methods used to gather information, keeping a close hold on intelligence, and conducting foreign intelligence gathering and operations. Consequently, it has rigid standards for employment such as requiring prospective employees to take a polygraph examination, and it is deeply reluctant to share information. This culture is at odds with what is needed for homeland security, and further raises concerns about the CIA's influence in domestic matters.[110] As several studies have noted, an effective homeland security model requires analyzing intelligence from domestic and foreign sources and

---

[104] Senate Governmental Affairs Committee, February 26, 2003.
[105] *Homeland Security Act of 2002*, p. 11.
[106] John Mintz, "At Homeland Security, Doubts Arise Over Intelligence," *Washington Post*, July 21, 2003, p. A12; Edward Alden, "U.S. Fails to 'Connect the Dots' By Pooling Its Terrorist Watch Lists," *Financial Times*, July 16, 2003, p. 7; "September 11 and Today," *Christian Science Monitor*, July 29, 2003, p. 10.
[107] George W. Bush, *Executive Order: Homeland Security Information Sharing* (Washington: White House Office of the Press Secretary, July 29, 2003).
[108] Interview with senior intelligence official, August 6, 2003.
[109] *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*, GAO-03-760 (Washington: United States Government Accounting Office, August 2003).
[110] Dan Eggen, "Center to Assess Terrorist Threat," *Washington Post*, May 1, 2003, p. A10; Robert Bryant, John Hamre, John Lawn, John MacGaffin, Howard Shapiro, and Jeffrey Smith, "America Needs More Spies – Intelligence and Security" *Economist*, July 12, 2003.

quickly disseminating it to relevant State and local actors and the private sector.[111] To be clear, there is little concern that information hasn't been – or won't be – shared if there is a specific and unambiguous threat about an attack in the United States. But there is anxiety that important information will not be shared efficiently with relevant State, local, private sector, and health entities in most other instances when the threat is more ambiguous but potentially just as serious.

In sum, the current DHS and intelligence structure has modestly improved coordination among Federal departments and agencies. While it is too early to make definitive conclusions, placing much of the power of collecting and analyzing homeland security threats in an agency that is primarily geared toward maintaining secrecy and focusing on foreign threats and operations may compromise homeland security. The current structure also unnecessarily complicates Federal communication with State and local actors and the private sector, sidelines the newly-created DHS, and largely duplicates what the CIA already has in its CTC.

Consequently, several steps can be taken. First, DHS should establish comprehensive procedures for coordinating with entities such as the FBI and CIA to share information with relevant State and local officials. While it is unlikely that DHS will have significant analytical capabilities in the near future, its primary intelligence role at the present should be as the focal point between States, locals, the private sector, and the intelligence community. Second, the United States Congress should consider transitioning TTIC from the DCI to DHS, or ensure its existence as a stand-alone agency separate from the CIA and responsible directly to the President. The Gilmore Commission laid out the logic for a stand-alone agency in its *Fourth Annual Report*. Moreover, DHS, which is supposed to be the hub of all homeland security efforts, is also a logical place where the fusion of terrorist analysis should take place.[112] Indeed, agencies within DHS have the central responsibility to act on intelligence to perform such important missions as protecting borders, screening airline passengers, securing critical infrastructure, and disseminating information to State and locals.

Recommendation: DHS has largely been sidelined regarding terrorist-related intelligence information. It has little analytical power and insufficiently developed capabilities to disseminate information to State, local, and private actors. **We recommend that DHS establish comprehensive procedures for sharing information with relevant State and local officials, and that the U.S. Congress consider either 1) transitioning TTIC from the DCI to DHS or 2) establishing it as an independent agency in the near future.**

2. Preparedness and Response

In order to improve the U.S.'s ability to prepare for and respond to future terrorist attacks and other major disasters, DHS took several steps. The first was to establish a Directorate for Emergency Preparedness and Response (EP&R), which primarily integrates the Federal Emergency Management Agency into the department. Its primary tasks include improving the U.S.'s preparation for, response to, and recovery from natural disasters and terrorist incidents, as well as developing and managing a national training and evaluation system to design curriculums, set standards, and evaluate local, State, and Federal training effort.[113]

The second step was to integrate the Office for Domestic Preparedness (ODP), formerly in the Department of Justice, into DHS's Directorate of Border and Transportation Security. ODP's primary

[111] Bruce Berkowitz, "A Fresh Start Against Terror," *New York Times*, August 4, 2003; Siobhan Gorman, "FBI, CIA Remain Worlds Apart," *National Journal*, August 1, 2003.
[112] On moving TTIC to DHS see James B. Steinberg, Hearing of the Senate Governmental Affairs Committee, February 14, 2003; Berkowitz, "A Fresh Start Against Terror"; *Protecting America's Freedom in the Information Age*, pp. 71-72; Joseph Lieberman, "Lieberman Hails Intelligence Analysis Center As Necessary; Says it Belongs in Homeland Security Department, Not CIA," Press Statement (Washington, DC: Senate Committee on Governmental Affairs, January 29, 2003).
[113] *Homeland Security Act of 2002*, pp. 78-79.

objectives are similar to those of the Directorate of Emergency Preparedness and Response, though the *Homeland Security Act of 2002* gives ODP "primary responsibility" for preparedness for terrorist attacks. ODP tasks include providing State and local governments and first responders with grants, training, and technical assistance to improve their readiness for terrorism incidents.[114] One of ODP's principle vehicles for doing this is through the National Domestic Preparedness Consortium, which consists of several training centers such as the Center for Domestic Preparedness and Texas A&M University's National Emergency Response and Rescue Training Center. The third step was to establish the Office of State and Local Government coordination as a stand-alone agency within the department to coordinate activities with State and local governments, assess their needs, and provide them with information, research, and technical support.[115]

What are the main challenges with the current DHS structure in improving preparedness and response to terrorist and other major disasters? The current structure suffers from a duplication of preparedness efforts and a lack of coordination among relevant entities.[116] ODP, which is located in the Directorate of Border and Transportation Security, issues grants to State and local first responders and offers terrorism preparedness training courses through the National Domestic Preparedness Consortium. The Directorate of Emergency Preparedness and Response (EP&R) issues some grants directly to State and local fire departments and offers training through such facilities as the Emergency Management Institute and the Noble Training Center. The Office of State and Local Government Coordination is the principal liaison to State and local officials, but does not administer grant programs.[117] As Figures 3 and 4 illustrates, there are several entities within DHS and the Federal government that have overlapping responsibilities for training and assistance.

Figure 3: Federal All-Hazards Assistance, 2003

	ODP (DHS)	EP&R (DHS)	Department of Health and Human Services (DHHS)	Department of Energy (DOE)
Training centers	Center for Domestic Preparedness NMIMT Texas A&M LSU	Emergency Management Institute National Fire Academy Noble Training Center	Centers for Public Health Preparedness	Nevada Test Site
Grants and Aid	State and Local Terrorism Prevention Grants Domestic Preparedness Equipment Grants Urban Area Security Initiative Funds Byrne Formula Grant s Local Law Enforcement Block Grants Program	Assistance to Firefighters Grants[118] Hazard Mitigation Grants Emergency Management Preparedness and Assistance Grants	Cooperative Agreement on Public Health Preparedness and Response for Bioterrorism Hospital Bioterrorism Preparedness Program Bioterrorism Training and Curriculum Development Emergency Medical Services for Children Trauma / Emergency Medical Services	Transportation Emergency Preparedness Program

Figure 4: Federal All-Hazards Training Courses, 2003[119]

	ODP / BTS (DHS)	EP&R (DHS)	DHHS	DOE	DoD	DOJ	DOT	EPA
Courses	53	61	2	40	9	2	6	3

[114] *Homeland Security Act of 2002*, pp. 57-58.
[115] *Homeland Security Act of 2002*, pp. 86-87.
[116] See U.S. Representatives John Sweeney and Jo Ann Emerson's comments, Hearing on FY2004 Emergency Preparedness and Response Directorate, House Appropriations Committee, April 30, 2003;
[117] John M. Doyle, "Ridge Says DHS Working to Change First-Responder Funding Formula," *Aviation Week's Homeland Security and Defense*, Vol. 2, No. 19, May 7, 2003, p. 4.
[118] Will likely be shifted to ODP in FY2004.
[119] *Compendium of Federal Terrorism Training:For State and Local Audiences* (Washington, DC: FEMA, 2003).

One of the major arguments for not consolidating these disparate entities is that preparedness efforts for natural disasters and terrorist attacks should be separated.[120] The logic is that they are distinct incidents and require different types of training, equipment, and strategy. Combining them would compromise both efforts. However, this logic is problematic, and the differences between terrorist attacks and natural disasters are not always clear-cut.[121] First, terrorist attacks can include a plethora of different incidents, ranging from conventional attacks like the September 2001 incidents in Washington and New York to biological, chemical, radiological, and nuclear attacks. Consequently, it is difficult to see the logic behind consolidating the training for incidents as different as chemical and biological attacks, but separating training for chemical spills and chemical attacks that are in many ways identical. Second, a number of well-respected training centers such as the Center for Domestic Preparedness currently teach preparedness for natural disasters and terrorist attacks. For instance, in 2003 the CDP taught such classes as "WMD Advanced Hazardous Materials Technician Training," which prepares hazard material technicians for both terrorist and HAZMAT incidents. Indeed, it is possible for training centers to teach a plethora of different types of classes to emergency responders. Third, since terrorist attacks are low probability events, an all-hazards approach to response and preparedness seems sensible in order to increase the utility of first responders by improving their preparedness for multiple types of events. After all, first responders will be the same for all types of events, and preparedness efforts are in many ways similar for incidents such as conventional terrorist attacks and natural disasters such as earthquakes.[122]

As U.S. Representative James Langevin noted in June 2003: "I am perplexed, along with many of my colleagues, about the apparently overlapping roles of the EP&R Directorate and the Office for Domestic Preparedness. This division … looks like a recipe for duplication of efforts – or worse, crucial tasks falling through the cracks. In addition, it seems to be breeding unnecessary confusion at the State and local level, as the very time we should be ensuring a clear direction and streamlined system for information-sharing, technical guidance, and funding assistance."[123] In addition to the Gilmore Commission, a number of reports have noted the redundancy of Federal preparedness efforts and the need for greater Federal coordination.[124] Indeed, the creation of DHS was supposed to eliminate these redundancies.

In the April 2003 *Semiannual Report to the Congress on the Department of Homeland Security*, the Office of Inspector General argues that placing planning, training, and equipment purchases for emergency management personnel in different DHS directorates creates problems with interdepartmental coordination, performance accountability, and fiscal accountability.[125] There are at least two other costs of not consolidating and coordinating preparedness efforts: confusion among State and local officials, and the absence of agreed-upon training standards. State and locals should have a one-stop clearinghouse for grants, training programs, and other types of terrorist and disaster preparedness assistance. The multiplicity of programs continues to lead to confusion at the State and local levels and makes it difficult

[120] Interview with Andrew T. Mitchell, Office for Domestic Preparedness, August 2002.
[121] There are several differences between terrorist attacks and natural disasters, but these don't outweigh the sensibility in combining them within the same directorate. For example, terrorist attacks have a prevention and prosecutorial component that do not exist for natural disasters.
[122] Additionally, we should also not rule out the possibility of terrorists using natural disasters as triggering events for attacks on first responders.
[123] U.S. Representative James Langevin, Hearing on Response to Terrorism: How is DHS Improving Our Capabilities? House Select Homeland Security Committee, June 19, 2003.
[124] See, for example, Amy E. Smithson and Leslie-Anne Levy, *Ataxia: The Chemical and Biological Terrorism Threat and the U.S. Response*, Report No. 35 (Washington, DC: The Henry L. Stimson Center, October 2000), p. 154; Richard A. Falkenrath, "Problems of Preparedness: U.S. Readiness for a Domestic Terrorist Attack," *International Security*, Vol. 25, No. 2, Spring 2001, pp. 147-186; *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822 (Washington, DC: U.S. General Accounting Office, September 2001); Daalder et al, *Assessing the Department of Homeland Security*, pp. vi, 21-24; *Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy*, GAO-02-549T (Washington, DC: U.S. General Accounting Office, March 2002).
[125] *Department of Homeland Security: Semiannual Report to the Congress* (Washington, DC: Office of Inspector General, April 2003), pp. 3-4.

for them to identify available Federal preparedness resources. Perhaps more seriously, the absence of coordinated preparedness efforts makes it difficult to develop training standards that are agreed upon and utilized by all relevant training centers. Are different training centers teaching the same preparedness and response methods for terrorist attacks and natural disasters? Are they providing adequate training for first responders? Individuals from both EP&R and ODP have acknowledged that there has been inadequate coordination between them.

Consequently, DHS should take at least three steps. First, it should consolidate responsibility for emergency response training, grants, and all-hazards assistance into one organization to ameliorate these drawbacks. It appears likely in 2004 that ODP will be moved to the DHS Office of State and Local Government to improve Federal assistance programs.[126] This may help consolidate existing grants by placing most in a single program, though some terrorism grants for incidents such as biological attacks will stay in other departments, such as Health and Human Services.[127] Unfortunately, this change does not adequately address terrorism and all-hazards training centers and courses, which will continue to suffer from insufficient unity of command and coordination. The logical and most efficient step would be to integrate natural disaster and terrorist training, grants, and other assistance into a single office. This could be done by integrating ODP and EP&R into one directorate, or perhaps at a minimum ensuring that training, grants, and other assistance were each consolidated into one office.

Second, DHS needs to develop a strategy for creating training standards for first responders. There have been some attempts to do this, such as ODP's *Emergency Responder Guidelines*, but these measures have been inadequate because the recommendations are not specific enough.[128] A good model might be the United States Army's Training and Evaluation Program (ARTEP). The ARTEP provides mission training plans and performance standards for active and reserve component commanders, staffs, units, and soldiers. It also describes the tasks each must be prepared to perform, the conditions under which they must be performed, and standards to which soldiers and units must perform their critical wartime missions.[129] These include essential tasks that soldiers should be able to perform, unit tasks for specific missions, and guidance to leaders and trainers for planning, preparing, executing, and evaluating training exercises. For example, a soldier in an infantry rifle platoon or squad should be able to assault a building, clear a trench line, and conduct an ambush, and his performance is monitored in measurable terms.[130] Consequently, in order to improve the preparedness of first responders and ensure they are receiving adequate training, DHS should develop comparable training plans for individual first responders such as police officers and firefighters, as well as definable units such as HAZMAT teams.

Recommendations:

Current DHS structure suffers from a duplication of emergency preparedness and response efforts. In particular, the existence of the Directorate of Emergency Preparedness and Response (EP&R) and the Office for Domestic Preparedness (ODP) in separate directorates is confusing for State and local officials and leads to problems with interdepartmental coordination, performance accountability, and fiscal accountability. **We recommend that DHS consolidate emergency response training, grants, and all-hazards assistance to ameliorate these drawbacks.**

There are still no agreed-upon standards for training first responders. This is primarily a result of insufficient coordination within DHS regarding preparedness efforts. A good model for DHS to consider

[126] See, for example, James Jay Carafano, "Fixing the Homeland Security Appropriations Bill," *Heritage Foundation Executive Memorandum*, No. 891, July 9, 2003; Michael Scardaville, "Adding Flexibility and Purpose to Domestic Preparedness Grant Programs," *Heritage Foundation Reports*, No. 1652, May 6, 2003.
[127] The retention of certain agencies such as HHS for public health responsibilities is probably necessary, but is not examined in this analysis.
[128] *Emergency Responder Guidelines* (Washington, DC: Office for Domestic Preparedness, 2002).
[129] See, for example, *Mission Training Plan for the Stryker Brigade Combat Team Infantry Rifle Platoon and Squad*, ARTEP 7-5-MTP (Fort Benning, GA: TRADOC, May 2003); *Mission Training Plan for the Military Intelligence Company (Armored Cavalry Regiment)*, ARTEP 34-114-30-MTP (Washington, DC: Headquarters, Department of the Army, December 2002).
[130] *Mission Training Plan for the Stryker Brigade Combat Team Infantry Rifle Platoon and Squad*, pp. 2-2 and 2-3.

is the United States Army's Training and Evaluation Program (ARTEP), which outlines essential tasks that must be prepared for, the conditions under which they must be performed, and the standards that must be met in their performance.[131] **We recommend that DHS develop a strategy for establishing training standards for first responders that outlines the tasks, conditions and standards of performance for individuals and units.**

3. Science and Technology

The absence of interoperable communications and equipment standards has been singled out as a serious problem in preparedness and response to terrorist attacks, including the response to the September 2001 attacks in Washington and New York City.[132] As a FEMA report concluded: "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."[133]

In order to help rectify this problem, DHS has several responsibilities. First, as outlined in the *Homeland Security Act of 2002*, the Directorate of Emergency Preparedness and Response was tasked with creating "comprehensive programs for developing interoperative communications technology, and helping to ensure that emergency response providers acquire such technology."[134] The *National Strategy for Homeland Security* similarly argues that one of the most important EP&R initiatives should be to "enable seamless communication among all responders."[135] Second, the Directorate of Science and Technology, which is in charge of research and development efforts and priorities in support of DHS missions, also plays an important role in developing standards. As noted in a May 2003 MOU, the Directorate of Science and Technology and the Department of Commerce's Technology Administration agreed to oversee "the development of standards" in order to establish the "successful development, testing, evaluation, and deployment" of critical technological tools to protect the homeland.[136]

What are the main challenges with DHS's structure and strategy for improving communications and equipment standards? There are several. To begin with, there continues to be a notable vacuum in authority for establishing at least minimal communication and equipment standards for emergency responders. As Figure 5 highlights, there are at least six Federal departments – the Departments of Homeland Security, Health and Human Services, Labor, Commerce, Defense, and Justice – and a number of interagency and independent organizations that develop homeland security-related communication and equipment standards.[137] Coordination is generally subpar, despite the existence of such groups as the Interagency Board for Equipment Standardization and InterOperability. This situation creates several problems.

[131] This does not mean directly transferring the ARTEP template to homeland security preparedness efforts. Rather, it means incorporating ARTEP's basic framework, including the development of standards by a central authority and the monitoring and enforcement of those standards to ensure that they are upheld.
[132] *After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon* (San Diego: Titan Systems Corporation, 2002); *Increasing FDNY's Preparedness* (New York: McKinsey & Company, 2002); Hart and Rudman, *America – Still Unprepared, Still in Danger*, p. 14.
[133] *A Nation Prepared: Federal Emergency Management Agency Strategic Plan, Fiscal Years 2003-2008* (Washington, DC: FEMA, 2002), p. 3.
[134] *Homeland Security Act of 2002*, p. 79.
[135] *National Strategy for Homeland Security*, p. x.
[136] Memorandum of Understanding between the Directorate of Science and Technology, U.S. Department of Homeland Security, and the Technology Administration, National Institute of Standards and Technology, U.S. Department of Commerce, May 2003.
[137] Note that such standard setting bodies and NIST, NTIA, OSHA, and NIOSH reside within these agencies.

Figure 5: Organizations that Develop Homeland Security Standards and Guidelines

Organization	Affiliation	Tasks
Directorate of Emergency Preparedness and Response (EP&R)	Department of Homeland Security	Establishes standards – including those with respect to the Nuclear Incident Response Team – and certifies when those standards have been met.
Directorate of Science and Technology (S&T)	Department of Homeland Security	Develops standards in conjunction with other offices such as Commerce's Technology Administration.
National Institute for Occupational Safety and Health (NIOSH)	Department of Health and Human Services	Conducts research and suggests standards to reduce injuries and illnesses among workers in high-priority areas and high-risk sectors. Provides workers, employers, and the public with information and training to prevent occupational injuries and illnesses.
Occupational Safety and Health Administration (OSHA)	Department of Labor	Establishes protective standards, works to enforce them, and offers technical assistance and consultation programs to employers and employees throughout the country.
National Institute of Standards and Technology (NIST)	Department of Commerce	Develops and promotes measurement, standards, and technology to enhance productivity.
National Telecommunications and Information Administration (NTIA)	Department of Commerce	Advises executive branch on domestic and international telecommunications and information technology issues, including standards.
National Institute of Justice (NIJ)	Department of Justice	Publishes and identifies research reports, guides, and other documents for practitioners, policymakers, and researchers interested in communications interoperability and information sharing.
Technical Support Working Group (TSWG)	Department of Defense	Develops guidelines for first responders to assist in the selection of detectors, personal protective equipment, and communications equipment for terrorist incidents.
Interagency Board for Equipment Standardization and InterOperability (IAB)	Departments of Justice and Defense	Publishes a standardized equipment list and promotes interoperability among civil and military WMD response units at local, State, and Federal levels.
Federal Communications Commission	Independent government agency	Regulates interstate and international communications by radio, television, wire, satellite, and cable.
National Fire Protection Association (NFPA)	Private organization	Develops and advocates scientifically-based consensus codes and standards, research, training, and education to reduce the global burden of fire and other hazards.
International Organization for Standardization (ISO)	Private organization	Develops voluntary technical standards for businesses across the globe.
Telecommunications Industry Association (TIA)	Private organization	Develops standards and facilitates the convergence of new communications networks.
American National Standards Institute (ANSI)	Private organization	Promotes and facilitates voluntary standards and conformity assessment systems for U.S. private sector.

First, there is confusion among State and local officials about what equipment to buy. For example, in 2002 the State of Indiana purchased 16,000 gas masks at a cost of $650,000 for police, firefighters, and emergency medical personnel. However, the masks were constructed of silicone, which chemical agents such as mustard gas can penetrate in a few minutes. A better – though more expensive – option would have been to purchase butyl rubber masks, which provide emergency responders with far better protection[138] Without a centralized information source for equipment and communications standards, State and local entities may purchase the wrong – or at least subpar – equipment and unnecessarily jeopardize the safety of emergency responders. As some studies have noted, this can also include the entire personal protective equipment (PPE) ensemble. Examples include incompatibility problems that have led to gaps between the face opening in chemical protective hoods and the self-contained breathing apparatus (SCBA) mask. Some first responders have complained that the SCBA tank can interfere with the rear brim of the helmet and limit movement – or even knock the helmet off.[139] The concern about the

[138] Karen Hensel, "Mask Confusion," Investigative Report for WISH-TV, Indianapolis; "State Officials Consider Replacing Thousands of New Gas Masks," *Associated Press*, February 17, 2003.
[139] Tom LaTourrette et al, *Protecting Emergency Responders: Community Views of Safety and Health Risks and Personal Protection Needs* , Vol. 2 (Santa Monica, CA: RAND, 2003), pp. 25-41.

absence of standards and confusion among State and local entities has been noted by the Gilmore Commission in the past, and these are critical issues that need immediate attention.[140]

Second, the absence of common standards increases the likelihood that departments will use incompatible communication systems and equipment, which may affect interoperability at the scene of major incidents. This problem can exist among local departments, among departments in neighboring jurisdictions, and between municipal departments and State or Federal agencies. For example, a common concern about respirator systems is that in the absence of even minimum performance standards, they are constructed by different manufacturers and have different fittings. This can create notable problems during extended emergencies as responders spend time trying to match up respirator parts such as air tanks and canisters with breathing devices, particularly if supplies are brought in from neighboring jurisdictions, Federal caches, or manufacturers.[141]

In sum, DHS can play an important role by compiling standards for equipment and communication systems, and acting as the centralized information source for State and local entities and the private sector. As the Gilmore Commission noted in its *Second Annual Report*, a single Federal office should "coordinate the development of nationally recognized standards for equipment, training, and laboratory protocols and techniques, with the ultimate objective being official certification."[142] In addition to compiling information, DHS could coordinate the assessment, testing, and certification of equipment from PPE to radios, cooperate with Federal agencies and the private sector, publish the results annually, and make them available on the internet for easy access. Some might respond that this should not be a Federal responsibility. But since interoperability and standardization problems are not being addressed by State and local entities, the most logical option is to pursue change through a top-down process led by DHS.

Recommendation: There are at least six Federal departments and a number of interagency and independent organizations that are involved in developing standards for communication systems and equipment. This situation makes it difficult for States and locals to know what to buy and increases the possibility of incompatible equipment. **We recommend that DHS compile and coordinate the development of standards for homeland security related equipment and communications systems, and become the single Federal government point of contact for information on technical standards for State and local entities and the private sector.**

4. Border and Transportation Security

Over the last century, the security of the United States has been facilitated by friendly and cooperative relations with Canada and Mexico to its north and south, and two vast oceans to its east and west. However, this sense of security has changed. Terrorists, their infrastructure, and other individuals have attempted to penetrate America's borders through various ports of entry such as seaports, coastlines, airports, highways, railroads, and waterways. Within DHS, border and transportation security includes a number of Federal agencies such as the United States Customs Service, the enforcement division of the Immigration and Naturalization Service, and the Transportation Security Administration. The primary focus here will be on the United States Coast Guard for several reasons. To begin with, the Coast Guard plays a critical border and transportation role as the lead Federal agency for maritime security. Furthermore, since some of its homeland security functions such as patrolling ports and coastlines have

[140] Note that failure to act quickly affects both the safety of responders and the fiscal position of State and local governments. Reality dictates that jurisdictions must purchase needed equipment for their first responders as soon as is possible. The failure of the Federal government to publish information about, and standards for, such equipment makes very real the possibility that substandard or incompatible equipment will be purchased. Jurisdictions will then have to either expend large sums to repurchase this substandard or incompatible equipment, or more likely live with it until some later date when it needs to be replaced. This is, therefore, an effort that must be tackled promptly and with vigor.

[141] Jackson et al, Protecting Emergency Responders, pp. 23-24.

[142] *Second Annual Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Santa Monica, CA: RAND, December 2000), p. xi.

been enhanced since September 2001, it offers a useful test case of how well Federal agencies are balancing their resources. However, as the last segment of this section illustrates, the issue of balancing resource allocation to "new" and "traditional" missions is relevant for a number of important homeland security functions such as cargo security and public health.

The Coast Guard has two primary sets of missions. First, its *homeland security* missions include patrolling ports, waterways, and coastlines; conducting drug and illegal migrant interdiction; performing military operations for the Department of Defense and sustaining military readiness; and conducting other law enforcement tasks such as eliminating illegal encroachment by foreign fishing vessels. These missions also include Marine Transportation Act of 2002 (MTSA) objectives such as performing port threat and vulnerability assessments.[143] Second, the Coast Guard's *non-homeland security* missions include protecting marine safety; conducting search and rescue operations; providing navigation assistance in ports and waterways; enforcing the protection of living marine resources; eliminating garbage, oil, and plastics that have been discharged into the water; and providing icebreaking capability in polar regions.[144] Both sets of missions are critical. As the *Homeland Security Act of 2002* argues, the Coast Guard is expected to maintain all of its core missions: "The authorities, functions, and capabilities of the Coast Guard to perform its missions shall be maintained intact and without significant reduction after the transfer of the Coast Guard to the Department [of Homeland Security]."[145]

What are the Coast Guard's main homeland security challenges? One of the primary challenges for the Coast Guard has been balancing its missions. Specifically, while it has put significant resources into some homeland security missions and performed U.S. military operations in Afghanistan and Iraq, it has decreased resources for important homeland security missions such as drug interdiction.[146] This is particularly troublesome since there is often a nexus between terrorist and drug-trafficking organizations. Furthermore, the Coast Guard's integration into DHS has changed its priorities and working parameters, and in some cases pulled it away from critical missions. As an April 2003 GAO report concluded:

> The emphasis the Coast Guard placed on security after September 11th has had varying effects on its level of effort among all of its missions … The most current available data show that some security-related missions, such as migrant interdiction and coastal security, have grown significantly since September 11th … However, the level of effort for other missions, most notably the interdiction of illegal drugs and fisheries enforcement, is substantially below pre-September 11th levels.[147]

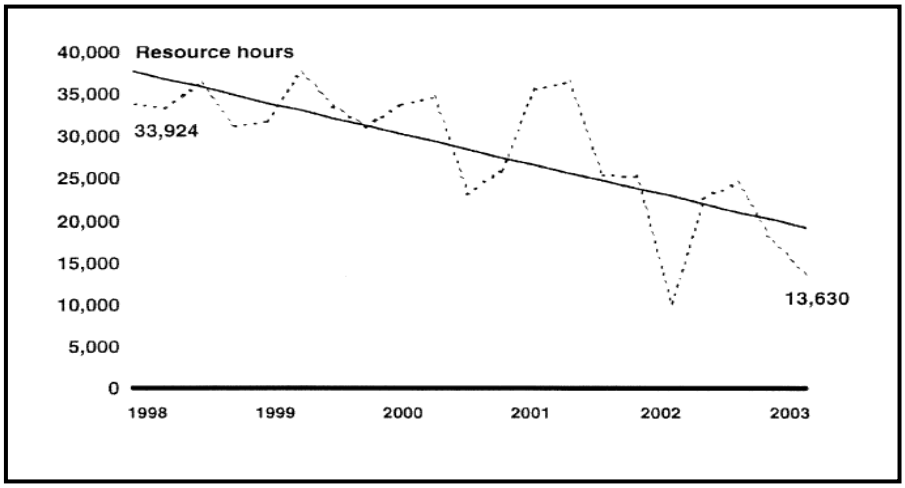
Following the September 2001 attacks, most Coast Guard cutters previously conducting offshore patrols for fisheries law enforcement and drug and migrant interdiction were ordered to patrol the entrances to such major ports as Boston, San Francisco, New York, and Miami. Smaller patrol boats and motorboats, which had been utilized for missions such as fisheries patrol, were used to conduct security patrols within port facilities.[148] Furthermore, Coast Guard resources have been used for the U.S. wars in Afghanistan

[143] *Maritime Transportation Security Act of 2002*, Public Law 107-295 (Washington: Government Printing Office, November 25, 2003).
[144] *Homeland Security Act of 2002*, p. 115; *U.S. Coast Guard FY 2002 Report* (Washington, DC: U.S. Coast Guard, 2002).
[145] *Homeland Security Act of 2002*, p. 115.
[146] *Coast Guard: Strategy Needed for Setting and Monitoring Levels of Effort for All Missions*, GAO-03-155 (Washington, DC: Government Accounting Office, November 2002); Christopher Lee, "Traditional Coast Guard Duties Suffer," *Washington Post*, April 2, 2003, p. A15; Michael E. O'Hanlon, Hearing of the Senate Governmental Affairs Committee, March 20, 2003; Alex Fryer, "Anti-Terror Workload a Worry," *Seattle Times*, May 26, 2003, p. B1; Senator Patty Murray, Hearing of the Senate Appropriations Subcommittee on Homeland Security, May 1, 2003; Ronald O'Rourke, *Homeland Security: Coast Guard Operations – Background and Issues for Congress* (Washington, DC: Congressional Research Service, June 2003).
[147] *Coast Guard: Challenges During the Transition to the Department of Homeland Security*, GAO-03-534T(Washington, DC: Government Accounting Office, April 2003), p. 5
[148] *Coast Guard: Strategy Needed for Setting and Monitoring Levels of Effort for All Missions*, p. 8.

(Operation Enduring Freedom) and Iraq (Operation Iraqi Freedom).[149] One way to measure the Coast Guard's efforts is to examine its "resource hours." The Coast Guard maintains information about how cutters, patrol boats, and aircraft are used; each hour that resources are utilized for a mission is termed a "resource hour." An examination of Coast Guard resource hours over the last several years shows a significant decline in several areas, most notably drug interdiction and fisheries enforcement.

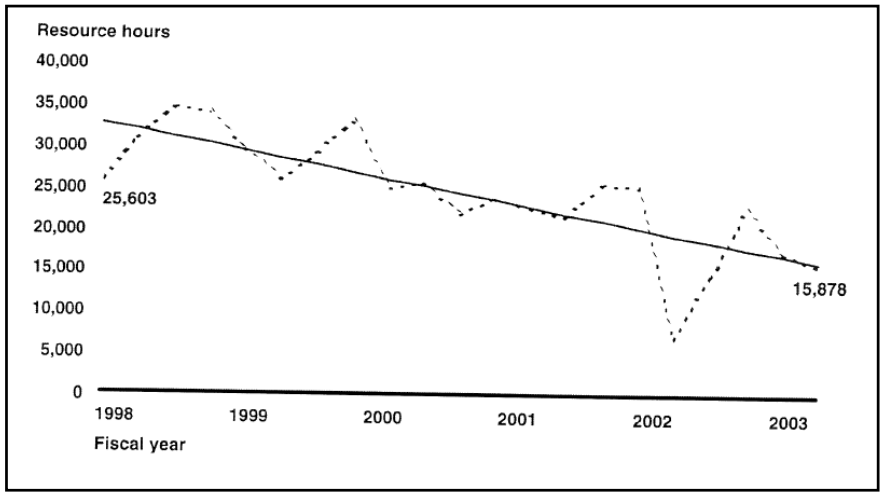
Specifically, the Coast Guard has substantially reduced its resources for drug interdiction, an important homeland security mission. Combating the flow of illegal drugs into the United States is a joint, interagency task, with contributions from the Department of Defense, the U.S. Customs Service, Coast Guard, and other Federal agencies. The Coast Guard is the lead Federal agency for maritime drug interdiction and shares lead responsibility for air interdiction with U.S. Customs, making it a critical U.S. government component. As Figure 6 illustrates, the Coast Guard's counterdrug efforts have dropped from approximately 35,000 resource hours at the end of 2000 to nearly 13,000 by 2003. For example, it has cut back on conducting counter-drug patrols in southern California and northern Mexico in order to pursue other homeland security missions such as port security.[150] This is a problem not only because drug interdiction by itself is an important homeland security and law enforcement mission of the United States, but because terrorist and drug-trafficking organizations are often intertwined. Such organizations as al-Qaeda, Hamas, Hizballah, and the Abu Sayyaf Group use drug trafficking to finance their operations. As Steven Casteel, Assistant Administrator for Intelligence at the Drug Enforcement Agency, recently argued: "Whether it is a State, such as formerly Taliban-controlled Afghanistan, or a narco-terrorist organization, such as the FARC, the nexus between drugs and terrorism is perilously evident."[151] Furthermore, fisheries enforcement includes protecting U.S. fishing grounds from foreign encroachment and enforcing domestic fishing laws and regulations through inspections and fishery patrols. As Figure 7 highlights, resource hours for fisheries enforcement have decreased from approximately 25,000 in 2001 to around 15,000 in 2003.

Figure 6: Resource Hours for Drug Interdiction[152]



[149] Rep. Harold Rogers, Hearing of the House Subcommittee on Homeland Security, April 10, 2003. On the Coast Guard's role in military operations see John Mintz and Vernon Loeb, "Coast Guard Fights to Retain War Role," *Washington Post*, August 31, 2003, p. A7.
[150] *Coast Guard: Strategy Needed for Setting and Monitoring Levels of Effort for All Missions*, p. 17.
[151] Steven W. Casteel, Statement Before the Senate Committee on the Judiciary, May 20, 2003.
[152] *Coast Guard: Challenges During the Transition to the Department of Homeland Security*, p. 11.

Figure 7: Resource Hours for Fisheries Enforcement[153]



The Coast Guard's challenges with balancing resources is also apparent in a number of other areas such as cargo security and public health. First, with respect to cargo security, DHS has struggled to balance the tasks of a) maximizing border security with b) ensuring that legitimate "low risk" cargo is cleared in a timely and efficient manner. Addressing this challenge falls principally to the Bureau of Customs and Border Protection (CBP) in DHS, which consists of the inspections component of the former U.S. Customs Service; the Border Patrol and Inspections component of the former Immigration and Naturalization Service; and the Animal and Plant Health Inspection Service, a former component of the U.S. Department of Agriculture. Indeed, CBP's increased antiterrorism efforts have not been met with adequate steps to speed up the movement of international commerce and travel coming into the United States.[154] This has potentially serious economic consequences. On the one hand, CBP plays a pivotal role in preventing high-risk, harmful cargo from coming into the country. On the other hand, it needs to do so in a timely manner because searching every cargo and traveler that enters the country would cripple the flow of legitimate trade and travel and would require an exorbitant resource commitment.

Second, the public health sector has struggled with balancing resources for homeland security and more traditional missions. This issue area comes mainly under the jurisdiction of the Department of Health and Human Services, though it is nonetheless a useful illustration of the trade-off dilemma. For example, some studies have noted that in the event of a large-scale infectious disease outbreak such as a bioterrorist attack involving anthrax or botulism, most hospitals would not have the capacity to accept and treat a sudden, large increase in the number of patients. They would not have sufficient medical equipment such as ventilators, personal protective equipment suits, or isolation beds.[155] However, meeting those needs presents hospitals with a trade-off. Since bioterrorism preparedness is expensive and attacks are low probability events, should hospitals redirect precious resources to create capacities that are not needed on a routine basis and may never be used? How do we measure this trade-off? The answers are not clear, and require further analysis of the costs and benefits of redirecting resources from traditional public health functions to new homeland security ones. Indeed, there have been concerns that the Federal smallpox vaccination program has diverted resources from such traditional public health activities as

[153] *Coast Guard: Challenges During the Transition to the Department of Homeland Security*, p. 11.
[154] *Homeland Security: Challenges Facing the Department of Homeland Security in Balancing its Border Security and Trade Facilitation Missions* (Washington, DC: Government Accounting Office, 2003).
[155] *Hospital Preparedness: Most Urban Hospitals Have Emergency Plans but Lack Certain Capacities for Bioterrorism Response* (Washington, DC: Government Accounting Office, 2003).

routine immunizations, health promotion, and screening.[156] It is conceivable that in some cases common resources could be utilized for both functions so that there is a dual-use benefit, but this will not always be an option.

In sum, DHS and other relevant government agencies need to think systematically about how they are balancing their resources, and what the costs and benefits are to redirecting resources away from traditional functions. For example, the Coast Guard has put significant resources into some missions such as port security and assisted in U.S. military operations in Afghanistan and Iraq, but it has decreased resources for important homeland security missions such as drug interdiction. This concern is also apparent in other areas such as cargo security and public health.

***Recommendation**:* Current DHS efforts have diminished and compromised important "traditional" missions of some component agencies. For example, the Coast Guard has put substantial resources into patrolling ports and assisting in U.S. military operations in Afghanistan and Iraq. But it has decreased resources for important homeland security missions such as drug interdiction. **We recommend that DHS conduct research to measure the effects of decreasing "traditional" missions of component agencies and adopting new missions related to homeland security.**

[156] Daniel J. Kuhles and David M. Ackman, "The Federal Smallpox Vaccination Program: Where Do We Go From Here?" *Health Affairs*, October 22, 2003; Andrea B. Staiti, Aaron Katz, and John F. Hoadley, "Has Bioterrorism Preparedness Improved Public Health?" Issue Brief, No. 65 (Washington, DC: Center for Studying Health System Change, July 2003); "Impact of Smallpox Vaccination Program on Local Public Health Services," Research Brief, No. 9 (Washington, DC: National Association of County and City Health Officials, February 2003).

APPENDIX H–DEVELOPING A STRATEGY FOR RESEARCH AND DEVELOPMENT IN THE DEPARTMENT OF HOMELAND SECURITY*

With the establishment of the Department of Homeland Security, protecting America from terrorism has become a top priority and permanent component of the Federal government. As such it represents a new force shaping the character of our national goals and activities. One very important responsibility of the Federal government, particularly since the end of World War II, has been to maintain a program of research and development in science, engineering, and technology. The justification for federally funded research and development is that public benefits exist that the private sector cannot capture (e.g., National Research Council, 2001a)[157]. This is clearly the case for many basic sciences, but also holds true for some more applied areas such as energy technologies and homeland security.

The Department of Homeland Security has a substantial research and development role. In its second year of funding, it has a research and development budget request of 1.0 billion dollars, giving it the eighth largest research and development budget among Federal departments and independent Federal research agencies (AAAS Intersociety Working Group, 2003). The vast majority of this funding is for homeland security-related work.[158] Eighty percent of this funding is for the Science and Technology Directorate, with most of the remainder in the Border and Transportation Security Directorate (AAAS Intersociety Working Group, 2003).

This sudden and large commitment of resources to a new mission[159] carries with it some important challenges. Chief among these challenges is for the Department of Homeland Security to organize and coordinate an effective research and development program amidst great uncertainty and across numerous operational needs. Moreover, DHS will have to contend with the challenges of implementing and coordinating research in an arena in which the organizations conducting research are almost entirely unrelated to the organizations that must implement the results of that research. Finally, Department of Homeland Security's research and development efforts will have to be developed mindful of the fact that substantial fractions of both the research and user communities largely are outside of the department.[160]

This appendix addresses the challenge of prioritizing and organizing research and development efforts funded and overseen by the Department of Homeland Security. It examines:

---

[157] This may result from the probability of achieving the anticipated benefits being too low to warrant industry investment, the expected duration between research and return of anticipated benefits being too long for industry to capture those investments, or the anticipated benefits being in a form that private industry does not value (e.g., environmental protection).

[158] Although 34 percent of the Department's total funding is for non-homeland security work, the majority of this funding is for the Emergency Preparedness and Response Directorate, the Secret Service, and non-homeland security-related work for the Coast Guard, which receive little or no research and development funding (U.S. Department of Homeland Security 2003a).

[159] Homeland security is currently not a formal functional are in the Federal government. Homeland security research and development spending is counted in the missions of defense, general science, agriculture, and transportation (AAAS Intersociety Working Group, 2003). As a result, there are no estimates of Federal research and development funds directed towards homeland security.

[160] The primary research performers include National Institutes of Health, Department of Energy and its national lab system, National Institute of Standards and Technology, Department of Defense, National Science Foundation, National Institute for Occupational Safety and Health, National Institute of Justice, Department of Agriculture, and Homeland Security Advanced Research Projects Agency. Only the last of these is in the Department of Homeland Security. The main users, on the other hand, are not primarily research and development agencies, and include Transportation Security Administration; Coast Guard; Federal Bureau of Investigation; Postal Service; private industry; and State and local emergency responders, emergency managers, and public health agencies (National Research Council, 2002).

*** Tom LaTourrette**

- Different ways to classify homeland security research and development
- Options for prioritizing research and development
- Likely challenges for research and development coordination and implementation
- Terrorism response standards.

For this discussion, we have in mind a comprehensive research and development program that includes activities directed at generating innovations in science and technology as well as the operational protocols, organizational structures, and standards that guide their application. While a primary goal is improving support to State and local authorities in the area of terrorism response, the report is intended to guide research and development in all areas of homeland security, such as information analysis, infrastructure protection, border and transportation security, and emergency preparedness and response.

This appendix is based on an examination of the literature concerning general principles of research and development prioritization, analyses of research and development prioritization in specific agencies and fields, and research and development in homeland security in particular. Project time and budget constraints limited the extent of the literature that could be reviewed. Because the amount of literature in the former two categories is extensive, only a sampling of such reports could be included. The findings in this report were developed primarily by examining general research and development policy principles in the context of homeland security.

Classifying Homeland Security Research and Development

Descriptions of Department of Homeland Security's research plans are not yet well-developed and general, and reflect significant flux in decisionmaking that is understandable given the early State of this new field (U.S. Department of Homeland Security, 2003b; Check, 2003).

Hence, an important first step in establishing research and development priorities for homeland security is to determine how to best classify research and development areas.. Classification of research and development helps define the scope of issues to be considered in the prioritization process. The way in which research and development areas are defined and classified also helps frame the research problems that need to be addressed.

Candidate areas for prioritization are often defined by the way an agency is organized, legislative mandate, or other means. Being new, the Department of Homeland Security does not have a well established suite of research and development areas among which to select priorities. Several classification schemes for homeland security research and development have been envisioned (e.g., President's Council of Advisors on Science and Technology, 2002; National Research Council, 2002; Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, 2000; U.S. Department of Homeland Security, 2003b). These include

- weapon type
- target type
- mission areas of constituent agencies
- phases of counterterrorism (e.g., intelligence, prevention, protection, response)
- technology area (e.g., sensors, computers, medicines, materials, communications)

as well as various combinations of these categories. The merits of different classification schemes can be examined in light of some particular characteristics of homeland security.

Perhaps the single most defining characteristic of homeland security is the great uncertainty surrounding the terrorist threat and how that threat may evolve. If threats evolve rapidly and in unpredictable ways, a

focus on weapon or target type may be restrictive and any chosen framework may not appropriately reflect the homeland security landscape in the future. Classification along these lines might therefore require frequent re-organization to stay current, which can be damaging to research and development efforts (National Research Council, 2000).

Another characteristic is the wide range of agency missions. While the mission of the Department of Homeland Security is focused on terrorism and natural disasters (Homeland Security Act of 2002), the missions of many of the 22 constituent agencies extend well beyond these areas. Classifying research and development according to agency mission would therefore be complicated by the need to account for these often disparate and possibly conflicting mission elements.

A classification according to phases of counterterrorism is attractive in some aspects: It would help insure that research and development addresses all aspects of counterterrorism efforts. It is also a relatively permanent construct that is not likely to evolve in the future.

A shortcoming of all of these schemes is that they are unique to homeland security and so do not naturally interface with the nation's existing research and development infrastructure. Homeland security must utilize the nation's existing research and development resources, such as national laboratories, university faculty, and in-house capabilities of Federal research agencies. These resources are all invested in a wide range of efforts and may not be able or willing to substantially retool themselves for homeland security; this is all the more apropos considering that most relevant research and development agencies remain outside the Department of Homeland Security and are therefore subject to minimal influence by the Department and its user agencies. The more homeland security is able to cast its research and development needs in more conventional research areas, the better able it will be to capitalize on the nation's excellent research and development capabilities. In this context, organizing homeland security research and development priorities around technology areas is attractive.

In practice, many research programs and projects pursued by the Department of Homeland Security will be derived from operational needs, in which case the organization of research areas will tend to emerge from the prioritization process itself. The resulting organization of homeland security research and development may therefore include a mix of dimensions. No arguments strongly support one scheme over another. However, the strengths and weaknesses of each should be considered by DHS decisionmakers in deliberations.

Prioritizing Homeland Security Research and Development

The Importance of Criteria

Much has been written about prioritizing research and development efforts (e.g., National Science Board, 2001; Bromley, 2003; National Research Council, 1998, 2000, 2002; Office of Technology Assessment, 1991; and many others). One of the most common critiques of existing approaches is a perceived lack of a clear methodology for priority setting and coordination. The resulting conclusion of nearly all such reports is that a strengthened process for research allocation decisions is needed. Without an explicit prioritization methodology, decisions can be based on undesirable factors such as faith in future payoffs, visibility and tenacity of proponent constituencies, or serendipity. As a result, such decisions can be difficult to defend and assess.

Efforts to systematize the prioritization process involve developing prioritization criteria. One of the strengths of such an approach stems from the observation that specific priorities can change dramatically and quickly, while criteria established for assessing priorities do not. Given the inherent uncertainties in assessing the terrorist threat, homeland security is particularly vulnerable to shifting priorities. This was

clearly demonstrated on September 11, 2001 and again after the anthrax attacks during the fall of 2001. The criteria established before these attacks remained largely valid and in general have much more stability and longevity than do the priorities derived from them (Bromley, 2003).

Another benefit of a criteria-driven approach is that it helps ensure that research and development activities are well-linked to the agency's or department's mission. In doing so, the criteria help keep research and development on target and provide accountability to the public (National Research Council, 1998).

Specific Criteria for Homeland Security R&D

Most discussions of criteria for prioritizing research and development in science and technology (e.g., National Science Board, 2001; Office of Technology Assessment, 1991; Bromley, 2003; National Research Council, 1998) call for three general elements to be considered: intrinsic merit, socioeconomic benefits, and programmatic concerns.

Intrinsic merit refers to such issues as objective and significance, breadth of interest, potential for new discoveries and understanding, and uniqueness. This criterion is relevant primarily to basic science and can usually be applied only at the individual project level. Socioeconomic benefits are the most generally applicable and include improvement of the human condition, economic and environmental benefits, and contribution to national pride and prestige. Programmatic concerns include the readiness of the research and development infrastructure to pursue the topic as well as the responsibility to develop and sustain a functioning infrastructure that is well-positioned to address a wide scope of topics.

With these general principles as a starting point, criteria for a research and development agenda under the auspices of the Department of Homeland Security can be developed by considering some important distinguishing characteristics of homeland security. These characteristics and their implications for designing prioritization criteria are described below.

A New Mission

The Department of Homeland Security is a new organization with a new mission. Because it represents a new research area, homeland security does not have a distinct or well-developed theoretical or empirical research base. Indeed, a major challenge for the Department of Homeland Security is to define the scope of research and generate a comprehensive, multi-disciplinary research portfolio that encompasses both basic and applied research. Consequently, the Department of Homeland Security must build upon existing basic research programs in other areas (Frist et el., 2002). In time, important basic research needs will undoubtedly emerge. In the mean time, however, homeland security research will need to concentrate on more downstream, or applied, research and development. This means that some criteria related to intrinsic merit, such as the potential for new discoveries and understanding, should initially be weighted less than socioeconomic and programmatic criteria.

An initial emphasis on applied research and development in the Department of Homeland Security has been affirmed by the Undersecretary for Science and Technology (Check, 2003). Such an emphasis has implications for which needs can be addressed now and which must await more basic research. For instance, many emergency responders have expressed a desire for broad-spectrum, real-time, and portable environmental sensors. They have also called for location monitoring technologies to help pinpoint trapped responders (LaTourrette et al,. 2003). Developing these technologies will require advances in basic research. In the meantime, applied research can be directed at achieving incremental improvements in existing technologies—such as making them more light-weight and easy to use.

Uncertainty

Another important characteristic of homeland security is the uncertainty that surrounds the terrorist threat and the difficulty in estimating how much this threat is mitigated with the introduction of new counter-measures. These uncertainties are problematic because estimates of the effectiveness of research and development conducted under the auspices of the Department of Homeland Security in preventing attacks or injuries require a baseline estimate of what attacks and injuries are expected to occur and what impact improved counter-measures or preventative efforts would have.

Because the uncertainty surrounding the terrorist threat (in terms of weapons, targets, severity, frequency) is so great, prioritizing research and development based on the type of threat it addresses is very difficult. One way to narrow the problem slightly is to assume that high attack frequencies cannot be sustained, because the mechanism would eventually be identified and intercepted. In this case priority would be given to research and development directed towards threats that have the potential to produce the greatest numbers of casualties in a given attack. A single biological or nuclear attack could realistically kill tens of thousands of people, while chemical, radiological, or conventional attacks are 10 to 1000 times less lethal (e.g., Davis et al., 2003). Therefore, on the basis of estimated casualties, research addressing biological and nuclear threats would receive priority.

However, given that other less catastrophic threats exist and have a greater probability of occurring, car bombs and suicide bombs, for example, research and development addressing other attack modes cannot be neglected. Thus an additional way to cope with the threat uncertainty is to make an effort to be comprehensive in terms of the spectrum of threats addressed in homeland security research.

The second uncertainty–estimating the effectiveness of a particular innovation in decreasing the frequency, magnitude, or impact of attacks–it somewhat more tractable. This uncertainty can be examined by considering the aspect of counterterrorism operations that a particular innovation would address. The effectiveness of a counterterrorism strategy will vary depending on the phase of counterterrorism activity it addresses or the target type it protects. For instance, for most threats, research aimed at improving attack prevention or interdiction has the potential to save many more lives than research addressing attack response. Thus, efforts to provide early warning of chemical or biological attacks by means of detectors, surveillance, and information sharing would receive priority over research on emergency responder protection and decontamination. Viewed in this context, some research and development efforts may emerge as particularly valuable and hence warrant high priority. Proposed innovations that address multiple threats, targets, or counterterrorism phases would warrant greater priority.

Risk Management

Another characteristic of the homeland security effort that can help shape how to think about prioritizing research and development in the Department of Homeland Security is the inherent objective of risk management. This approach is used by the Environmental Protection Agency, which has developed some criteria designed around this goal. Many of these criteria can be adapted to homeland security. A major difference between the challenges faced by environmental protection and homeland security, however, is that sources of environmental risks are generally more identifiable and their potential effects more quantifiable than terrorism risks. Nonetheless, for those terrorism risks that have been identified, the concept of risk management may be very effective in prioritizing research and development options.

The U.S. Environmental Protection Agency's (2001) risk-based criteria start with identifying the effect that proposed research would address and assessing whether the effect is sufficiently characterized to develop risk management options. If so, the next step is to determine whether risk management options

(which, for homeland security, may include diplomatic, military, political, legal, procedural, organizational, or technical) currently exist. Finally, if options amenable to development through research and development exist (procedural, organizational, or technical), could new such solutions effectively mitigate the risk cost-effectively and in a manner acceptable to stakeholders? This evaluation process requires an understanding of the potential benefits of research and development solutions within the context of the larger array of potential approaches to reducing the threat of terrorism. Such an approach has the advantage of taking a holistic view of an issue.

Decentralized Organization

Another relevant characteristic of the homeland security arena is that there is a substantial separation between those performing research and development and those responsible for implementing the results of that research and development–such as private industry and State and local responder organizations. Such a decentralized arrangement can lead to a form of principle-agent problem. This can result in research being conducted without the necessary input from the end-users, which could lead to misdirected or irrelevant efforts. Also, research performers may not receive the support and guidance they need to succeed (see "Coordinating Research and Development" section below for more discussion of this topic).

These problems will impede any research and development effort, but may be particularly detrimental in homeland security, where user requirements and priorities may evolve quickly and in unexpected ways. Because of these potential problems, it is important that research and development options be explicitly examined in the context of how they will address the needs of the user agencies, particularly State and local agencies. One approach for accomplishing this coordination for the case of local emergency responders is discussed in later in this report. In general, it will be important to gather expert and stakeholder input early in the research and development process and maintain interaction between these groups throughout the process to help assure that DHS research programs and user needs stay in alignment.

Dual Use Applications

A final defining characteristic of the Department of Homeland Security's effort is that it will likely be characterized by intense periods of great need, followed by longer periods of less activity. In this respect DHS is similar to the Department of Defense. While there will always be important ongoing activity, such as surveillance, training, and systems development, much of the technology and activity that will be supported by research and development, particularly that addressing terrorism response, will be used on an intermittent basis. Thus, it is important to consider how any homeland security research and development could have other benefits as well (e.g., improving the public health system, improving response to natural disasters and industrial accidents, reducing theft at ports, military applications). This so called "dual-use" criterion is particularly important given that many of the users of research and development supported by DHS are local municipalities with limited budgets, which limits their ability to acquire new equipment and provide specialized training. In addition, most of the agencies that make up the Department of Homeland Security have missions that extend well beyond that of the Department. The Department of Homeland Security's mission explicitly states that it must ensure that the functions of the agencies and sub-divisions within the Department that are not related directly to securing the homeland are not diminished or neglected (Homeland Security Act of 2002). This suggests the need for DHS to develop a rigorous and comprehensive approach to identifying potential dual-use applications and their user communities and then regularly consult with them to confirm if the desired dual-use benefits are being achieved.

Proposed Criteria

Table 1 summarizes the above discussion and presents a set of criteria for prioritizing research and development for homeland security. The recommendations made here should be viewed as illustrative and not necessarily complete or in an appropriate rank order.

Table 1-Criteria for Prioritizing Homeland Security Research and Development

Category	Criteria
Research benefits	• Relevance to high-impact threats (biological and nuclear) • Potential to reduce threat • Risk management considerations • Is the targeted effect sufficiently well characterized to develop risk management options? • Do risk management options for this effect currently exist? • Could new technical solutions effectively mitigate the risk cost-effectively and in a manner acceptable to stakeholders? • Addresses needs of research and development users particularly at local and State level • Applicability to non-homeland security use • Relevance to non-homeland security mission of DHS agency • Relevance to non-homeland security use beyond DHS
Programmatic considerations	• Is the necessary research and development infrastructure in place (researchers with relevant knowledge and skills, necessary laboratories, equipment, and methods)? • Is some government agency already supporting it? • Is industry supporting it?

These criteria should provide a provisional basis on which the Department of Homeland Security can examine and rank its research and development options. Applying these criteria will require substantial expert and stakeholder input, as evaluating candidate options against several of the criteria requires predicting the success and impact of research before it has been conducted.[161] The most constructive avenue for the Department of Homeland Security to define and evaluate candidate research options will be to convene workshops or expert panels of researchers, administrators, and user groups. This approach is routinely used for setting research agendas in government and industry (e.g., National Institute for Occupational Safety and Health, 1996; National Institutes of Health, 2003; American Forest and Paper Association, 1999; Pollard et al., 2003) and. Given the decentralization of researchers and end users in the homeland security arena, it will be important that DHS efforts strive to be as inclusive as possible. Representation by State and local agencies and government research agencies outside Department of Homeland Security will be especially valuable.

Coordinating R&D

As noted earlier, a significant portion of the research and development the Department of Homeland Security funds or participates in likely will be executed by agencies housed outside of the department. Moreover, those who seek to apply and use the resulting innovations (such as private industry and State and local response organizations) also will be third parties operating outside of the jurisdiction of DHS.

[161] Further, not all criteria suggested above are likely to be equally important, and some weighting may need to be included in prioritization efforts.

This decentralization has important implications for homeland security research. When an agency performing research is not the principal beneficiary of that research, the performing agency tends not to be heavily invested in the success or failure of a program or project. In contrast, a more vertically integrated agency tends to be more involved and supportive of the research it sponsors. For example, the Department of Defense has a large operational investment in the results of the research it supports. Consequently, the Department of Defense is more realistic about the funds and time needed to complete a project. This contrasts with National Science Foundation and National Institutes of Health, where the agency has less at stake in the success of a project or program because there is no expectation of direct use and there is no timetable for making progress (Office of Technology Assessment, 1991). A potential implication for homeland security is that research conducted in support of the Department's mission by outside agencies may not be responsive to evolving needs or may not receive the support and attention it needs to be successful.

The Department of Homeland Security cannot emulate the vertically integrated model of the Department of Defense. While some of the fragmentation may be lessened in the future with the maturation of the Department's Homeland Security Advanced Research Projects Agency and Homeland Security Institute, a substantial fraction of relevant research will likely always be conducted outside the Department. In addition, the Department must support the needs of State and local emergency responders, emergency managers, and public health agencies, whose operations and needs will always be largely beyond the Department's control.

Research Performers

The alternative to vertical integration is close coordination and partnership. On the research performer side, allowing the Department of Homeland Security to be involved in guiding and evaluating relevant research carried out in outside organizations will strengthen homeland security research (e.g., President's Council of Advisors on Science and Technology, 2002). The importance of such coordination was acknowledged by Congress and the Administration in forming the Department of Homeland Security, although few formal agreements were granted. The department has an advisory role in guiding the National Institutes of Health's bioterror research and has authority to utilize the Department of Energy's national laboratories and sites (Malakoff, 2002). The level of success of homeland security research and development efforts across the entire Federal government will depend heavily on effective interagency cooperation. Such cooperation can be enhanced by the further development of formal relationships between the Department of Homeland Security and outside research agencies.

There are over 50 Federal agencies conducting research that is potentially relevant to the Department's mission. One approach to help guide the selection of agencies with which DHS might want to develop formal research relationships is to array agency research activities and capabilities against homeland security objectives. Such an array could be used to identify matches between existing research activity and homeland security goals. Agencies with matches could then be considered by DHS for partnerships. Numerous potentially beneficial partners beyond those already mentioned could be envisioned, including the National Institute of Standards and Technology, various agencies within the Department of Defense, the National Science Foundation, the National Institute for Occupational Safety and Health, the National Institute of Justice, and the Department of Agriculture. An additional benefit of such an exercise would be to identify gaps in Federal counterterrorism research that the Department of Homeland Security may choose to concentrate on filling through its internal programs.

Interagency relationships could encompass issues such as research prioritization, design, and funding; facility sharing; project and program evaluation; or technology engineering and deployment approaches. The most appropriate type of relationship might depend on factors such as the status of an activity or capability (i.e., existing, under development, planned) or whether the activity is expected to result in

increased knowledge or a deployable system. One example of a potentially beneficial relationship is coordinating with the National Institute for Occupational Safety and Health on the design of research objectives and standards parameters for respiratory protection for terrorism response. Relationships could entail as little as DHS offering to supplement agency or program research budgets or as much as transferring programs into the Department of Homeland Security.

Agency activities related to terrorism could be determined from annual reports or a survey. Some compilations of this sort have already been made (e.g., Office of Management and Budget, 2003; President's Council of Advisors on Science and Technology, 2002). A more challenging aspect is deciding what activities to target, that is, the homeland security objectives. Defining these is an ongoing process and will become more clear as homeland security research is classified and prioritized.

Intramural vs. Extramural Research

A related question is determining which research to conduct within Federal research laboratories (intramural) and which to grant or contract to universities, industry, and non-profit research institutions (extramural). This could apply to research originating from the Department of Homeland Security or partner agencies. There is no simple formula for balancing intramural and extramural research. An analysis of the strengths and weaknesses of each (Office of Technology Assessment, 1991) revealed some useful insights that can act as guides. Strengths of intramural research include the ability to

- Maintain research over decades
- More easily apply a multidisciplinary approach to problems
- More often fund higher risk research because the laboratories can absorb a setback without jeopardizing young faculty or graduate student careers
- Allow project managers to more easily maintain involvement in research
- Be "put on the fast track" when the results are needed quickly
- Assure access and maintenance for large facilities, making Federal laboratories sometimes the only sensible place to site them
- Strengths of extramural research include the ability to
- Access the most talented personnel (Federal laboratories must pay government salaries and often lack the prestige of a university)
- Access the "open market" for the most appropriate lab or team for a particular project
- Stay on the cutting edge of research. Many Federal laboratories are large organizations and some have obsolete missions.

While the second list is shorter, this does not necessarily indicate that extramural research is not worth considering. Access to top personnel can be a particularly strong advantage. A single world-class investigator can generate ideas and enthusiasm to elevate a research program dramatically. In research, leadership is not synonymous with management or administration (National Research Council, 2000).

Research Users

On the research user side, many relevant agencies reside within the Department of Homeland Security (see introduction). This should help insure that the users' procedures, technologies, and operational environments are understood and taken into consideration in determining research priorities and evaluating their progress. In addition, the Department may be able to mandate the use of certain approaches or technologies in order to further improve the link between operations and research.

One notable exception is State and local agencies. Supporting these agencies' research and development needs is one of the important challenges for the Department of Homeland Security. To facilitate the

linkage between Federal research and development and State and local agency needs, the President's Council of Advisors on Science and Technology (2002) recommended the establishment of a "coordinating council" for State and local governments. This council would oversee the process of receiving input from, and relaying information to, pertinent State and local operators regarding needed programs or technologies. Another important role of such a council would be to design, manage, and evaluate pilot programs for new technologies at the State and local level. These activities should be high priorities for the Department's Office of State and Local Government Coordination.

One approach to linking research and development efforts to emergency responder operational requirements is described below. This model could potentially be adopted for other State and local agencies with counterterrorism responsibilities, such as emergency management and public health.

One Effort to Identify the R&D Needs of Emergency Responders

An effort to develop a technology plan for emergency responders that may be useful to the Department of Homeland Security decisionmakers is "Project Responder" (Pollard et al., 2003). This work presents a multi-step process aimed at (a) ensuring that Federal planners understand the capabilities needed by emergency responders and (b) focusing technology development on filling identified gaps in these capabilities. We describe this process below, then discuss how it can be further strengthened and focused.

The process is based on a set of 12 National Terrorism Response Objectives:

1. Personal Protection
2. Detection, Identification, and Assessment
3. Unified Incident Command Decision Support and Interoperable Communications
4. Response and Recovery
5. Emergency Management Preparation and Planning
6. Crisis Evaluation and Management
7. All-Source Situational Understanding
8. Medical Response
9. Public Health Readiness for Biological Agent Event
10. Logistics Support
11. Criminal Investigation and Attribution
12. Agricultural Mitigation and Restoration

Extensive input from emergency responders was used to break down each objective into a number of functional capabilities and associated operational environments. The functional capabilities are subordinate requirements supporting the objective. For example, the functional capabilities for the personal protection objective are body protection from all hazards, long-term respiratory protection–oxygen available, long-term respiratory protection–oxygen deficient, responder decontamination, and escape respiratory protection. The operational environments represent the context in which the functional capabilities would be employed. Based on emergency responder input, Project Responder used the environments created by five weapon types–chemical, biological, radiological, nuclear, and explosive/incendiary–for most response objective categories.

The next step involves inventorying current capabilities and comparing them against the functional capabilities to identify capability gaps. An evaluation is conducted for each combination of functional capability and operational environment to determine if the capability in that environment exists today, is marginal or unevenly available among responders, or does not yet exist. This step requires collaborative input from technology users (the emergency responder community) and researchers and technologists (government laboratories, universities, industry).

Capability-environment combinations that do not exist today, termed capability gaps, are then evaluated to assess what approaches–including procedures, organization, training, coordination, and technology–can

be used to resolve them. Finally, for those gaps that are determined to be amenable to technological solutions, technology goals are developed. These goals are intended to cast the problem in terms appropriate for the research community, and would identify a specific technology advancement that would be developed, the agency best suited to conduct the research, metrics to measure the advancement, timelines for progress, and the funding required. Development of technology goals would be formulated in an iterative process that involves emergency responders, researchers and technologists, and technology planners (government agencies, policy researchers).

The Project Responder technology planning methodology was developed with extensive input from the emergency responder community to insure that the proposed planning framework would capture the key capabilities needed to conduct emergency response operations. Subsequent vetting with numerous Federal agency representatives and local emergency responders indicates that it has the potential to focus and prioritize national investment in advanced technologies for combating terrorism (Pollard et al., 2003). The approach is ideally suited for identifying capability gaps and research needs for emergency responders across a wide spectrum of terrorism response activities. Importantly, the methodology includes roles for all stakeholders and provides and analytical bridge between research and development efforts and emergency responder operational needs.

The Project Responder approach can be made even more useful by expanding its scope. It seems unnecessarily restricted to identifying technology needs. Homeland security research and development must address more than technology, and the approach appears to be well suited to identifying both technical and nontechnical solutions to capability gaps. Nontechnical solutions may include improving operational procedures, organizational structures, training, or coordination. An important example is the need for operational procedures for different responder services designed for specific types of terrorist attacks (LaTourrette et al., 2003).

The Project Responder methodology is designed to be comprehensive in identifying research and development needs for emergency responders. Another way in which it could be improved is to incorporate prioritization considerations. Evaluating the candidate research areas according to the criteria and considerations in Table 1 could help identify those areas warranting higher priority. For example, gaps related to high impact threats or gaps that, when filled, will have large benefits, could be prioritized. Another important consideration for emergency responders is applicability to non-homeland security use. Additional equipment introduces numerous burdens for emergency responders, such as difficulties in assessing when specialized gear is called for, the necessity to train departments and individuals on proper use, maintaining proficiency and familiarity with seldom-used gear, and increased storage, transportation, and maintenance requirements (LaTourrette et al., 2003). Ultimately, research and development addressing emergency responder needs must be weighed in the context of research and development in other areas of homeland security, such as border and transportation security, intelligence analysis, and infrastructure protection. In order to provide Department-wide perspective on the research and development needs in different areas and to assist with Department-wide prioritization, representatives from these other areas could be included in the assessment and prioritization of emergency responder research and development needs.

Terrorism Response Standards

The issue of standards for terrorism response has received considerable attention throughout the formation and early operations of the Department of Homeland Security. Standards can have important implications for the nascent research and development agenda of the Department of Homeland Security. One implication is that standards require a substantial body of supporting research and hence can play an important role in determining the direction of Department of Homeland Security research and development. A standard that requires capabilities beyond what are currently available, such as is being considered for biological and chemical agent detectors (U.S. Department of Homeland Security, 2003b),

must be preceded by research and development to attain that capability. A second implication is that standards will drive the diffusion and use of particular technologies and counterterrorism activities. Thus, the Department of Homeland Security can use standards as a mechanism to promote the dissemination of new technologies and procedures emerging from the research and development pipeline. Finally, development and implementation of the standards themselves will require research support in the form of establishing performance requirements, designing certification and testing procedures, and validating their performance in the field. The Department of Homeland Security may thus need to provide research support to standards-setting and certification organizations.

Types of Standards

Terrorism response standards are generally directed at two levels: those that apply to equipment design and performance and those that concern overall preparedness, including equipment, procedures, training, supplies, and facilities.

Equipment standards development is progressing naturally through mechanisms and institutions that have existed prior to the formation of DHS. For example, one of the top priorities of emergency responders in the context of terrorism response is protection from chemical warfare agents (e.g., LaTourrette et al., 2003; Pollard et al., 2003). These concerns have been raised in standard-setting organizations, where candidate solutions have been proposed, evaluated, refined, and agreed upon in an open and representative forum. The National Fire Protection Association, a widely recognized independent organization, has developed a standard for protective garments for chemical and biological terrorism incidents (National Fire Protection Association, 2001). The National Institute for Occupational Safety and Health, a Federal agency, working with a number of other organizations, has recently developed standards and certification procedures for respiratory protection for chemical, biological, radiological, and nuclear weapons (National Institute for Occupational Safety and Health, 2001). These and other similar standards-development institutions and mechanisms appear to be well-positioned to continue to address equipment standards for terrorism response. The Department of Homeland Security's role in equipment standards development, therefore, might be limited to collaboration and support, for example, in the area of funding to support the activities of these organizations.

In contrast, no institutions or mechanisms currently exist to develop and enforce the more complex and multidisciplinary standards that would be required for terrorism preparedness for emergency response organizations While current standards-setting efforts do go beyond equipment and address operating procedures (e.g., the National Fire Protection Association publishes a standard on recommended practices for responding to hazardous materials incidents), standards for terrorism preparedness cover a much broader scope which falls beyond the purview and capabilities of a single organization. Developing such standards will require creating new capabilities and organizations, and this suggests a more prominent role for DHS.

Options for Generating Standards

Canada (2003) has outlined several policy approaches for generating terrorism preparedness standards that merit consideration by the Department of Homeland Security. These options and some of their implications are summarized below.

- Maintain the Status Quo. There is by no means universal agreement within the homeland security community on whether terrorism preparedness standards are necessary. Some note the extensive effort already devoted to funding, planning, and training for disaster response and argue that current response capabilities are very good. The response to the September 11, 2001 attacks is cited as an example of the speed and scale at which the current system is able to operate. A related argument is that current equipment and response standards are adequate, and that

appropriate new standards will evolve as necessary. This reasoning is based on the assumption that standards are only useful when they serve a clear objective, and that the current uncertainty surrounding the terrorist threat precludes the development of useful preparedness standards.

- Encourage Development and Adoption. This entails promoting a voluntary consensus process. This is the most common process used to create a wide variety of standards, including those developed by the National Fire Protection Association. In short, this is a structured process that involves a number of stakeholders, including users, manufacturers, researchers, associations, and government agencies. It incorporates the principals of due process, openness, balanced participation, written procedures, and an appeals process. The American National Standards Institute advocates these principles. The National Research Council found that this process is effective, particularly when Federal agencies participate, and found that it is often faster than Federal regulatory approaches and results in standards that are as stringent and demanding as Federal regulatory standards. Congress endorsed this approach in the National Technology Transfer Advancement Act of 1995 and reaffirmed its commitment to it in the Homeland Security Act of 2002. Success of this approach requires high participation from stakeholders and good communication among participants.

  While widely heralded, this approach offers Federal authorities limited influence over the pace and direction of activities. Aside from increasing grant funding to nongovernmental standard-setting organizations or sponsoring interagency standardization working groups, the government has few options for encouraging this process. And there may be little motivation to advance such an effort voluntarily. The large number of stakeholder groups required and the scope and complexity of the task may deter the community from undertaking or completing it. As a result, this process might not result in the desired level of preparedness.

- Condition Federal Assistance. Another approach is would be to adopt preparedness standards that State and local agencies would be required to meet as a condition for receiving Federal assistance. The Federal government has a long tradition of conditioning grants. In fact, the Department of Homeland Security's Office of Domestic Preparedness currently requires recipients to complete a needs assessment before receiving funds, and equipment grants may only be used to purchase approved equipment.

  A challenge with this approach is establishing the appropriate balance between specific operational and technical (micro) standards and overall performance (macro) standards. Complying with excessive micro standards may require agencies to alter their plans, equipment, or training to such an extent that they would decline the assistance. Compliance with overly broad performance standards, on the other hand, is difficult to evaluate and may result in agencies not achieving the desired level of preparedness. A reasonable compromise would be to have the standards define specific performance goals, but allow local agencies discretion in determining how to achieve these goals. Note that conditioning Federal assistance does not solve the problem of what standards should be chosen and how they should be developed. Either a voluntary consensus or Federal process must still be employed.

- Promulgate Federal Regulations. The most aggressive approach would be for DHS to develop and implement preparedness standards or to direct other Federal agencies to do so. This would result in the highest degree of compliance, since Federal regulations are enforceable under the law. As with conditioning Federal assistance, this approach is quite common, with agencies such as the Occupational Safety and Health Administration, National Highway and Traffic Safety Administration, and U.S. Environmental Protection Agency enforcing regulations addressing public safety and health. And this approach, too, has already been adopted in the homeland security arena: the Public Health Security and Bioterrorism Preparedness Act of 2002 required

community water systems serving more than 3,300 people to complete a vulnerability assessment and develop an emergency response plan.

While a Federal regulatory approach may be the best way to assure that standards are developed and enforced, it has some potential pitfalls that must be considered. First, in general, Federal regulations are less likely than a voluntary consensus to be crafted with the necessary technical knowledge and appropriate stakeholder representation. This may not be true for terrorism preparedness standards, however, given the large scope and complexity involved. Nonetheless, efforts should be made to incorporate as many existing voluntary standards as possible, as many nongovernmental organizations, such as the National Fire Protection Association, have access to more subject matter expertise and are more familiar with the standards-development process.

Second, Federal standards may raise some federalism issues. States or local jurisdictions might argue that Federal preparedness regulations represent an unfunded mandate. Unfunded mandates are discouraged, though not forbidden, by law and exceptions for national security needs are permitted. Nonetheless, States may oppose Federal standards that are more stringent than current standards, particularly if they pose significant burdens in terms of replacing equipment, re-training personnel, or modifying facilities. Preemption of State laws and interference with current practices may also be a concern. Extensive disaster response plans and intergovernmental partnerships have been developed in particular areas to address their unique needs with their available resources. Modification of these plans to focus on terrorism, particularly if such modification is viewed as interfering with the region's ability to respond to other public safety concerns, such as natural disasters, may be opposed. If the Department of Homeland Security chooses to mandate Federal terrorism preparedness standards, States may challenge them on these grounds.

Overcoming Uncertainty in Standards Development

Any effort to develop terrorism preparedness standards, regardless of the role of DHS, is further complicated by the tremendous level of uncertainty surrounding terrorism response. In the first place, the uncertainty about the terrorist threat–what kinds of weapons may be used, what sites may be targeted, how often such actions may be attempted–makes it difficult to provide much specificity in a preparedness standard. This leaves the choice of making preparedness standards either very general or somewhat arbitrarily focused on particular possibilities. The former choice will be difficult to distinguish from existing general disaster preparedness plans. This may indicate that terrorism preparedness standards are unnecessary and that efforts should focus on disaster preparedness standards instead. The danger of the latter choice is that standards could become obsolete as threats evolve; frequent updating of standards to match the latest threat may make it impossible for State and local agencies to keep up.

A second important uncertainty impacting terrorism preparedness standards is how emergency responders and other State and local agencies will operate in a terrorism response. In-depth discussions with emergency responders around the country reveal that few specific operational procedures for terrorism response exist (LaTourrette et al., 2003) and that such scenes can entail high levels of stress (Jackson et al., 2002). This means that, even if the details of a specific of attack were known ahead of time, what responders will actually be doing during the response can only be predicted in very general terms. This contrasts markedly with more common types of responses, such as structural fires, where response procedures and training are well-established and institutionalized. Developing preparedness standards is impeded by not knowing what responders need to be prepared to do. While preparedness standards may help better define terrorism response operations, this is not necessarily the case. Thus, the development of preparedness standards will be greatly facilitated and the usefulness of those standards will be greatly enhanced by first developing terrorism response operational procedures.

These uncertainties indicate that the Department of Homeland Security will need to proceed with caution in developing and implementing terrorism response standards. In particular, because standards have the potential to influence research and development decisions and "lock-in" particular technologies or procedures, it is important that standards development be conducted iteratively and in close coordination with the research and development of counterterrorism technologies and operational procedures.

References

AAAS Intersociety Working Group (2003) AAAS Report XXVIII:
Research and Development FY 2004, American Association for the Advancement of Science, Washington, DC, available at http://www.aaas.org/spp/rd/rd04main.htm.

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (2000) *Second Annual Report to the President and the Congress*, available at http://www.rand.org/nsrd/terrpanel/terror2.pdf.

American Forest and Paper Association (1999*) The Path Forward: An Implementation Plan, U.S. Department of Energy Office of Industrial Technologies*, Washington, DC, available at http://www.oit.doe.gov/forest/pdfs/forest_roadmap.pdf.

Bromley DA (2003) "What Criteria Should be Used to Establish Funding Priorities?," *Physics Today,* June, 2003, pp. 54-55.

Canada B (2003) *Homeland Security: Standards for State and Local Preparedness*, Congressional Research Service report RL31680, Library of Congress, Washington, DC.

Check E (2003) "Homeland Science Chief Wants Quick Fixes," *Nature*, vol. 423, p. 106.

Davis LE, LaTourrette T, Mosher DE, Davis LM, and Howell DR (2003) *Individual Preparedness and Response to Chemical, Radiological, Nuclear, and Biological Terrorist Attacks*, MR-1731-SF, RAND, Santa Monica, CA, available at http://www.rand.org/publications/MR/MR1731.

Frist W, Marburger JH, Lederberg J, Schneider W, and Neal H (2002), *Marshalling Science, Bridging the Gap: How to Win the War Against Terrorism and Build a Better Peace,* Center for the Study of the Presidency, Washington DC, available at http://www.thepresidency.org/pubs/indexpubs.htm.

Homeland Security Act of 2002 (H.R. 5005), Title 1, Sec. 101 (b), available at http://www.dhs.gov/dhspublic/display?theme=46.

Jackson BA, Peterson DJ, Bartis JT, LaTourrette T, Brahmakulam IT, Houser A, and Sollinger JM (2002) *Protecting Emergency Responders: Lessons Learned from Terrorist Attacks*, CF-176-OSTP, RAND, Santa Monica, CA, available at http://www.rand.org/publications/CF/CF176/.

LaTourrette T, Peterson DJ, Bartis JT, Jackson BA, and Houser, A (2003), *Protecting Emergency Responders, Volume 2: Community Views of Safety and Health Risks and Personal Protection Needs,* MR-1646-NIOSH, RAND, Santa Monica, CA, available at http://www.rand.org/publications/MR/MR1646/.

Malakoff D (2002) "New Agency Contains Strong Science Arm," *Science*, vol. 298, p. 1534.

National Fire Protection Association (2001) NFPA 1994—Standard on Protective Ensembles for Chemical/Biological Terrorism Incidents, National Fire Protection Association, Quincy, MA.

National Institute for Occupational Safety and Health (1996)
National Occupational Research Agenda, DHHS (NIOSH) Publication No. 96-115, National Institute for Occupational Safety and Health, Washington, DC.

National Institute for Occupational Safety and Health (2001)

Approval of Self-Contained Breathing Respirators for Emergency Workers in Terrorist Attacks, National Institute for Occupational Safety and Health, Washington, DC, available at http://www.cdc.gov/niosh/npptl/scbasite.html

National Institutes of Health (2003) Setting Research Priorities at the National Institutes of Health, National Institutes of Health, Bethesda, MD, available at http://www.nih.gov/about/researchpriorities.htm.

National Research Council (1998) *Scientific Opportunities and Public Needs: Improving Priority Setting and Public Input at the National Institutes of Health,* National Academies Press, Washington, DC.

National Research Council (2000) *Strengthening Science at the U.S. Environmental Protection Agency: Research Management and Peer-Review Practices,* National Academies Press, Washington, DC.

National Research Council (2001a) *Energy Research at DOE: Was It Worth It?*, National Academies Press, Washington, DC.

National Research Council (2001b) *Implementing the Government Performance and Results Act for Research: A Status Report,* National Academies Press, Washington, DC.

National Research Council (2002) *Making the Nation Safer: The Role Of Science and Technology In Countering Terrorism,* National Academies Press, Washington, DC.

National Science Board (2001) Federal Research Resources: A Process for Setting Priorities, NSB 01-156, National Science Foundation, Washington, DC, available at http://www.nsf.gov/pubsys/ods/getpub.cfm?nsb01156.

Office of Management and Budget (2003) *2003 Report to Congress on Combating Terrorism,* Office of Management and Budget, Washington, DC, available at http://www.whitehouse.gov/omb/inforeg/2003_combat_terr.pdf

Office of Technology Assessment (1991) *Federally Funded Research: Decisions for a Decade,* available at http://www.wws.princeton.edu/~ota/ns20/pubs_f.html.

Pollard NA, Tuohy RV, and Garwin T (2003) *Project Responder, Interim Report: Emergency Responders' Needs, Goals, and Priorities,* Oklahoma City National Memorial Institute for the Prevention of Terrorism, Oklahoma City, OK, available at http://www.mipt.org/pdf/projectresponderneeds.pdf.

President's Council of Advisors on Science and Technology (2002), *Report on Maximizing the Contribution of Science and Technology Within the Department of Homeland Security,* Office of Science and Technology Policy, Washington, DC, available at http://www.OSTP.gov/PCAST/FINAL%20DHS%20REPORT%20WITH%20APPENDICES.pdf.

U.S. Department of Homeland Security (2003a) Department of Homeland Security Budget in Brief - Fiscal Year 2004, available at http://www.dhs.gov/interweb/assetlibrary/FY_2004_BUDGET_IN_BRIEF.pdf.

U.S. Department of Homeland Security (2003b) Address by Dr. Charles E. McQueary to the DOE Facilities Caucus Breakfast Meeting, available at http://www.dhs.gov/dhspublic/display?content=1818.

U.S. Environmental Protection Agency (2001) Office of Research and Development Strategic Plan, EPA/600/R-01/003, Washington, DC, available at http://www.epa.gov/osp/stplan.htm.

APPENDIX I–COMMUNICATIONS INTEROPERABILITY AND EMERGENCY RESPONSE*

The exchange of information, whether by voice over a radio handset, via computer systems, or directly face-to-face, is crucial to the effectiveness of response operations and to the safety of individual responders. Without it, emergency workers have only a limited ability to remain aware of evolving emergency situations, access tactical and threat information, and call on assistance and reinforcement. Communications are particularly important in larger, more complex incidents involving multiple responding organizations. In multiagency and multijurisdictional response operations, communication provides the links that make coordinated and organized action possible. From joint police and rescue efforts at a major traffic accident to large-scale multiagency, multi-service responses to a natural disaster or terrorist attack, the need to share information among responders and their organizations is essential.

Failures in communication can reduce the effectiveness of response operations and put the safety of responders at risk. As the tragedy of September 11, 2001 showed, breakdowns in communications among individuals and responding organizations have the potential to contribute to responder injuries and loss of life. Similarly, when responders cannot effectively share tactical and operational information, their ability to act effectively can be reduced. At many large-scale incidents, including the Pentagon on 9/11, the 1993 World Trade Center bombing, and at the Murrah Federal Building in Oklahoma City, failures in communication systems forced responders to use messengers to relay messages around the incident scenes and among responding organizations, delaying or preventing the exchange of critical incident information.[162,163,164]

Significant effort in this area has focused on the ability of response organizations' radios or other communications systems to connect – or *interoperate* – allowing their members to talk to one another.[165] Although the technical barriers that prevent responders from *talking* with one another are a critical component of this problem, there are organizational and procedural components that must also be in place before responders can effectively *communicate*.[166] Effective communication requires the means to exchange information, the practices that ensure that the needed information is delivered at the right time and in the right amount to meet operational needs, and the communications procedures (e.g., common terminologies) to ensure that the information is understandable for its intended recipients. As a result, this analysis adopts a definition of communications interoperability that includes all components necessary to ensure that individual emergency responders and response managers have access to critical information during response operations regardless of organizational, jurisdictional, or functional boundaries. Because of the range of responder organizations potentially involved in large-scale response operations – including fire, emergency medical services, law enforcement, public health, State, Federal, and volunteer groups – the generic term *public safety agencies* will be used throughout the discussion.

[162] Manzi C, Powers MJ, Zetterlund K. "Special Report: Critical Information Flows in the Alfred P. Murrah Building Bombing: A Case Study," May 2003. http://www.cbaci.org/murrahcasestudyfinal.pdf (Date Accessed: May 2003).
[163] Manning WA, ed., "The World Trade Center Bombing: Report and Analysis," 1993. http://www.usfa.fema.gov/downloads/pdf/publications/tr-076.pdf (Date Accessed: May 2003).
[164] Arlington County, Virginia. "Arlington County After-Action Report on the Response to September 11 Terrorist Attack on the Pentagon," 2002. http://www.co.arlington.va.us/fire/edu/about/pdf/after_report.pdf (Date Accessed: May 2003), A-10.
[165] Communications interoperability problems can affect all forms of public safety communications including the exchange of data via computer terminals, crosslinking of databases, geographic information systems, etc. This paper will focus on radio communications, though many of the strategies and approaches described also apply, to differing extents, to these other communications systems and problems.
[166] Rubin DL and Maniscalco P "EMS Incident Management: Operational Communications" Emergency Medical Services, May 2000, 93-95.

The following discussion introduces the sources of interoperability problems. Because this problem has been recognized for some time, a range of solutions has been developed and pilot efforts deployed to address it. Based on the review of the available solutions, the final section identifies areas where additional efforts and examination are needed to most effectively promote public safety communications interoperability.

Sources of Communications Interoperability Problems

Throughout the public safety community, the communication systems currently in place often lack the capability for diverse responders to communicate with one another at multiagency operations. While these problems are often most serious among agencies from different jurisdictions or different levels of government, even agencies from the same jurisdiction frequently cannot readily communicate due to technical problems or differences in their organizations' procedures and communications practices.

Technical Sources of Interoperability Problems

Although many technologies are being applied to public safety communications and information sharing needs – such as field-accessible computer systems, cellular technology, and other mechanisms – the major route used to exchange information during on-going multiagency, multijurisdictional response operations is hand-held, tactical radio systems. As a result, concerns surrounding communications interoperability generally focus on the capabilities and characteristics of these radio systems.

Interoperability failures arise from two types of system incompatibility:

1. Different organizations' communications systems may operate on separate, and therefore incompatible, radio frequencies, and
2. Proprietary differences among radio systems produced by different manufacturers can make radios incompatible, even if they use the same radio frequency.

Incompatible Radio Frequencies. All radio systems utilize a portion of the radio spectrum to send and receive signals carrying voice or other data. The radio spectrum consists of a continuous series of frequencies, divided into a finite set of frequency channels across which signals can be broadcast. Because a finite number of these broadcasting channels exist, the radio spectrum is a limited public resource. The Federal Communications Commission (FCC) has designated certain frequency bands, which are ranges of adjacent frequencies, for specific uses, such as television broadcasting, commercial radio, and public safety communications.

Because of the way this division was carried out, the frequencies allocated for public safety use are scattered across the radio spectrum. Instead of a single "slice" of frequencies, the public safety spectrum is fragmented into 10 different bands (Figure 1). Most radio equipment can only broadcast across one to three of these bands.[167] This means that if a fire department operates in one band of frequencies and a police department operates on another, they cannot use their radios to speak directly to each other.

[167] Imel KJ and Hart JW "Understanding Wireless Communications in Public Safety: A Guidebook to Technology, Issues, Planning and Management," January 2003. http://rmlectc.dri.du.edu/documents/GuideWC/Front(VersII).PDF (Date Accessed: September 2003), 108.

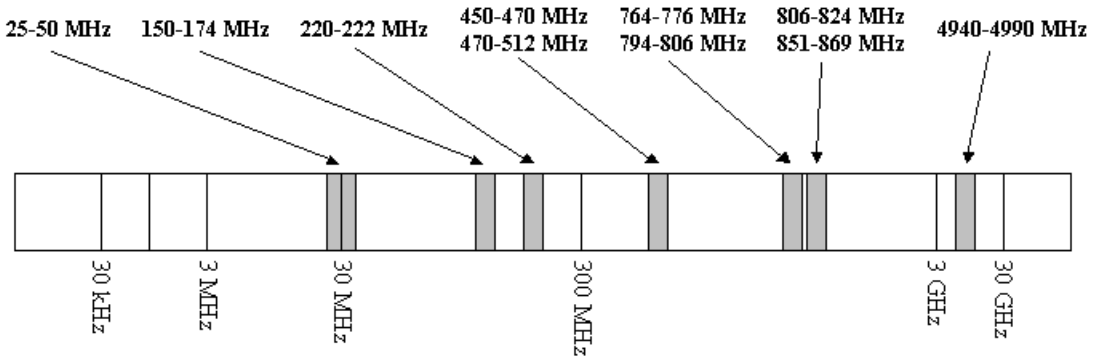


Figure Adapted from: National Task Force on Interoperability, "When They Can't Talk, Lives are Lost: What Public Officials Need To Know About Interoperability." February 2003. http://www.agileprogram.org/ntfi/ntfi_brochure.pdf.

Figure 1: Segments of the Radio Spectrum Allocated to Public Safety Communication

Proprietary Differences. Even when radios utilize the same portion of the radio spectrum, they cannot necessarily interoperate. Radios produced by different manufacturers can have proprietary differences – such as the way the transmitted signal is structured – that make it impossible for them to communicate with one another. As a result, adjacent public safety agencies might both have systems that operate in the same section of the radio spectrum but will still be unable to communicate. For example, differences among the encryption techniques used by manufacturers to enable secure communication can make their communications systems incompatible.[168]

Procedural and Organizational Interoperability Issues

Although differences among communications systems are a primary source of interoperability problems, even addressing all technical issues would not be enough to ensure effective communication among responders at multi-agency or multijurisdictional operations. Differences in operational procedures and training between responding organizations can also create barriers to effective communication.

Significant differences can exist in two main areas:

1. Procedures and training regarding the available capabilities of communications systems, and
2. Protocols associated with how communications systems are used during response operations.

Capabilities of Communications Systems. Differences in procedures and training among different response organizations can get in the way of effective use of available interoperability assets. For example, public safety organizations or services may manage their radio channels differently – e.g., labeling or naming them in significantly different ways. The resulting confusion can produce communications failures even if the radio systems themselves actually are interoperable.[169] Similarly, unless responder training specifically addresses interoperability, responders or radio operators may be unaware of, or unable to use, interoperability capabilities that are already available.[170] For example,

[168] Public Safety Wireless Network, "Public Safety Wireless Communications Standards Awareness Guide," http://www.publicsafetywins.gov/PolicySolutions/Standards/PSWNSTDS.pdf
[169] Imel KJ and Hart JW "Understanding Wireless Communications in Public Safety: A Guidebook to Technology, Issues, Planning and Management," January 2003. http://rmlectc.dri.du.edu/documents/GuideWC/Front(VersII).PDF (Date Accessed: September 2003), 108.
[170] "Post-Symposium Support Report - New Jersey Public Safety Communications Interoperability Conference," December 2002. http://www.pswn.gov/admin/librarydocs11/NJ_post_symposium_report.pdf (Date Accessed: September 2003)

knowledge of interoperability capabilities and procedures can be lost when responders retire or are reassigned.[171]

Communications Operational Protocols. Beyond awareness of radio systems' capabilities, effective communication also requires a common understanding among public safety organizations of how radio systems should be used during major response operations. Common definitions are needed for:

- What information should be communicated,
- How it should be communicated, and
- To whom it should be communicated.

What to Communicate. In large-scale emergency events, the sheer volume of traffic can overwhelm communication systems. Heavy traffic on radio or other systems can effectively render them inoperable after an event. If response organizations' communications procedures result in excessive radio traffic, even completely interoperable radio systems may not be effective. Problems with excessive traffic on communication systems, including voice radio and cellular systems, have been cited in many large-scale response operations including the September 11th attacks. Operational usage protocols that reduce traffic can help preserve the utility of communications systems.

How to Communicate. Differences in the ways responders communicate can also hinder the transfer of information during response operations. If responders from different organizations use different vocabularies, significant misunderstandings can occur. Developing common terminologies is an important component in the design of effective incident management systems for multiagency operations.[172] If different organizations refer to the same pieces of equipment or operations using different terms, effective communication and coordinated action are made much more difficult. Furthermore, some public safety agencies use codes in an effort to reduce the volume of radio traffic and improve the communication efficiency. Although such radio codes can work effectively for individual organizations, they can cause problems during multiagency or multijurisdictional operations. Confusion can rapidly develop if two or more organizations use different codes for the same equipment or response activities.[173]

With Whom to Communicate. Beyond its potential to clog radio systems, excessive communications traffic can also overwhelm the attention of response commanders and prevent them from effectively using critical information. Responders and organizations playing different roles at a multiagency, multijurisdictional incident need access to different types and amounts of information to carry out their activities. Too much irrelevant communication can result in information overload and hinder decisionmaking. This problem was highlighted by responders involved in the September 11th response operations at the World Trade Center in New York City.[174] If response organizations do not adopt similar conventions about what information should be transmitted to which commanders or units, the extraneous traffic can distract, confuse, and otherwise degrade the capability to effectively communicate. If a response operation lacks a clear chain of command or available communications resources are not effectively allocated and managed, these problems can increase significantly.

---

[171] Public Safety Wireless Network "Operational Best Practices for Managing Trunked Land Mobile Radio Systems," May 2003. http://www.pswn.gov/admin/librarydocs11%5COperational_Best_Practices_for_Trunked_Radio_Systems.pdf, 24.

[172] Christen H, Maniscalco P, Vickery A, and Winslow F "An Overview of Incident Management Systems," Perspectives on Preparedness, Executive Session on Domestic Preparedness, John F. Kennedy School of Government, Harvard University, September 2001. http://bcsia.ksg.harvard.edu/BCSIA_content/documents/An_Overview_of_Incident_Management_Systems.pdf (Date Accessed: May 2003).

[173] Rubin DL and Maniscalco P "EMS Incident Management: Operational Communications" Emergency Medical Services, May 2000, 93-95.

[174] Interviews with the author.

Solutions: A Range of Strategies for Improved Communications

In an effort to improve communications interoperability, a number of programs and organizations have been put in place to address these problems. Selected examples include the Public Safety Wireless Network program,[175] the National Institute of Justice's AGILE program,[176] and the National Task Force on Interoperability.[177] A variety of other efforts have also been carried out at the Federal, State, and local level and in the private sector.[178] Such efforts have developed a range of strategies relevant to both communications systems interoperability problems and the organizational interoperability concerns as well.

Technical Approaches to Building Communications Interoperability

Significant effort has been devoted in both the public and private sectors to addressing the technical sources of interoperability failures. Efforts have been focused in four main areas:

1. Coordination efforts to ensure public safety organizations have compatible radio systems
2. Radio spectrum allocation
3. Technological strategies including the use of bridges or gateways among incompatible systems, the use of supplemental communications systems, or other radio traffic or access control approaches
4. Technology standards to address differences among manufacturers' systems

Coordination. The most straightforward approach to prevent incompatibilities among public safety agencies' communications systems is for those organizations to coordinate their purchasing decisions and buy systems that can interoperate. Such multiagency and cross-jurisdictional coordination could be aimed at complete interoperability, i.e., ensuring that all involved agencies can communicate all the time, or at more limited solutions for use when needed. Beyond their interoperability benefits, these efforts can also result in cost savings for States and individual localities as a result of the increased purchasing power provided by coordinated acquisition.

Although this multiorganizational approach to communication systems design can provide a solution to interoperability problems, there are a number of barriers to effectively putting it into practice:[179]

- Response organizations' different communications needs,[180] operational circumstances, or political issues can reduce their desire to coordinate or make doing so more difficult. Without strong leadership to bring together the relevant organizations, these differences can significantly handicap interoperability programs.
- Differences in acquisition, planning, and funding cycles among organizations complicate efforts to move to common and compatible systems. In some cases, large enough differences in funding availability or procurement cycles can make it very difficult for individual organizations to participate in interoperability efforts.

[175] http://www.pswn.gov
[176] http://www.agileprogram.org
[177] http://www.agileprogram.org/ntfi/justnet.html
[178] See http://pssummit.its.bldrdoc.gov/ for a review of many Federal, State, and local interoperability efforts.
[179] National Task Force on Interoperability, "Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives" http://www.agileprogram.org/ntfi/ntfi_guide.pdf (Date Accessed: September 2003).
[180] For example, some public safety organizations may need to communicate more frequently than others or have significantly different security requirements. Such divergence in requirements can make it more difficult to select common or compatible systems across organizations.

- Organizations with significant investments in legacy communications systems may hesitate to move toward new interoperable systems.

As the number of organizations involved in a coordination effort increases – e.g., moving from synchronizing the communication systems of a small number of local public safety agencies to a statewide or regional effort – such barriers to coordination can become even more difficult to address.

In order to facilitate building interoperability among organizations, significant effort has been focused on developing approaches to reduce or eliminate barriers to coordination. Examples have included developing shared governance structures, such as boards or joint commissions, to provide sufficient authority for coordination efforts while addressing multiple organizations' priorities and constraints; support of demonstration and pilot efforts; and preparation of information resources to assist in planning and coordination.[181]

Radio Spectrum Allocation. Since the fragmentation of the radio spectrum devoted to public safety communications is a major source of interoperability problems, changes in the location or amount of spectrum available are a potential route to addressing the problem. In fact, issues surrounding radio spectrum are linked to most other approaches to putting communications interoperability in place. Because radio spectrum is a finite resource, scarcity of channels for public safety communication represent a significant constraint on the design of new approaches for providing interoperability. Two trends have heightened this scarcity:

- Increasing demand for public safety communications, such as wireless data terminals;[182] and
- Interference from other strong signals near public safety frequencies, such as commercial mobile telephones.[183]

As a result, even if coordination efforts were successful in providing public safety agencies with compatible radios operating in the same parts of the radio spectrum,[184] a lack of sufficient spectrum would still handicap interoperability efforts.

Changes to spectrum allocations and usage are therefore an important component of interoperability efforts.[185] Technological strategies, such as the use of "trunked" systems that manage communications more efficiently or new systems that can fit more communications channels within a slice of radio spectrum, are one approach. Tools have also been developed to assist spectrum allocation in radio system planning.[186] Policy efforts are also underway at the national level to allocate additional spectrum to

[181] National Task Force on Interoperability, "Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives" http://www.agileprogram.org/ntfi/ntfi_guide.pdf (Date Accessed: September 2003).
[182] Smith B and Tolman T "Can We Talk? Public Safety and the Interoperability Challenge" National Institute of Justice Journal, April 2000, 18-21.
[183] National Task Force on Interoperability, "Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives" http://www.agileprogram.org/ntfi/ntfi_guide.pdf (Date Accessed: September 2003).
[184] In addition, radios operating on different frequencies have different operating characteristics that make it less desirable to have all public safety agencies using similar systems. For example, some systems have better performance characteristics in some terrain types or within buildings.
[185] Scannell K and Davis A "Danger: Missing Signals" *The Wall Street Journal*, March 17, 2003, B1.
[186] See, for example, http://www.iacptechnology.org/LEIM/2003Presentations/NIJPresentations/ AGILEProgramUpdate.pdf

public safety agencies[187] or reallocate spectrum in existing bands.[188] Both efforts face complex issues in rationalizing public safety needs with the needs of current users of the relevant radio spectrum.[189]

Technological Strategies. A range of hardware-based strategies has been developed to either link responder communications systems or to provide some interoperability at large-scale events. The most basic hardware strategy for rapid interoperability is for responders to simply "trade radios," thereby allowing selected members of separate organizations access to all relevant communications. While such a strategy is quick and straightforward, the need for individuals to juggle different radios and monitor many separate communications streams makes it a less than ideal solution. Having multiple separate streams of information coming through different radios can result in missed communications and misunderstandings. As a result, a several other technology-based strategies have been or are being developed, including:

- Use of supplemental communications systems - Cellular telephones, paging systems, or other special systems deployed at an event have been used to provide some interoperability.[190]
- Connections between communications systems – Bridge devices can be installed at either responder dispatch centers or in the field to interlink disparate radio systems and provide cross communication. Such system interconnections can be made to permanently connect systems to provide day-to-day interoperability or installed for individual response operations.
- Technical solutions for non-technical interoperability problems – Features have been built into communications systems to address the risk that excessive communication traffic will either degrade the performance of a communications system or result in information overload. Priority access features can provide commanders the ability to complete critical communications when needed.[191] Similarly, the ability to subdivide radio systems into talk-groups or allocate different radio frequencies to separate response functions also provide strategies to address these issues.
- Flexible radio technologies – New radio technologies, such as software-based radios[192] or internet protocol communications approaches, may provide ways to reconfigure radios to operate on many different communications systems.[193] Similarly, for systems across the public safety community, a variety of efforts have applied the first three strategies to improve interoperability; flexible radio technologies are still being developed and deployed and may provide additional technical interoperability options in the future.

Technology Standards. Technology standards seek to eliminate incompatibilities among radio systems produced by different manufacturers by defining common ways of radio signal encoding and management. Commonly accepted standards that serve as the basis for equipment design reduce the variation among different technologies available in a market and provide public safety organizations with the assurance that, if their communications system adheres to the standards, it will be able to

[187] National Task Force on Interoperability, "Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives" http://www.agileprogram.org/ntfi/ntfi_guide.pdf (Date Accessed: September 2003).
[188] "In the Matter of Improving Public Safety Communications in the 800 MHz Band - Consolidating the 900 MHz Industrial Land Transportation and Business Pool Channels" http://www.iafc.org/downloads/fccfiling1202.pdf (Date Accessed: September 2003).
[189] For example, in one legislative effort, spectrum has been allocated to public safety organizations that is currently occupied by television broadcasting. Initially, the deadline for those stations to vacate the spectrum was tied to adoption of digital television by consumers, making it difficult to determine a timetable when it would be available for public safety use. (National Task Force on Interoperability, "Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives: Supplemental Resources," http://www.agileprogram.org/ntfi/ntfi_supplemental.pdf (Date Accessed: September 2003).
[190] For public-use systems, e.g., cellular telephones, the increased communications traffic after a major event can render them useless as a source of interoperability. Efforts to provide priority access to these systems for public safety agencies could alleviate this problem. (http://wps.ncs.gov/)
[191] The GETS system, which provides priority access to landline telephone networks, has been in place for many years. The WPS system, which provides similar access to cellular telephone resources, was been put in place recently to address problems public safety agencies faced using mobile phones after large-scale emergencies.
[192] http://www.pswn.gov/admin/librarydocs9/software_defined_radio_report_final.doc
[193] See http://www.publicsafetywins.gov/TechSolutions/TechMain.cfm for descriptions.

communicate with other compliant equipment.[194] In the public safety area, a variety of standards development efforts have been underway with participation from both the private and public sectors.[195,196,197] Prominent efforts include the Project 25 family of standards (also titled Telecommunications Industry Association/Electronics Industry Association [TIA/EIA] 102)[198] and Project MESA, an international effort between the US TIA and the European Telecommunications Standards Institute.[199]

Although standards are an effective strategy to rationalize differences among competing technologies, developing standards can be a difficult process. In order to ensure that standards are well designed, the development process must be open to technical and user input across all relevant communities. The absence of key participants from the process can result in standards that are technologically deficient, do not address all relevant concerns, or do not meet the needs of the user communities. For example, law enforcement and health responders generally require the capability to encrypt communications to address security and patient privacy concerns; if groups with unique needs are not included in standards development then the resulting solutions will likely not be acceptable.

Once developed, the adoption of standards can also be a complex process as manufacturers and users transition to manufacturing, purchasing, and using compliant equipment. The willingness of manufacturers to produce equipment matched to a given standard is dependant on the availability of a market for the products. Acceptance of a standard by both manufacturers and customers can also be affected by assumptions about whether the standards will change over time. A range of government actions, including preferential procurement of compliant equipment directly or through grant programs, can promote the adoption of technology standards.

Non-Technical Approaches for Increasing Interoperability

Although technical solutions can address many interoperability issues, a range of non-technical approaches can also contribute to improved communication among responders at large-scale incidents. Straightforward strategies such as response organizations utilizing a common command post – putting commanders from different organizations close enough to talk face-to-face – can improve interagency communication at the management level.[200] A variety of other non-technical components are also needed to support any effective communications interoperability effort. They include:

- Common terminologies and radio languages to minimize the potential for miscommunication
- Training efforts to ensure responders from different organizations know what interoperability capabilities are available and how to use them
- Procedures to manage communications as incidents increase in size and to define information flows among command levels or functional branches of the response operation
- Broad-based understandings of appropriate radio discipline so responder radio traffic does not undermine the exchange of critical information

[194] Public Safety Wireless Network, "Public Safety Wireless Communications Standards Awareness Guide," http://www.publicsafetywins.gov/PolicySolutions/Standards/PSWNSTDS.pdf
[195] http://www.eeel.nist.gov/810.02/public_safety.html
[196] http://www.agileprogram.org/standards/justnet.html
[197] http://www.nlectc.org/nlectcse/download/pietra_may2002_standards.pdf
[198] http://www.project25.org/; http://www.tiaonline.org/standards/project_25/index.cfm
[199] http://www.projectmesa.org/whitepaper/WhitePaper_MESA_0110.pdf
[200] See, for example, discussion of the Pentagon September 11 response operations in Arlington County, Virginia. "Arlington County After-Action Report on the Response to September 11 Terrorist Attack on the Pentagon," 2002. http://www.co.arlington.va.us/fire/edu/about/pdf/after_report.pdf (Date Accessed: May 2003)

Putting these non-technical components of effective communications interoperability in place requires coordination among public safety organizations during preparedness planning. Current national level efforts to standardize incident management across the responder community, through development and application of the National Incident Management System, could provide a mechanism to put common communications practices and procedures in place.

Residual Needs for Improving Communications Interoperability

As described in the previous sections, a range of efforts have been underway for some time in all levels of government, non-governmental organizations, and the private sector seeking to foster improved communications interoperability among public safety agencies. In both the technical and non-technical arenas, these efforts have developed a range of solutions that can address interoperability problems. In addition, these programs have made progress in promoting the adoption of interoperability solutions by lowering the barriers to coordination among public safety agencies, developing and evaluating new technology options for communications, beginning to address spectrum allocation concerns, and developing both technology and practice standards. These efforts have been valuable both for promoting the development of interoperability among groups of public safety organizations and helping shape the evolution of public safety communications in the future. In some areas and jurisdictions, application of these strategies has resulted in effective solutions for public safety communications needs.

To address interoperability concerns for the nation overall, particularly to ensure effective communications are available at large-scale response operations to terrorist attack or major natural disasters, additional efforts in three areas would be valuable:

- Developing common communications procedures and practices to address the non-technical sources of interoperability failures
- Characterizing the strengths and weakness of different local, State, or regional interoperability strategies
- Developing a clearer understanding of how different local, State, or regional interoperability efforts do or do not address the communications needs of large response operations to terrorist attack or natural disaster

Common Communications Procedures and Practices. Even if all the technological problems that lead to interoperability problems were addressed, common procedures and practices are needed among responding organizations to ensure that communications are effective. If response organizations use different radio codes or transmissions clog the airwaves during major events, no technological solution will be sufficient to address the problems. Because such standardization efforts are most effective when they are aimed broadly, such an effort to build common protocols for response communications would ideally occur at the national level.

Better Characterization of Different Interoperability Efforts. Many efforts at fostering interoperability have been focused at the local, State, or regional level. This has been the case because any near term, national-scale solution to communications interoperability would be very costly, and the appropriate strategy for pursuing such a broad-based effort has not been clear. This smaller-scale approach to these problems has provided the opportunity to pilot test a range of interoperability solutions and match specific strategies to local needs and operational constraints. In light of these practical and functional reasons, there are benefits to pursuing varied approaches to promoting interoperability. However, as a component of such a strategy, there is a need for greater crosscutting examination of the strengths and weakness of the different strategies to achieve interoperability. Although success stories are available for the full range of options described in the previous sections, a systematic understanding is needed of the circumstances where each is most applicable and the local requirements and conditions that influence the

success of different efforts. Such examination would make it possible to more rigorously identify the strengths and weaknesses of different approaches, and to take better advantage of the lessons learned in different interoperability efforts.

Defining Interoperability Needs for National Preparedness. In the context of national-level preparedness, there is also a need to better understand whether diverse local, State, or regional interoperability solutions will meet the communications needs of responders involved in large-scale natural disaster or terrorist incident response operations. Although the fundamental problem – the need for responders and response organizations to communicate – is the same in small-scale events and major disasters, the solutions required may differ. As incidents increase in scale, the numbers of organizations and responders can increase rapidly:

- Routine emergencies likely require involvement of only a few responders from a small number of local response organizations.
- Large local events may require participation of larger numbers of response organizations from the local area and potentially nearby via mutual assistance agreements.
- Major disasters or terrorist attacks can involve hundreds of organizations, potentially drawn from across the country or internationally.

It is not clear that the communications needs for incidents at different scales are the same. For routine events, effective communication may require the ability of all members of an area's public safety agencies to communicate directly with each other at an incident scene. But as incidents increase in size and the potential volume of communications traffic increases, the ability of all responders to communicate on common frequencies or systems could actually hinder the effective transfer of critical information. For such incidents, focusing interoperability efforts on public safety organizations' commanders or within particular response functions may be a more effective approach to meeting response communications needs. There is a clear need to more completely define the communication needs at national scale response operations with respect to communication among the commanders of involved response organizations, different layers of incident management system, and for tactical control of response units.[201]

Without a clear definition of communications needs at major homeland security-related events, it is impossible to determine if or how rapidly current interoperability efforts are addressing those needs or whether additional efforts are needed to supplement them. In some cases, on-going interoperability efforts may already include the ingredients necessary to effectively scale up for national-scale response operations, in others they may not. The diversity of interoperability efforts across the nation makes it difficult to predict how communications will scale up in any particular area. In the event that local efforts are not providing the communications capabilities needed for national-scale events, strategies must be developed to provide them. Such national-scale strategies could apply a number of the solutions discussed in the previous sections, but should be designed to be robust across a range of circumstances and to take advantage of interoperability capabilities that are already or are being put in place at the local, State, or regional level. A crosscutting understanding of these areas from the national perspective could be built through broader based experiments, pilot projects, and exercises aimed at developing generally applicable best practices for large-scale incident communications.

[201] Initial efforts have been made to produce such a template, however it is not clear whether they fully address all the organizations that would be involved in a major terrorist attack or all potential natural disasters. See Imel KJ and Hart JW "Understanding Wireless Communications in Public Safety: A Guidebook to Technology, Issues, Planning and Management," January 2003, 107.

APPENDIX J–TRENDS IN TERRORISM*

Since the advent of the Gilmore Commission over five years ago, more and more individuals in the first responder and policymaking community have begun to monitor trends in terrorist attacks worldwide. In many ways, the attacks on 11 September 2001 represent a watershed in how Americans understand terrorist threats to the U.S. homeland. Yet this attack was not an isolated incident: over worldwide, over 7,700 people have died in terrorist attacks and over 19,100 have been injured during the 1999-2003 tenure of the Gilmore Commission, *not counting the 11 September 2001 attacks*. A substantial number of these casualties occurred as part of the al-Aqsa Intifada in Israel and the Israeli occupied territories, which began in September 2000, almost two years after the start of the Gilmore Commission. Other attacks, however, have been directed at the United States, its citizens and allies overseas, including the October 2002 attacks in against a tourist nightclub in Bali and the November 2003 attack against the British consulate in Istanbul.

This appendix provides a brief overview of patterns in terrorism since January 1999.

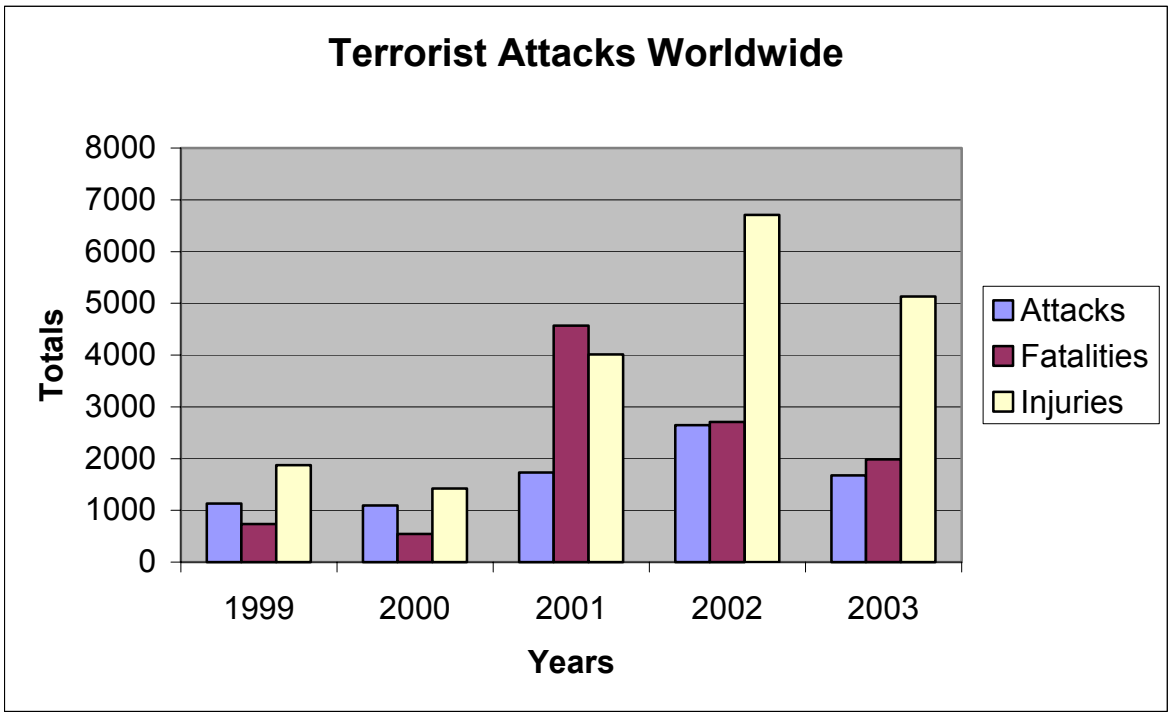


Chart 1

The first chart, "Terrorist Attacks Worldwide," captures the number of terrorist attacks, fatalities, and injuries by year from 1 January 1999 through 1 November 2003. The numbers in these charts are taken from the RAND Terrorism Chronology and the RAND-MIPT Terrorism Incident Database. These databases track terrorist attacks worldwide, defined as follows:

> *Terrorism* is defined by the nature of the act, not by the identity of the perpetrators or the nature of the cause. Terrorism is violence, or the threat of violence, calculated to create an atmosphere of fear and alarm. These acts are designed to coerce others into actions they would otherwise not undertake or refrain from taking actions that they desired to take. All terrorist acts are crimes. Many would also be violations of the rules of war, if a State of war existed. This violence or threat of violence is generally directed against

---

*** Rebekah (Kim) Cragin**

civilian targets. The motives of all terrorists are political, and terrorist actions are generally carried out in a way that will achieve maximum publicity. The perpetrators are members of an organized group and, unlike other criminals, they often claim credit for their acts. Finally, terrorist acts are intended to produce effects beyond the immediate physical damage they cause, having long-term psychological repercussions on a particular target audience. The fear created by terrorists, for example, may be intended to cause people to exaggerate the strength of the terrorists and the importance of the cause, to provoke governmental overreaction, to discourage dissent or simply to intimidate and thereby enforce compliance with their demands.

The databases track both international and domestic terrorist attacks. The attack on 11 September 2001, for example, is defined as an *international* attack in the RAND-MIPT database, because al-Qaeda terrorists crossed international borders into the United States to conduct this attack. Similarly, the previously mentioned attack by the Jemaah Islamiyah in Bali is also defined as *international*, because it targeted foreign tourists. In contrast, the 1995 attack by Timothy McVeigh in Oklahoma City is defined as a *domestic* attack, because it was conducted by a U.S. citizen, with primary residence in the United States, against a U.S. target. Similarly, the December 2000 attacks by Jemaah Islamiyah against local Christian churches in Indonesia are defined as domestic attacks.

Chart 1 illustrates the general increase in the number of international and domestic terrorist attacks worldwide during the past five years. The ratio of international to domestic attacks is approximately 1 international attack for every 6 domestic attacks; so of the approximately 1000 attacks in 1999, over 600 were conducted by local groups against local targets. This chart also highlights the significant increase in casualties per attack over this time period. Even disregarding 2001 and the 11 September attack, casualties (fatalities and injuries) witness a disproportionate increase in 2002 and 2003, as compared to attacks. It is difficult to discern what might account for the general increase in terrorist attacks since 1999. The following graph explores one possible explanation: it is the result of suicide bombings in the al-Aqsa Intifada.

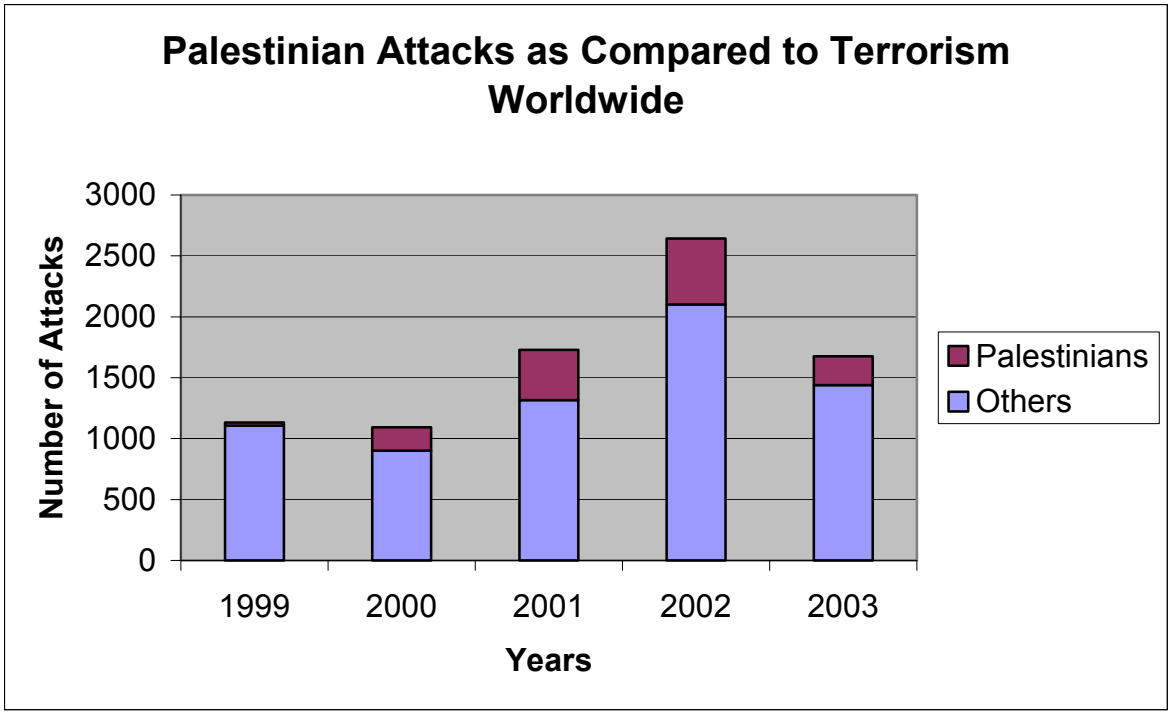


Chart 2

As mentioned previously, the al-Aqsa Intifada arguably represents another significant event in the chronology of terrorist attacks during the past five years. The second chart, "Palestinian Attacks as Compared to Terrorism Worldwide," therefore, highlights the proportion of terrorist attacks that take place in Israel and the Israeli occupied territories. These attacks have clearly increased since the beginning of the al-Aqsa Intifada in September 2000, yet the proportion of attacks is not as significant as one might expect from media coverage. Indeed, these attacks do not appear to alter the general trend in terrorism worldwide, as illustrated below. Comparing Chart 1 (above) and Chart 3 (below), both demonstrate a general increase in the number of terrorist attacks since 1999, as well as a disproportionate increase in casualties per attack.

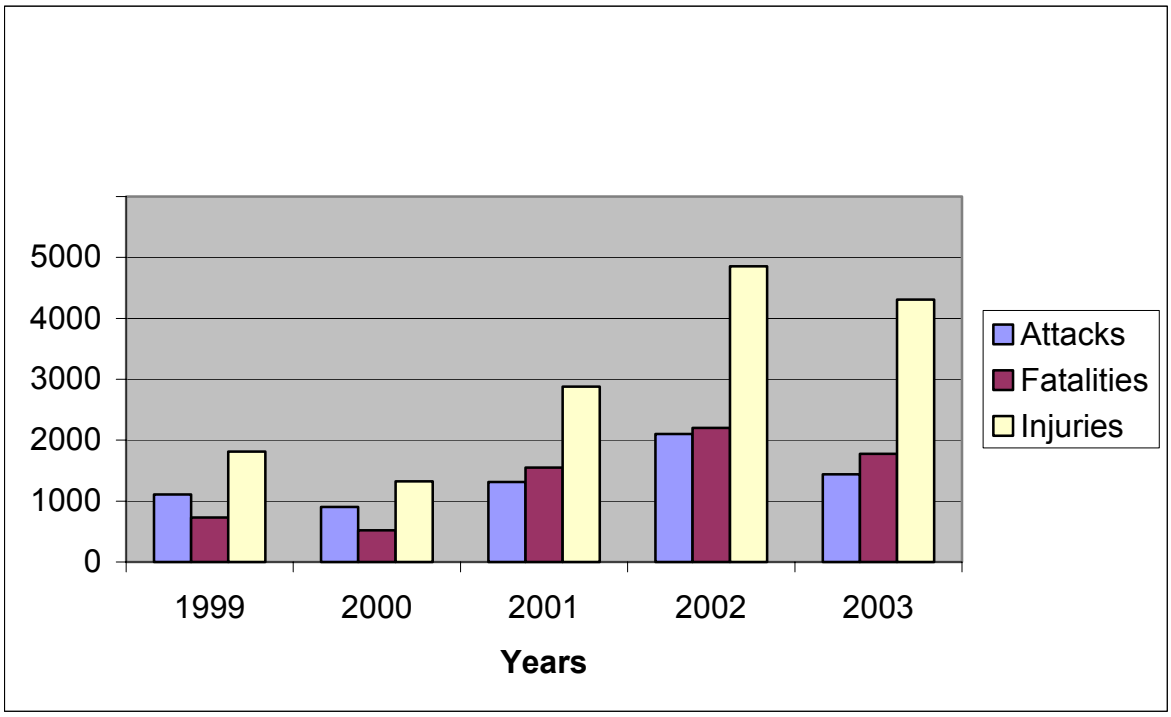


Chart 3

This third chart, "Terrorism Worldwide: Subtracting 9/11 and Attacks in Israel, West Bank, and Gaza" follows the same basic pattern of attacks as the first chart. Indeed, the primary difference is found in the fatalities figures for 2001, which is due to the al-Qaeda attacks on the World Trade Center in New York and the Pentagon.

Finally, Chart 4, "Pattern's In Lethality of Terrorists Attacks," (as well as Chart 1) illustrates a fairly significant trend in terrorism: fatalities per attack have increased. Indeed, prior to 2001, the number of fatalities per attack averaged well below 1. Now this trend has reversed, with fatalities trending higher on average compared with the number of attacks per year.

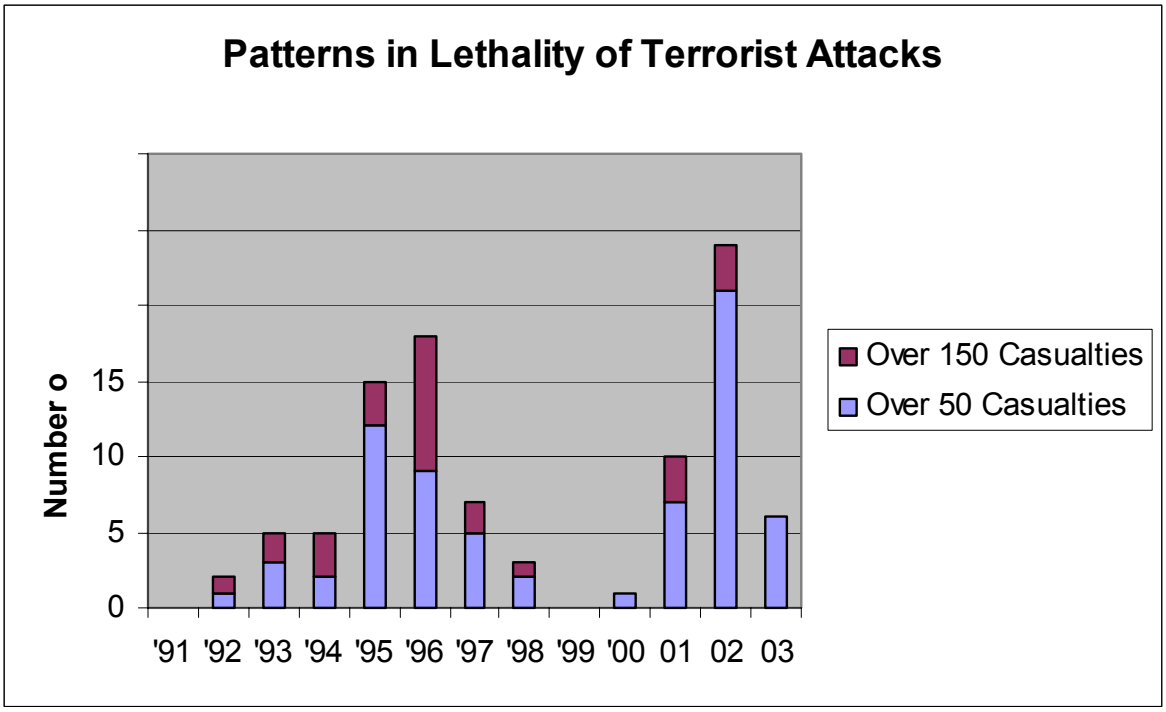

Patterns in Lethality of Terrorist Attacks
Number o
0
5
10
15
'91 '92 '93 '94 '95 '96 '97 '98 '99 '00 01 02 03
Over 150 Casualties
Over 50 Casualties

Chart 4

APPENDIX K—STATUS OF PREVIOUS ADVISORY PANEL RECOMMENDATIONS

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Border	That the Office of Homeland Security create an intergovernmental border advisory group, with representatives of the responsible Federal agencies and with State, local, and private sector partners from jurisdictions with significant ports of entry			X		This recommendation has been partially implemented. A border advisory group has been established within the DHS' Directorate for Border and Transportation Security. The coordination of Federal border security activities has been strengthened by the consolidation of border security organizations and authorities within DHS. A Policy Coordination Committee of the Homeland Security Council has been established to cover border security, territorial waters, and airspace security.
Border	That the Office of Homeland Security facilitate the full integration of affected Federal, State and local entities, including U.S. Coast Guard "Captains of the Port," representatives of airports of entry, and border crossing communities, into local or regional "port security committees," as well as into any adjacent Joint Terrorism Task Force (coordinated by the FBI) or other interagency mechanisms			X		This recommendation is being implemented in the maritime domain. According to DHS, as of 2002 "port security committees [had] already been informally established around the country and [new regulations] establish Area Maritime Security Committees that will address the complex and diverse security needs of each of our 361 ports." The Committees comprise representatives from "federal, state and local agencies, industry" and other organizations.
Border	That the Office of Homeland Security ensure that all agencies with border responsibilities are included as full partners in the intelligence collection, analysis, and dissemination process, as related to border issues			X		Border agencies under DHS collect information and participate in analysis at DHS as well as contributing to intelligence activities at the TTIC.
Border	That the Office of Homeland Security create a "Border Security Awareness" database system to collect and disseminate information about immigration and border control; and that the Congress mandate participation of relevant Federal agencies and provide adequate resources to fund it			X		The Enhanced Border Security Act of 2001 includes a plan to "develop and implement a unified electronic data system to provide real-time access to relevant law enforcement and intelligence database information." It also includes a plan for Entry and Exit (E/E) Data System to be used in confirming identities.
Border	That the Congress enact legislation requiring all shippers to submit cargo manifest information on any shipment transiting U.S. borders at a minimum simultaneous with the arrival of such goods at any U.S. port of entry, with the imposition of severe penalties for noncompliance			X		U.S. Customs Service's Container Security Initiative (CSI) went into effect in February 2003. CSI tightens reporting requirements for cargo coming into the United States. The initiative includes a 24-hour Advance Cargo Manifest Declaration Rule, affecting ocean-going cargo. Land and air shipments are subject to the regulations as of October 1, 2003. Under the CSI plan, Customs is also enlisting international ports to comply with tighter security practices and will set rules for maintaining the integrity of cargo at a later date.
Border	That the President direct the establishment of "Trusted Shipper" programs within the relevant agencies of government			X		FAA strengthened the Known Shipper Program on October 9, 2001 TSA strengthened this program. Passenger air carriers, all-cargo carriers, and freight forwarders are now responsible for verifying a customer's status. TSA is also moving forward with the Known Shipper Database and automated Indirect Air Carrier certification/recertification and plans full deployment of the database in FY 04. A 'trusted shipper' program was also implemented by U.S. Customs. It is known as the Importer Compliance Monitoring Program. When Customs is satisfied that a shipper is 'low-risk', after both self-audits and examination by Customs, it is issued a 'trusted shipper' designation. This year Secretary Ridge also announced the extension of the FAST program, which has been in place on the Canadian border, to the southern U.S. border. The FAST program is a 'trusted shipper' program for trucks that can navigate the borders more quickly through preregistration and screening.

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Border	That the Congress, in consultation with appropriate Executive Branch agencies, expand Coast Guard authority to include vessels that are owned in a majority percentage by U.S. persons			X		Under the Customs Enforcement Statute (19 USC. §1581a), which applies to the so-called "customs waters" of the United States, the Coast Guard may "...go on board any vessel and examine, inspect, and search the vessel and examine every part thereof and any person...or cargo on board, and to this end may...stop such vessel." This applies to both U.S. and foreign vessels without regard to whether the vessel is bound for the U.S. The Maritime Transportation Anti-Terrorism Act of 2002 (HR 3983) establishes a requirement for the Coast Guard to assess the effectiveness of security systems in certain foreign ports, and to deny entry to vessels from ports that do not maintain effective security.
Border	That the Congress increase resources for the U.S. Coast Guard for homeland security missions			X		increase of $1 billion over FY 2002). The President's FY 2004 Budget requests an additional $500 million, a 10% increase over the FY 2003 enacted level. Since 2001 the Coast Guard, has seen the largest increase in its operating expenses since World War II. These new dollars will fund the hiring of 2,200 active-duty personnel, including 160 Sea Marshals for armed escort of high-interest vessels. The increase includes funding for an enhanced Coast Guard presence and response, including support for 44 port security response boats, six new maritime SWAT teams, and increased armed boardings, escorts, and patrols. There are $105 million available in grants for ports across the county to improve security. (DHS website)
Border	We recommend that the U.S. government negotiate more comprehensive treaties and agreements for combating terrorism with Canada and Mexico			X		New security arrangements have been established with Canada. The US-Mexico Border Partnership Action Plan was established in March 2002. The plan is a 22-point agreement to build a smart border for the 21st century that will better secure the U.S.-Mexican border while simultaneously speeding the legitimate flow of goods and people across it
Critical Infrastructure Protection	That the President direct that the interagency policymaking panel on critical infrastructure include representatives form State and local governments, as well as the private sector			X		An advisory panel has not been created. However, DHS (National Cyber Security Division) is considering options for interagency and outside expert advisory organizations. In addition, DHS is planning a national “Cyber Security Summit” to bring together representatives from across the critical infrastructures, industry, government and academia to collaborate on solutions for security challenges identified in the White House National Strategy to Secure Cyberspace.
Critical Infrastructure Protection	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 finding to the President and the Congress			X		The recommended commission has not been created.
Critical Infrastructure Protection	That the President establish a government-funded, not-for-profit entity that can represent the interests of all stakeholders, public and private---national security, law enforcement, other government functions, and business and industry concerns---to provide cyber detection, alert, and warning functions			X		To counter cyber attacks across the internet, the DHS (National Cyber Security Division) established in 2003 a partnership with Carnegie Mellon University’s CERT Coordination Center to create US-CERT, a not-for-profit organization coordinating prevention, protection, and response. US-CERT plans to expand to include partnerships with private sector security vendors and domestic and international organizations. These groups will cooperate to prevent and respond to cyber attacks.
Critical Infrastructure Protection	That the Congress and the Executive Branch convene a "summit" to address, on an urgent basis, necessary changes to a wide range of federal statutes in order to provide necessary protection and incentive changes that would enhance cyber assurance			X		In December 2003, DHS convened a National Cyber Security Summit, which focused on establishing common criteria for detecting and reporting threats as an optimal incident response.
Critical Infrastructure Protection	That the Congress create a special "Cyber Court" patterned after the court established in the Foreign Intelligence Surveillance Act FISA			X		A Cyber Court has not been created.

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Critical Infrastructure Protection	That the Office of Homeland Security develop and implement a comprehensive plan for RDT&E to enhance cyber security			X		In January 2003, the Institute for Information Infrastructure Protection (I3P) unveiled its Cyber Security Research and Development Agenda, which identifies critical areas that require significant research and development to help secure the nation's information infrastructure. The I3P, a consortium of 23 leading cybersecurity research institutions from academia, national labs and nonprofit organizations, is funded by the Commerce Department's National Institute of Standards and Technology. On November 27, 2002, President Bush signed into law the Cyber Security Research and Development Act (P.L. 107-305), authorizing nearly $903 million over five years to the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST). The funding will go towards an array of programs to improve basic research in computer security, encourage partnerships between industry and academia, as well as to generate a new cybersecurity workforce.
Critical Infrastructure Protection	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				X	There are no NIEs underway or planned on this subject. However, the National Intelligence Council is completing an NIE on worldwide biological weapon threats, which covers certain aspects of the terrorist threat to U.S. agriculture. USDA has conducted a comprehensive assessment of threats posed by terrorists and vulnerabilities of domestic and imported food. The FBI is conducting a comprehensive assessment of the terrorist threat to the U.S. homeland.
Critical Infrastructure Protection	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				X	The National Strategy for Homeland Security designates agriculture as a critical infrastructure. Agricultural production and food are represented in the NRP.
Critical Infrastructure Protection	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				X	The USDA is expanding its training of lab personnel and testing capabilities. USDA has established the National Animal Health Laboratory Network -- a network of Federal and State resources that expands lab capacity and permits a rapid response to animal health diseases. Certain labs operated by States and universities will cooperate in disease surveillance.
Critical Infrastructure Protection	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 loses following an agroterrorism attack; and that the Secretary of Health and Human Services should develop a parallel system for non-meat or poultry food				X	This recommendation has not been implemented. There is no clear path to Federal relief for agricultural and food producers who suffer losses caused by an agroterrorism attack. Such losses are not clearly covered in the Agricultural Assistance Act of 2003, which was established primarily to aid producers who suffer losses caused by drought. The Terrorism Risk Insurance Act of 2002 excludes crop and livestock operations from Federal compensation programs for insured losses resulting from acts of terrorism.
Critical Infrastructure Protection	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 and 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				X	USDA has developed new guidance documents on preparedness; it is distributing them to industry and posting them on the internet. USDA is conducting training seminars to boost awareness of foreign animal diseases. USDA is conducting exercises with Federal and State organizations as well as attack simulations.
Critical Infrastructure Protection	That the Congress establish and that the President support an Independent Commission to suggest strategies for the protection of the nation's critical infrastructures				X	The National Infrastructure Advisory Council (NIAC) met on Wednesday, January 8, 2003. The Council advises the President on the security of information systems for critical infrastructure supporting other sectors of the economy, including banking and finance, transportation, energy, manufacturing, and emergency government services. At this meeting, the Council continued its deliberations on comments to be delivered to President Bush

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
						concerning the draft National Strategy to Secure Cyberspace.
Critical Infrastructure Protection	That the President direct that the National Intelligence Council perform a comprehensive National Intelligence Estimate on the threats to the nation's critical infrastructure				X	There are no NIEs underway or planned on these subjects; however, the National Intelligence Council is completing an NIE on worldwide biological weapon threats, which covers certain aspects of the terrorist threat to infrastructure in the U.S. homeland. The FBI is conducting a comprehensive assessment of the terrorist threat to the U.S. homeland. IAIP is responsible for vulnerability assessments for CIP.
Critical Infrastructure Protection	That DHS elevate the priority of measures necessary for baggage and cargo screening on commercial passenger aircraft, especially non-passenger cargo				X	New screening measures are being implemented or developed by DHS.
Critical Infrastructure Protection	That DHS, in conjunction with the airline industry, develop comprehensive guidelines for improving the security of general aviation				X	TSA plans to issue formal guidelines early next year for improving security at more than 18,000 airports and landing strips used by about 214,000 general aviation aircraft. In November 2003 an aviation industry group advising DHS proposed guidelines for the Department's review and consideration.
Critical Infrastructure Protection	That DHS make dam security a priority, and consider establishing regulations for more effective security of dam facilities				X	Many state laws protect dams. FERC has worked with the FBI and DHS to assess vulnerabilities, develop a comprehensive security plan, and has obtained security clearances for some dam officials. In September 2002, FERC issued a notice of proposed rules 18 CFR parts 375 and 388, which would restrict public information about FERC's critical infrastructure. The Bureau of Reclamation issued Directives and Standards FAC 01-06, to establish the requirements for performing an annual Reclamation-wide assessment of dam safety, security, and related operations and maintenance activities. The annual reporting requirements are intended to promote the collection of factual input and objective evidence to assess the effectiveness of dam safety, security, and related operations.
Critical Infrastructure Protection	That the President direct the merger of physical and cyber security policy development into a single policy entity in the White House				X	The White House's Homeland Security Council develops and coordinates policy on physical and cyber security issues.
Critical Infrastructure Protection	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				X	This recommendation has not been implemented.
Health and Medical	That the Assistant Director for Health and Medical Programs seek advice and input from Federal, State, and local public health officials, and from representatives of public and private medical care providers, to ensure that such issues are an important part of the national strategy		X			The President's Homeland Security Council Executive Order (March 2002) established the Homeland Security Advisory Panel and several Senior Advisory Committees, including one on Emergency Services, Law Enforcement, and Public Health and Hospitals.
Health and Medical	That the National Office for Combating Terrorism consult with the professional organizations, especially those with licensing or certification requirements, to find acceptable methods to implement such programs, including the prospect of providing Federal resources to support certified training programs		X			Several organizations both not-for-profit and for-profit now offer continuing medical education and training. For instance, the American College of Radiology, the American Medical Association, the CDC, the Emergency Management Institute, the Office of Emergency Preparedness in DHHS, and the American Institute of Homeland Defense. These are just a few and do not suggest an endorsement. However, there is no unified, agreed upon overall certification for medical preparedness for terrorism. DHHS announced $26.6 million in new grants to strengthen bioterrorism training and education for the nation's health professions workforce as part of DHHS' Bioterrorism Training and Curriculum Development Program, created with the passage of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Health and Medical	Medical authorities must establish standards for hospital facilities that include minimum capabilities in every hospital to treat victims of a terrorist attack		X			As part of the National Bioterrorism Hospital Preparedness Program that was funded at a level of $498 million in FY03, HRSA grant awardees are to develop a work plan that includes six priority areas, each with critical benchmarks, which must be implemented. Measurable milestones, and a proposed budget must also be provided. Under Priority Area #2: Regional Surge Capacity for the Care of Adult and Pediatric Victims Critical Benchmark #2-1: the awardee must establish a system that allows the triage, treatment and disposition of 500 adult and pediatric patients per 1,000,000 population, with acute illness or trauma requiring hospitalization from a biological, chemical, radiological or explosive terrorist incident. Such facilities must be able to support the initial evaluation and treatment of 10 adult and pediatric patients with clinical contagious syndrome suggestive of smallpox, plague or hemorrhagic fever, prior to movement to a definitive isolation facility.
Health and Medical	The National Office should review existing Federal and State authorities for mandatory or prescriptive activities such as vaccination and quarantine. It should provide reports that will ensure that Federal, State, and local response entities have a mutual understanding of the authorities and procedures at all levels of government		X			The Model State Health Emergency Powers Act was introduced or adopted in 43 states or territories as of August 11, 2003. CDC established a website dedicated to protocols for preparation for, and response to, catastrophic events. This site contains information for clinicians, health departments and other decision makers.
Health and Medical	Adequate stockpiles of vaccines should be created and made accessible for rapid response to a terrorist biological attack		X			In 1999 the CDC and DVA started the National Pharmaceutical Stockpile. NPS originally had 8 push packages of pharmaceuticals and medical supplies and currently has 12. In 2003, NPS was transferred to DHS and renamed the Strategic National Stockpile. DHHS designated surge capacity for 500 patients in each state or region as critical benchmark of its Bioterrorism Hospital Preparedness Plan in 2002. In July 2002, the Bush administration purchased $428 million of smallpox vaccine and now there are 286 million doses available. In June 2002 DoD and DHHS officials announced a cooperative effort for response to anthrax incidents. DoD made available the anthrax vaccine to stockpile for civilian use.
Health and Medical	Medical entities such as the Joint Commission on Accreditation of Healthcare Organizations should conduct periodic assessments of medical facilities and capabilities. Evaluation criteria should include a comprehensive, clear, coordinated, and testable response plan. Medical facilities should test their plans, preferably annually, and ideally through a multi-disciplinary exercise with all response disciplines		X			HRSA established the Hospital Preparedness Program, which is dedicated to upgrading the preparedness of the Nation's hospitals and public health entities to respond to bioterrorism and other outbreaks of infectious disease. This programs works to develop and implement regional plans to improve the capacity of hospitals, their emergency departments, outpatient centers, EMS systems, and other collaborating health care entities for responding to incidents requiring mass immunizations, treatment, isolation and quarantine in the aftermath of bioterrorism of other outbreaks of infectious disease. The first year of this program (2002) was dedicated to conducting a needs assessment.
Health and Medical	Medical and health authorities should establish critical information gathering and dissemination, especially for CBRN attacks. They should simplify and standardize mandatory reporting		X			CDC's Health Alert Network was established to provide communications capabilities at all State and local public health laboratories. Connecting public health and clinical laboratories is a Critical Benchmark of DHHS' 2002 Emergency Supplemental Funding.
Health and Medical	That Federal, State, and local entities as well as affected private-sector medical organizations fully implement the American Medical Association (AMA) "Report and Recommendations on Medical Preparedness for Terrorism and Other Disasters"			X		A unified public-private entity at the federal level has not been created; however, some of the sub recommendations have been implemented in part. As noted in 41 above several organizations are providing education and training, the CDC and others also provide on-line informational resources, the CDC disseminated the model plan for mass smallpox vaccination and several pilot programs are ongoing with respect to improving surveillance and reporting of diseases.
Health and Medical	That medical systems fully implement the JCAHO Revised Emergency Management Standard			X		The new Emergency Management standards for hospitals, long term care, behavioral health, and ambulatory care were implemented on January 1, 2001, introducing new concepts into existing standards and infusing the concept of community involvement into the management process. The revised standards broaden the framework provided in the standards to assist organizations in preparing for and managing a variety of potential emergencies

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Health and Medical	That the Congress provide sufficient resources to the DHHS for full implementation of related CDC and public health preparedness programs including Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response			X		FY 02, 03, and 04 budgets allocated $940 million for State and local bioterrorism preparedness. A portion of this amount was made available to support disease detection and outbreak control, including epidemiological and medical response; State, local and regional preparedness planning and coordination; and the conduct of training exercises that included State public health and hospital systems.
Health and Medical	That the Congress provide sufficient resources to the DHHS for full implementation of related CDC and public health preparedness programs including fully resource the CDC Laboratory Response Network for Bioterrorism			X		FY 02, 03, and 04 budgets allocated $940 million for State and local bioterrorism preparedness. Within this amount, funds were made available to support and enhance the Laboratory Response Network.
Health and Medical	That the Congress provide sufficient resources to the DHHS for full implementation of related CDC and public health preparedness programs including fully resource the CDC Secure and Rapid Communications Networks			X		FY 02, 03, and 04 budget allocated $940 million for State and local bioterrorism preparedness. Within this amount, funds were made available to expand the rapid and secure communications networks
Health and Medical	That DHHS, in coordination with the Office of Homeland Security, develop standard models for health and medical responses to a variety of hazards for use at Federal, State, and local levels and in conjunction with the private sector			X		CDC and NIOSH have large amounts of information on their web pages for response to chemical and biological agents (http://www.cdc.gov/niosh/topics/emres/). The National Disaster Medical System under DHS has developed Standard Patient Treatment Forms. However comprehensive models from a single source are not available. The Association of State and Territorial Directors of Health Promotion and Public Health Education have developed the Model Emergency Response Communications Planning for Infectious Disease Outbreaks and Bioterrorist Events - Second Edition.
Health and Medical	That the Secretary of DHHS reestablish a pre-hospital Emergency Medical Services (EMS) program office			X		This recommendation has not been implemented.
Health and Medical	That the Secretary of Transportation direct the National Highway Traffic Safety Administration's Office of Emergency Medical Service to revise the existing Emergency Medical Technician (EMT) and Paramedic National Standardized Training Curricula, and corresponding Refresher Curricula			X		The US Department of Justice and the Federal Emergency Management Agency have created a self-study program designed to provide the basic awareness training to prepare first responders to respond to incidents of terrorism safely and effectively. This training is designed for Fire, emergency medical, hazmat, incident command and law enforcement responders.
Health and Medical	That the Congress increase Federal resources for exercises that are informed by and targeted at State and local health and medical entities			X		FY 02 budget allocated $940 million for State and local bioterrorism preparedness. A portion of these funds was used to conduct training exercises that included State public health and hospital systems.
Health and Medical	That the Office of Homeland Security, with advice from its related national advisory board and in coordination with DHHS and DVA, review and recommend appropriate changes to plans for the stockpile of vaccines and critical supplies			X		Since September 11, 2001, the stockpile has been transferred to DHS, renamed the Strategic National Stockpile and enhanced as follows: supplemental funds have been appropriated to expand the stockpile and to acquire additional antibiotics and pediatric-related supplies; blast, burn and trauma supplies have been added to the stockpile; the number of deployable "push packages" that are located at 10 sites across the United States has increased from 8 to 12; the SNS program has increased the technical assistance that it provides to State and local emergency response planners and developed and disseminated a guidance document to prepare planning officials to receive and distribute materials in the event of an emergency. Additionally, SNS staff conduct site visits where they assess state and local SNS preparedness plans, conduct classroom training, and provide hands-on training by supporting State and local emergency response exercises. The SNS program is now responsible for storing and transporting anthrax and smallpox vaccines.
Health and Medical	That the Office of Homeland Security, on the advice of its related national advisory board, and in coordination with the responsible Federal agencies, develop a comprehensive plan for the full spectrum of medical and health research for terrorism-related medical issues, including the psychological repercussions of terrorism and pre-hospital interventions			X		The bioterrorism research initiative represents the largest single increase in resources for any initiative in the history of NIH. The funding level requested for FY04 would support an estimated 1,000 biodefense research awards. NIH is also establishing a new network of 8 regional extramural Centers of Excellence for Biodefense and Emerging Infectious Diseases. The new centers will help bring together and stimulate the best work in the biodefense field, as well as helping to develop the base of scientific expertise needed for aggressive ongoing research.

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Health and Medical	That the Secretary of DHHS, in conjunction with the Office of Homeland Security and its related advisory board, conduct a thorough review of the authorities, structures, and capabilities under MMRS and NDMS			X		On Jan. 24, 2003 DHHS Secretary Tommy G. Thompson announced more than $200 million in funding for the first installment in the $1 billion designed to rebuild state and local public health infrastructure. The areas to be targeted in this first round included the Metropolitan Medical Response System. The MMRS funding will add an additional 25 new cities to those which have already received funding in past years and will mean that 80 percent of the U.S. population will be covered by an MMRS plan. On March 1st, 2003, MMRS joined the Federal Emergency Management Agency (FEMA) and other programs from the DHHS, DOE, and DOJ to become the Emergency Preparedness and Response Directorate of the new Department of Homeland Security.
Health and Medical	That the Office of Homeland Security develop an information and education program on the legal and procedural problems involved in a health and medical response to terrorism, and in coordination with the Department of Justice and the American Bar Association, consider the efficacy of model laws or other programs to enhance future responses to such events			X		To unify and update the laws relating to health and medical response to terrorism DHHS commissioned Larry Goston to draft the Model State Emergency Health Powers Act. On December 11, 2002, CDC's Public Health Law Program, the Association of State and Territorial Health Officials (ASTHO), and the National Association of County and City Health Officials (NACCHO) sponsored a workshop on selected legal and policy issues related to public health legal preparedness for bioterrorism.
Health and Medical	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				X	Support on the order of $1 billion per year was budgeted for 2002 and 2003.
Health and Medical	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				X	On September 2, 2003, DHS announced plans to create a system that would result in "One Access Point for State and Local Grants". With the implementation of this plan, State and local governments will only have to contact one office in DHS for information related to funding opportunities, as well as to receive grant guidance, coordination, and oversight.
Health and Medical	That DHHS, in consultation with the 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				X	DHHS is currently funding (FY04) several efforts to develop measures and evaluation tools for public health and hospital preparedness.
Health and Medical	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				X	There are several models for local workforce needs, but no specific federal model for terrorism response has been developed.
Health and Medical	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				X	In August 2002, DHHS created the Secretary's Council on Public Health Preparedness. The Council's responsibilities include assessing the nation's hospitals' preparedness for terrorist attacks. As a result of this assessment, $135 million was allocated for hospital preparedness in FY02; $518 million was allocated in FY03. The Hospital Preparedness program was initiated in 2003 to help States, territories, and municipalities develop and implement biological and chemical preparedness plans focused on hospitals. Funds are being used to set up hospital preparedness offices with bioterrorism coordinators and medical advisors, complete needs assessments, develop and implement regional hospital plans to manage a large scale epidemic, and to focus on four first priority areas: medication and vaccine distribution, isolation and decontamination, communication, and biological disaster drills.
Health and Medical	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				X	On April 1, 2003, the CDC dedicated the Marcus Emergency Operations Center, a new facility that strengthens the agency's response to health crises and promotes faster, better-coordinated responses to public health emergencies across the United States. The secure communications hub supports, organizes and manages all emergency operations between CDC, DHHS, as well as federal intelligence and emergency response officials, DHS, and state and local public health officials.

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Health and Medical	That 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				X	DHHS's FY04 budget allocated $518 million for public health and medical emergencies
Health and Medical	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				X	This recommendation has not yet been implemented.
Health and Medical	That DHHS evaluate current processes for providing required technical assistance to States and localities, and implement changes to make the system more responsive				X	In early 2003, Recently, the SNS prepared specific guidance and provided technical assistance to states to help them effectively manage the deployment of the SNS within their jurisdictions. In September 2003, CDC issued guidelines on how state and local public health officials should respond to a smallpox outbreak including technical assistance with respect to mass vaccination. CDC is working to strengthen its internal Emergency Preparedness and Response infrastructure to provide enhanced technical and programmatic assistance to state and local health agencies.
Health and Medical	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 goals				X	This recommendation has not yet been implemented.
Health and Medical	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				X	In 2002, NIAID developed a strategic plan for counter-bioterrorism research. The NIAID biodefense research agenda focuses on studies of microbial biology and host responses to microbes; the development of new vaccines, therapies, and diagnostic tools; and the development of research resources such as appropriate laboratory facilities. NIAID is receiving significantly more resources - $1.6 billion in FY03. NIAID is coordinating genome sequencing for biological agents in Categories A-C with USDA, DOE, and the CDC. NIAID also established a cooperative program with the U.S. Army Research Institute for Infectious Diseases and is working with DoD on the development of therapeutics and vaccines.
Health and Medical	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 legislations 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				X	As of August 11, 2003, the Act has been introduced in whole or part through bills or resolutions in 43 state legislatures, the District of Columbia, and the Northern Mariannas Islands. Thirty-two states [AL, AZ, CT, DE, FL, GA, HI, IA, ID, IL, LA, ME, MD, MN, MO, MT, NV, NH, NM, NC, OK, OR, PA, RI, SC, SD, TN, UT, VT, VA, WI, and WY] and DC have passed bills or resolutions that include provisions from or are closely related to the Act.
Health and Medical	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 (pg. 64) 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				X	HIPAA permits covered entities to disclose protected health information to law enforcement in certain circumstances.
Health and Medical	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				X	DHS has a number of initiatives aimed at public education and information sharing. Examples include the “Ready.gov” program (see http://www.ready.gov/), projects undertaken via the Citizen Corps (see http://www.citizencorps.gov/), and work with the American Red Cross’ national network of citizen volunteers.

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Health and Medical	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				X	NIMH is conducting and supporting research relevant to preparation for and response to the psychosocial sequelae of terrorism and mass emergencies. It integrates basic science, clinical practice and health care system factors in two broad groups: 1. Terror Victim Research and 2. Terrorism Related Research.
Health and Medical	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				X	The Intelligence Community has enhanced its ability with respect to bioterrorism threats.
Health and Medical	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				X	Deployment of the Strategic National Stockpile (formerly NPS) is Critical Capacity #4 defined in the CDC cooperative agreements to improve emergency public health preparedness including bioterrorism. As such plans, training and testing are expected. These critical capacities are required in the State plans and are to be implemented in the budget period. The consequence for not doing so is unclear. The CDC is working on measuring readiness by transitioning from critical capacities to readiness goals and readiness indicators.
Health and Medical	That DHHS, in collaboration with DHS and DoD, establish a national strategy for vaccine development for bioterrorism, which will be consistent with the nations needs for other vaccines				X	An overall vaccine strategy that covers basic research through manufacturing and post marketing surveillance has not been developed, but NIAID in cooperation with DoD has developed a research strategy and agenda that includes vaccines. In addition the President signed BioShield, which is meant to encourage industry participation in bioterrorism defenses.
Health and Medical	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 safer smallpox vaccine				X	In December 2002, President Bush, announced plans to vaccinate 500,000 key workers against the disease and an intention that by mid-2003 10 million US citizens would be vaccinated. In February 2003, DHHS announced the award of two contracts totaling up to $20 million in first-year funding to develop safer smallpox vaccines. Because of the urgent need for safer smallpox vaccines, the new contract emphasizes timely completion of predetermined objectives.
Intelligence	Undertake continuing, comprehensive and articulate assessments of potential, credible, terrorist threats within the United States, and the ensuing risk and vulnerability assessments	X				In 2003, the FBI established the position of Executive Assistant Director for Intelligence and an Office of Intelligence. The new office is completing a near-term threat assessment and has begun work on a longer-term assessment of domestic threats from terrorism, foreign intelligence, cybercrime, and organized crime.
Intelligence	More attention be paid to assessments of the higher-probability/lower-consequence threats—not at the expense of, but in addition to, assessments of the lower-probability/higher-consequence threats	X				The FBI is making a comprehensive assessment of the terrorist threat to U.S. territory. It is not clear that higher probability/lower consequence threats will be a focus of the Bureau's analysis
Intelligence	More needs to be and can be done to obtain and share information on potential terrorist threats at all levels of government, to provide more effective deterrence, prevention, interdiction, or response, using modern information technology	X				Modest improvements in intelligence sharing have been achieved. IAIP coordinates and analyzes information on terrorist threats, assesses vulnerabilities, and disseminates information. The TTIC was created in May 2003 to coordinate and provide terrorism-related threat analysis to the President, DHS, and other federal agencies. The DCI oversees TTIC. TTIC will house a database of terrorists that officials across the country will be able to access and act upon. TTIC is staffed by representatives of the CIA, NSA, FBI, DHS, DOD, and DHS. In August 2003, the GAO determined that improvement is required to establish processes and procedures for sharing information at all levels of government. In August 2003, DHS Secretary Ridge announced that governors and other state-level officials would be granted security clearances to receive classified information on homeland security developments and activities. Ridge stated that DHS would work through governors to reach local officials. The White House has directed DHS to develop by March 2004, a revamped system for information sharing between all government agencies and the private sector.
Intelligence	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		X			The FY02 Intelligence bill (Section 403) directed that the guidelines be rescinded. The CIA formally rescinded the 1995 recruiting guidelines just after the July 2002 release of the House Permanent Select Committee on Intelligence, subcommittee on Terrorism and Homeland Security report on Counterterrorism Intelligence Capabilities and Performance Prior to 9-11

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Intelligence	An expansion and improvement in research, development, test, and evaluation (RDT&E) of reliable sensors and rapid readout capability, and the subsequent fielding of a new generation of measurement and signature intelligence (MASINT) technology based on enhanced RDT&E efforts		X			According to the intelligence community's Central MASINT Office, enhanced RDT&E efforts have been pursued and have already led to the deployment of improved MASINT technologies. The MASINT Office is also expanding the number of personnel focusing on chemical and biological terrorism threats.
Intelligence	A thorough review, by a panel of Department of Justice (DOJ) officials and knowledgeable citizens outside the Federal government, of the terrorism portion of the Attorney General's "Domestic Guidelines." We recommend that the panel review the domestic guidelines for clarity, in the interests of strengthening them, while providing for the protection of civil rights and liberties		X			After September 11, 2001, AG Ashcroft authorized the FBI to waive the AG guidelines, with headquarters approval, in extraordinary cases to prevent and investigate terrorism and directed a top-to-bottom review of the guidelines to ensure that they provide field agents with the legal authority to prevent terrorist attacks. On May 30, 2002 new AG's Guidelines went into effect .
Intelligence	That the Attorney General direct the Office of Intelligence Policy and Review to modify its procedures to conform to the Foreign Intelligence Surveillance Act statutory requirements		X			Internal policy changes have resulted in processes in line with FISA.
Intelligence	That the National Office for Combating Terrorism foster research and development in forensics technology and analysis and implement an Indications and Warning System for the rapid dissemination of information developed by enhanced forensics		X			According to the Intelligence Community's Central MASINT Office, forensics technology is being improved. A database of microbial agent signatures has been established. The DHS also has a biological forensics research program. DHS is sponsoring research on a national microbial forensics system and has partnered with the FBI to develop the National Bioforensics Analysis Center (BFAC). Details of the Indications and Warning system are classified.
Intelligence	The National Office should promote a system for providing some form of security clearance to selected State and Local officials nationwide, and methods of disseminating classified information to these officials in near real time		X			In 2002, DoJ sponsored and OHS participated in a forum on "Justice Information Sharing" that was co-hosted by the National Governors Association. Key initiatives discussed included the National Homeland Security Advisory System, Homeland Security Notices, a new center for two-way information sharing, and a future, uniform system for information sharing. In August 2003, DHS Secretary Ridge announced that governors and other state-level officials would be granted security clearances to receive classified information on homeland security developments and activities. Ridge stated that DHS would work through governors to reach local officials with critical information. However, there is still a lack of necessary clearances, clearances do not transfer from one Federal agency to another, and information sharing is still insufficient.
Intelligence	That the FBI consider implementing a "Reports Officer" or similar system, analogous to the process used by the CIA, for tracking and analyzing terrorism indicators and warning					The FBI has implemented a "Reports Officer" system.
Intelligence	That agencies of the Federal government increase and accelerate the sharing of terrorism-related threat assessments and intelligence with appropriate State and local officials and response organizations			X		See also item 12. In 2002, the initial integration of collaboration networks for the FBI, local law enforcement, the intelligence community, and the State Department was completed. This initiative enables a range a functions, from secure e-mail exchange to searches of one another's databases. The intelligence community's Open Source Information System (OSIS) now serves as a central hub connecting State's intranet (called Opened) and the FBI's LEO. LEO also serves as the backbone for Joint Terrorism Task Force Information Sharing Initiative pilots, which integrate Federal, State and local databases. In addition, the Terrorist Threat Integration Center (TTIC) commenced operations in January 2003.
Intelligence	That the President direct the establishment of a National Counter Terrorism Center (NCTC)				X	The NCTC was not created. The Terrorist Threat Integration Center was announced by President Bush in his 2003 State of the Union Address and started on May 1, 2003. The TTIC has certain authorities and planned capabilities that had been recommended for the NCTC.
Intelligence	That the collection of intelligence and other information on 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				X	The NCTC was not created. DoJ, working through the FBI, maintains lead responsibility for intelligence collection activities within the United States.
Intelligence	That the Congress ensure that oversight of the NCTC be concentrated in the intelligence committee in each House				X	The TTIC will presumably be principally within the oversight of the intelligence committees

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Intelligence	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 of preparedness and response resources				X	In 2003, the FBI established the position of Executive Assistant Director for Intelligence and an Office of Intelligence. The new office is completing a near term threat assessment and has begun work on a longer term assessment of domestic threats from terrorism, foreign intelligence, cybercrime, and organized crime.
Intelligence	That the Congress and 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. (pg. 48) 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				X	The DHS does not have authority to direct intelligence requirements. Through its participation in the TTIC, the DHS can contribute to an interagency process for establishing such requirements. DHS has a limited organic capability for intelligence analysis.
Research and Development	That the Technical Support Working Group (TSWG) become an adjunct to the National Office for Combating Terrorism in the same manner that it now serves in the NSC process and that it expand its coordination role for technical aspects of RDT&E for combating terrorism		X			While TSWG is still fundamentally a joint DOS-DOD effort, it is now conducting R&D directly for DHS.
Research and Development	That the Assistant Director for RDT&E and National Standards of the National Office for Combating Terrorism either enter into a formal relationship with OSTP or have appropriate members of the OSTP staff detailed to the National Office for Combating Terrorism on a rotational basis		X			OSTP staff are dual-hatted or detailed to DHS and the HSC staff.
Research and Development	That the Assistant for RDT&E for National Standards develop equipment testing protocols and continue to explore the prospect of financial support from vendors for equipment live agent test and evaluation, leading to Federal certification		X			There is a multi-agency collaborative effort to develop a suite of 37 standards for emergency response equipment to be implemented over the next 5 years.
Research and Development	That the Assistant Director for RDT&E and National Standards develop, as part of the national strategy, a comprehensive plan for long-range research for combating terrorism		X			HSARPA has developed both a short and long-term research agenda for combating terrorism.
Research and Development	Expand and consolidate research, development, and integration of sensor, detector and warning systems			X		Expanded research in DHS S&T on sensor technologies
Role of Military	Configure Federal military response assets to support and reinforce existing structures and systems			X		A number of Federal military units—with varying levels of specialized training and equipment—are prepared to provide military support to civil authorities. However, none of these assets are dedicated to the MSCA mission and they could be deployed abroad. The Federal government does fund, and the states control, National Guard Weapons of Mass Destruction Civil Support Teams, small units (22 uniformed military personnel) that deploy to assess incidents and coordinate additional Federal and state response activities.
Role of Military	That the Secretary of Defense seek and that the Congress approve the authority to establish a new under secretary position for homeland security			X		In the FY03 National Defense Authorization Act, the Congress approved the creation of the position of ASD (HD). On 25 March 2003, Deputy Secretary Wolfowitz issued a memo describing the duties of the ASD (HD) as follows: “His principal duty is the overall supervision of the homeland defense activities of the Department under the authority, direction and control of the Under Secretary of Defense for Policy (USD (P)) and, as appropriate, in coordination with the Chairman of the Joint Chiefs of Staff (CJCS). As such, he will oversee HD activities, develop policies, conduct analyses, provide advice, and make recommendations on HD, support to civil authorities, emergency preparedness and domestic crisis management matters within the Department.” The ASD (HD) has direct access to the Secretary of Defense because of his Executive Agent responsibilities for military support to civil authorities.

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Role of Military	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			X		This recommendation has been implemented nearly in full. On 1 October 2002, U.S. Northern Command was formed. The command will reach full operational capability on 1 October 2003 and assume unified command and control of nearly all Federal military forces providing support to civil authorities within the continental United States. Commander, U.S. Pacific Command is responsible for providing similar civil support to Hawaii and the Pacific U.S. Territories. Commander, U.S. Special Operations Command will control counterterrorist operations by federal military forces within U.S. territory.
Role of Military	That the Secretary of Defense direct the development of more detailed plans for the use of the military domestically across the spectrum of potential activities, and coordinate with State and other Federal agencies in the creation of more State- or regional-specific plans. We further recommend that the secretary direct the military departments to institute specific training in military units most likely to be involved in military support to civil authorities and to expand military involvement in related exercises with Federal, State, and local agencies			X		This recommendation has not been fully implemented. Prior to the Panel's 2001 report, the Department of Defense (DoD) had established numerous plans for the use of the military domestically (e.g., "Garden Plot" in response to domestic disturbances and "Graphic Hand" in response to postal emergencies). Since the initiation of Operation Noble Eagle on 12 September 2001, DoD has developed additional plans for homeland defense activities; that is, military combat operations for the air, land, and maritime defense of the United States. According to DoD, it is constrained in developing detailed plans to support the Department of Homeland Security (DHS) until DHS identifies specific requirements for Federal military support.
Role of Military	Expand training and exercises in relevant military units and with Federal, State and local responders			X		NORTHCOM has established response and training requirements for newly created Quick Reaction Forces (QRFs). DoD has for many years conducted programs to prepare military forces for domestic operations. For example, the MACDIS mission is assigned on a rotating basis to state National Guard and selected active Army units, which then train for the mission. According to DoD, numerous interagency agreements provide for civil-military emergency response training. For example, the National Disaster Medical System is a public/private sector partnership that supplements state and local medical resources during disasters or major emergencies. The Federal partners are the DHS, DHHS, DVA, and DoD. NORTHCOM, and its component commands, conduct periodic exercises with civil authorities. Military installations throughout the country routinely participate in disaster response exercises DoD resourced the 32 National Guard WMD-CSTs to conduct monthly exercises with state and local emergency response teams.
Role of Military	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.			X		To date, there have been no requirements established by DHS for the military to support homeland security missions. On 9 July 2003, the Secretary of Defense issued a memorandum directing studies on rebalancing the U.S. armed forces' mix. The Secretary's memo directs a specific study on the Reserve Component's Role in homeland defense. Based upon the established DOD requirements, ASD (RA) prepare a report on Reserve Component Contributions to HD and CS that will recommend the appropriate roles, force mix, priorities, command relationships, and resources required for conducting these missions." In May 2003, LTG Steven Blum, NGB Chief, unveiled a proposal to convert certain NG medical and engineering units into incident response teams. These teams may be based by region. They will not be dedicated to homeland operations. On 21 May 2003, the NGB issued a written description of LTG Blum's plan. According to NGB, Blum's proposal will add to the units' mission essential task lists. LTG Blum has proposed a one-year test of his concept in FY04.
Role of Military	That the Secretary of defense publish a compendium, in layman's terms, of the statutory authorities for using the military domestically to combat terrorism, with detailed explanations about the procedures for implementing those authorities			X		This recommendation has not been implemented. There is no indication that DoD sees a need to develop the recommended compendium at this time. According to DoD, the National Command Authority will make the decision on which statutory authority will be used to deploy Guard forces to meet domestic emergencies, other than State Active Duty. Therefore, DoD does not support the need for a layman's legal primer. Defense Coordinating Officers (DCO), installation commanders, and domestic Joint Task Force commanders are trained in the legal aspects of military assistance to civil authorities, according to DoD.

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Role of Military	That the Secretary of Defense improve the full-time liaison elements located in the 10 FEMA regions and assign those elements expanded missions to enhance coordination with State and local agencies in planning, training, and exercising emergency response missions			X		This recommendation has been partially implemented. According to DoD, its liaison activities have been strengthened since the Panel's recommendation, but there are currently no plans to expand the missions of the Emergency Preparedness Liaison Officer Regional Teams, which currently require the commitment of some 200 military personnel.
Role of Military	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				X	According to DoD, NORTHCOM cannot conduct comprehensive planning for civil support until DHS establishes civil support requirements. Moreover, according to DoD, NORTHCOM's mission is clearly stated as follows: "United States Northern Command will conduct operations to deter, prevent, preempt, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned area of responsibility; as directed by the President or Secretary of Defense, provide military assistance to civil authorities including consequence management operations." This mission statement is broad enough to cover the full spectrum of potential activities that would require the provision of military support to civil authorities (MSCA), DoD says.
Role of Military	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				X	This recommendation has been partially implemented. Commander NORTHCOM will acquire operational control as required over the forces needed to execute missions in NORTHCOM's area of responsibility. NORTHCOM has no assigned forces, other than certain command elements (e.g., JTF-6 and JTF-CS). Commander, U.S. Special Operations Command will control counterterrorist operations by military forces operating within U.S. territory.
Role of Military	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 the Title 10; and the 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				X	This recommendation has not been implemented. However, the DoD has worked with Congress to revise title 10 USC, Section 12304, to permit Reserve component mobilization for response to terrorist incidents. DoD is working with the Congress to further clarify title 10 to permit the President to mobilize all Reserve components, not just the National Guard, in response to domestic "all hazards" disasters. Congress has not consolidated in a single title 10 section the homeland security-related authorities for the use of the military domestically. DoD has no plans to develop a "handbook" on the legal authorities governing the domestic use of the military.
Role of Military	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				X	This recommendation is currently being implemented. The DHS is coordinating a national effort to identify homeland security requirements. The DHS is coordinating with DoD on this effort. Within DoD, the ASD (HD) will establish civil support requirements and direct the Joint Staff and Commander, NORTHCOM to develop plans to meet these requirements.
Role of Military	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				X	Commander NORTHCOM has operational control, as required, over Quick Reaction Forces. Commander NORTHCOM establishes training requirements for the QRFs. However, Commander NORTHCOM does not fund civil support training; thus, he must request that Services fund training to meet his requirements for civil support. Beyond the QRFs, other military units with specialized training are made available to Commander NORTHCOM, as required. NG units within the several states also undergo MACDIS training. It is possible that civil support mission training will be expanded. On 9 July 2003, the Secretary of Defense issued a memorandum (see details above) directing a number of studies on rebalancing the U.S. armed forces' mix of Active and Reserve component personnel. A study on RC civil support training requirements was also completed for ASD Reserve Affairs in May 2003. The Chief of the National Guard Bureau has proposed (see details above) to train and equip certain NG units to provide specialized civil support following a domestic WMD event. This initiative could lead to the creation of dual-missioned NG units.
Role of Military	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				X	This recommendation has been partially implemented. Commander, NORTHCOM submits his civil support training requirements to the Chairman, Joint Chiefs of Staff. The Chairman validates them and passes them on to the Services to develop the capabilities to meet those requirements. However, as mentioned previously, Commander, NORTHCOM does not maintain funds to support this training.

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Role of Military	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 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 a terrorist attack				X	This recommendation has been partially implemented. In response to potential terrorist threats to the United States during Operation Iraqi Freedom, NORTHCOM established a requirement for Quick Reaction Forces. They are not solely dedicated to domestic operations; they can be deployed abroad.
Role of Military	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				X	Existing title 32 USC authority applies to required NG training and selected operational missions. According to DOD, it reviews state requests for title 32 funding of NG personnel performing operational missions on a case-by-case basis. In general, requests that support NG execution of federal missions are considered for title 32 funding. It is the DOD position that DHS grants, not DOD funding, should be the channel used to finance the planning, training and exercises needed by Governors to support their individual state homeland security plans. In addition, DOD is opposed to changes in existing procedures. As DOD sees it, these procedures ensure that Federal Agency requests for military assistance are evaluated and, if approved, fulfilled by military forces in federal status.
Role of Military	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 (pg. 102) 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. (pg. 102) 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				X	This recommendation has not been implemented. Congress has not provided new title 32 authorities for employing the National Guard on a multi-state basis. Federal DoD funds cannot be expended to perform state activities. DoD has no plan to recommend changes to existing Interstate Compact agreements, which have provisions for the interstate deployment of National Guard forces. (Guardsmen deployed under Interstate Compacts do so in a State Active Duty status, where the requesting state reimburses the supporting states.) Finally, it is DoD's position that numerous other federal agencies have responsibility for responding to domestic emergencies that may involve multiple states. Their considerable resources should be exhausted prior to turning to DoD assets.
Role of Military	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				X	This recommendation has not been implemented. As we noted above, new Reserve component roles in Homeland Defense and Military Assistance to Civil Authorities are now under study, as directed by the Secretary of Defense on 9 July 2003. However, it is DoD's position that, before dedicating force structure to any homeland security mission, DHS must establish what missions need to be performed as well as the Federal, State, or local entities that should perform them.
Strategy and Structure	Develop a national strategy to address the issues of domestic preparedness and response to terrorist incidents	X				On 16 July 2002, President George Bush released his "National Strategy for Homeland Security." The Strategy is comprehensive; it covers preparedness and response issues from a national perspective.
Strategy and Structure	There needs to be a "Federal Government Strategy" component of the national strategy—one which clearly articulates Federal responsibilities, roles, and missions, and distinguishes those from state and local ones	X				Federal strategy continues to evolve. Key elements in the strategy are currently established in the National Strategy for Homeland Security, Homeland Security Presidential Directive 5, and the National Response Plan.
Strategy and Structure	The national strategy must have a "bottom-up" approach—thatit be developed in close consultation and collaboration with state and local officials, and the law enforcement and emergency response communities from across the country	X				The National Strategy for Homeland Security was developed principally by the White House. However, State and local input is assisting in the development of the NRP and NIMS.
Strategy and Structure	The national strategy must have the direct leadership, guidance, and imprimatur of the President	X				The President is directing initiatives through his National Strategy for Homeland Security, Presidential Directives, and other instruments.
Strategy and Structure	Comprehensive public education and information programs must be developed, programs that will provide straight-forward, timely information and advice both prior to any terrorist incident and in the immediate aftermath of any attack	X				DHS has a number of initiatives aimed at public education and information sharing. Examples include the "Ready.gov" program (see http://www.ready.gov/), projects undertaken via the Citizen Corps (see http://www.citizencorps.gov/), and work with the American Red Cross' national network of citizen volunteers.

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Strategy and Structure	The national strategy should include incidents involving conventional weapons that have the potential to cause significant casualties or physical damage; as well as incidents involving CBRN devices that may not be capable of producing "mass casualties" but that can, nevertheless, produce considerable fear, panic, or other major disruptions to the infrastructure or economy of the potential domestic target	X				The National Strategy for Homeland Security is an all-hazards strategy.
Strategy and Structure	Further support and develop the NDPO as a focal point for related preparedness information and for directing state and local entities to the appropriate agency of the Federal government for obtaining information, assistance and support	X				In accordance with the Homeland Security Act of 2002, the National Domestic Preparedness Office was transferred to DHS' Directorate for Emergency Preparedness and Response. Current DHS structure suffers from a duplication of emergency preparedness and response efforts. In particular, the existence of the Directorate of Emergency Preparedness and Response and the Office of Domestic Preparedness in separate directorates is confusing for state and local officials and has created problems with interdepartmental coordination, performance accountability, and fiscal accountability. In August 2003, DHS Secretary Ridge informed the National Governors Association that DHS was working to establish a "one stop shop" for Federal homeland security grants and assistance
Strategy and Structure	The Panel recommends that the Congress consider forming an ad hoc Joint Special or Select Committee, composed of representatives of the various committees with oversight and funding responsibilities for domestic preparedness and response, and give such an entity the authority to make determinations that will result in more coherent efforts at the Federal level	X				Three new committees have been established in the Congress for oversight and appropriations: the House Select Committee on Homeland Security, the House Appropriations Committee, Subcommittee on Homeland Security, and the Senate Committee on Appropriations, Subcommittee on Homeland Security. These committees commenced operations in 2003.
Strategy and Structure	The Panel recommends that there be a revision and codification of universal, unambiguous, and easily understandable definitions of the various terms related to combating terrorism and the terrorist threat	X				Homeland Security-related terms and definitions are increasingly becoming standardized with the release of the National Strategy for Homeland Security and the development of the NRP and NIMS
Strategy and Structure	Standardize equipment and communications systems between the different levels of first responders to ensure better compatibility and inter-operability between potential responders	X				DHS has established Project SAFECOM to promote wireless communications interoperability at the Federal, State, and local levels. A number of Federal agencies are pursuing standardization programs (e.g., such as those conducted by the National Fire Protection Association), but these are limited in scope. A comprehensive, national approach to equipment standardization has not been established. Several states have increased investments in inter-operability and some report significant progress that will enhance their response capabilities. Additional coordination with Federal responders is required to support a comprehensive national effort.
Strategy and Structure	The Advisory panel recommends that the next President develop and present to the Congress a national strategy for combating terrorism within one year of assuming office		X			The President released his National Strategy for Homeland Security in July 2002. In his remarks, the President noted that the document is a "national, not a Federal strategy."
Strategy and Structure	We recommend the establishment of a senior level coordination entity in the Executive Office of the President, entitled the "National Office for Combating Terrorism, " with the responsibility for developing domestic and international policy an for coordination the program and budget of the Federal government's activities for combating terrorism		X			October 8, 2002 President Bush established the Office of Homeland Security in the White House.
Strategy and Structure	We recommend the establishment of 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		X			Three new committees have been established in the Congress for oversight and appropriations: the House Select Committee on Homeland Security, the House Appropriations Committee, Subcommittee on Homeland Security, and the Senate Committee on Appropriations, Subcommittee on Homeland Security. These committees commenced operations in 2003. In addition, the House Armed Services Committee created a special oversight panel on terrorism and the House Permanent Select Committee on Intelligence created a subcommittee on Terrorism and Homeland Security.

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Strategy and Structure	We recommend that the Department of Justice, in consultation with the appropriate committees of Congress as well as knowledgeable members of the scientific, health and medical communities, and State and local government, continually review existing statutory authorities and regulations. The purpose would be propose specific prohibitions, or at least mandatory reporting procedures, on the domestic sale and purchase of precursors and special equipment that pose a direct, significant risk of being used to make and deliver CBRN weapons or agents		X			The CDC issued 42 CFR Part 1003 the Possession Use and Transfer of Select Agents and Toxins: Interim Final Rule December 13, 2002, which implements part of Public Health Security and Bioterrorism Prevention and Response Act of 2002 , and the USDA established similar protections under CFR Part 331 and 9 CFR Part 121 the Agricultural Bioterrorism Prevention Act of 2002: Possession, Use, and Transfer of Biological Agents and Toxins. Regulations regarding radiological sources have not changed.
Strategy and Structure	That the National Office for Combating Terrorism foster the development of a protected, single-source web page system, linking appropriate combating terrorism information and databases across all functional disciplines		X			The Federal Government has not established a comprehensive, web-based information clearinghouse.
Strategy and Structure	That the senior emergency management entity in each State function as the prime *Focal Point* for that State for domestic preparedness for terrorism		X			Each State has created a Homeland Security Agency or designated the senior emergency management entity as the *Focal Point* for interacting with the Federal government.
Strategy and Structure	That the Federal Response Plan (FRP) be the single source Federal document for “all-hazards” response planning. All applicable Federal departments and agencies should include their plans to respond to terrorist attacks as annexes to the FRP, in accordance with a specific FRP template. The FRP and the relevant Federal agency plans should include input from State and local entities		X			HSPD-5 directs the DHS Secretary to develop and establish a National Incident Management System and a National Response Plan. According to the HSPD, the NRP will "integrate Federal Government domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan."
Strategy and Structure	That the National Emergency Management Association, in conjunction with the Federal Emergency Management Agency, develop a “model” State plan, flexible enough to fit any State’s specific circumstances, but with certain standard features		X			ABS and NEMA developed a strategic plan for Iowa for terrorist incident preparedness. NEMA used the Iowa plan as a model for other States.
Strategy and Structure	That the National Office for Combating Terrorism conduct inventories of State and local programs for capabilities that can be utilized in a national context, especially training and exercise programs		X			This recommendation has been partially implemented. The DHS is currently working with the several States to access their level of preparedness and to identify capability gaps that require Federal assistance to mitigate. DHS has conducted an inventory of state and local training programs. States are also conducting their own inventories of homeland security-related programs.
Strategy and Structure	That the National Office for Combating Terrorism promote multijurisdictional mutual assistance compacts, using the FBI Joint Terrorism Task Forces as one model, and facilitate the implementation of interstate mutual assistance compacts among states, through FEMA Regional Offices		X			FEMA supports the EMAC program and promotes it by providing resources. Multi-state programs are also supported by the NIMS. The evolving NIMS will require all jurisdictions to join mutual aid compacts as a condition for receiving Federal homeland security grants.
Strategy and Structure	More intense tactical and operational planning to facilitate "second wave" capabilities from outside entities after the depletion of local resources					"Second- wave” considerations are included in EMACs.
Strategy and Structure	That States utilize one of the standardized multi-state compacts either the Emergency Management Assistance Compact or the States Compact					47 states and 4 territories have adopted the EMAC endorsed by NEMA and FEMA. CA has the States Compact with surrounding states
Strategy and Structure	That the National Office for Combating Terrorism identify and promote a standardized Incident Command System (ICS) model for tactical operations for response to terrorist incidents that is part of an all-hazards approach. We recommend the identification and promotion, by the National Office for Combating Terrorism, of a standardized Unified Command System (UCS) model for operations and multi-agency, multijurisdictional coordination above the tactical operations level. When significant Federal resources are employed that involve two or more Federal agencies, we recommend a single Federal Emergency Operations Center (EOC) be established as part of the UCS. Further that each jurisdiction with an ICS and UCS develop operational templates to provide for alignment of decision-making structures based on the weapon, means of delivery, and severity of the attack		X			Homeland Security Presidential Decision Directive/HSPD-5 directs the Secretary of DHS to establish NIMS, a comprehensive incident response system for the Nation. According to the Directive, the “system will provide a consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among Federal, State, and local capabilities, the NIMS will include a core set of concepts, principles, terminology, and technologies covering the incident command system; multi-agency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certification; and the collection, tracking, and reporting of incident information and incident resources."

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Strategy and Structure	That the President always designate a Federal civilian agency other than the Department of Defense as the Lead Federal Agency		X			According to Homeland Security Presidential Decision Directive/HSPD-5, "The Secretary of Homeland Security is the principal Federal official for domestic incident management. Pursuant to the Homeland Security Act of 2002, the Secretary is responsible for coordinating Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies."
Strategy and Structure	Restructuring education and training opportunities to account for the high number of volunteer personnel in key "first responder" disciplines		X			In 2003, DHS provided $19 million in grant money to train citizens to be better prepared to respond to emergency situations in their communities through local Community Emergency Response Teams. This amount is in addition to $17 million distributed through the FY 02 supplemental appropriation.
Strategy and Structure	That the Assistant Director for Domestic Programs in the National Office develop exercise scenarios that are realistic and meet the needs of the State and local response entities and that all major exercises include an independent evaluation		X			The U.S. Congress directed Department of State and Department of Justice to conduct a series of challenging, role-playing exercises involving the senior Federal, State, and local officials who would direct a national response to an actual WMD attack. The result was "Top Officials" (TOPOFF), a national-level domestic and international exercise series designed to produce a more effective, coordinated, global response to WMD terrorism.
Strategy and Structure	That the Assistant Director for RDT&E and National Standards of the National Office for Combating Terrorism establish a national standards program for combating terrorism, focusing on equipment, training, and laboratory processes and that the National Institute for Standards and Technology and the National Institute for Occupational Safety and Health be designated as Federal "co-lead" agencies for the technical aspects of standards development		X			Numerous government agencies currently develop homeland security-related equipment standards. Coordination of the various activities is insufficient. The IAB for Equipment Standardization and Interoperability Working Group was established in 1998, but it does not lead for all for all relevant activities. NIOSH, NIST, National Fire Protection Association, and the Occupational Safety and Health Administration have entered into a Memorandum of Understanding defining each agency or organization's role in developing, establishing, and enforcing standards or guidelines for responders' respiratory protective devices.
Strategy and Structure	That Federal agencies design related training and equipment programs as part of all-hazards preparedness			X		In FY02 FEMA funded ($100 million) governments to update their all-hazards EOPs, to include a focus on WMD incidents. DOJ's OJP provided funds to the states in FY02 for the purchase of specialized equipment to enhance the capability of state and local agencies to respond to incidents of terrorism involving the use of weapons of mass destruction, for the protection of critical infrastructure, and for costs related to the development and conduct of WMD exercises. The ODP equipment grant funds enhanced WMD response. The Compendium of Federal Terrorism Training lists courses for federal WMD training.
Strategy and Structure	That Federal agencies with training and equipment programs design or redesign those programs to include sustainment components			X		This recommendation has not been implemented. To meet a number of requirements, DHS is reviewing and assessing relevant Federal training and equipment programs. Among Federal agencies, there are overlapping responsibilities for relevant training courses.
Strategy and Structure	That the Congress increase that level of funding to States and local government for combating terrorism			X		Equipment for first responders funding increased from $15 million in FY 1998 to $102 million in FY01; medical responder from $0 to $2 million; special response units from $99 to $191. The First Responder Initiative in 2003 is intended to help state and local governments assess their needs and apply for resources directly related to responding to terrorist incidents. While the bill passed by the Congress does not fully support the kind of broad, needs-based grant program requested by the President, the Department has made it a top priority to quickly get the money to states and localities. Part of this funding includes $745 million to help fund local first responders through the Firefighters Grant Program. There is a much-needed $25 million for interoperability improvements, so that first responders of all types, including fire fighters, police, and emergency medical technicians, can communicate on the same frequencies. $25 million will help states and localities modernize their emergency operations centers, and $20 million is allocated for the Community Emergency Response Training Program.
Strategy and Structure	Consolidating information and application procedures for Federal grant programs for terrorism preparedness in the Office of Homeland Security and that all funding and grant programs be coordinated through the States			X		In August 2003, DHS Secretary Ridge informed the National Governors Association that DHS was working to establish a "one stop shop" for Federal homeland security grants and assistance.

CATEGORY	RECOMMENDATION	1999	2000	2001	2002	OUTCOME
Strategy and Structure	Designing and scheduling Federal preparedness programs so that first responders, particularly those in volunteer-based fire and EMS organizations, can participate			X		See also item 8. FEMA trained a record number of leaders from volunteer fire departments for its Volunteer Incentive Program in 2003. This reflects a 42% rise in admissions for the program.
Strategy and Structure	That the Office Homeland Security serve as a clearinghouse for information about Federal programs, assets, and agencies with responsibilities for combating terrorism			X		The Office of Domestic Preparedness (ODP) established a Helpline in October 2001. The Helpline is a non-emergency resource for State and local emergency responders on all of the ODP's programs. It provides information on the characteristics and control of WMD materials, defensive equipment, mitigation techniques, and available Federal assets. ODP also established a Domestic Preparedness Equipment Technical Support Program, which provides technical support to jurisdictions in the utilization, sustainment, and calibration of detection equipment. It also started the Domestic Preparedness Support Information Clearinghouse, which is a clearinghouse of information on domestic preparedness, counter terrorism, and WMD information.
Strategy and Structure	That the Office of Homeland Security develop ongoing programs, as part of the implementation of national strategy, for public education prior to terrorist events about the causes and effects of terrorism and for coordinating public pronouncements during and following an attack			X		See also item 8, above. DHS has created a website (www.ready.gov) dedicated exclusively to educating the general public on issues related to the causes and effects of terrorism as well as what to do in case of a terrorist attack.
Strategy and Structure	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				X	These responsibilities are defined in the National Strategy for Homeland Security, the NRP, the NIMS, and HSPD-5.
Strategy and Structure	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				X	This recommendation has not been implemented. Both DHS and DHHS continue to maintain key authorities for bioterrorism response.
Strategy and Structure	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				X	The Homeland Security Council has been established for interagency coordination.
Strategy and Structure	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				X	Accomplished through the Homeland Security Act of 2002, the USA PATRIOT Act, and other related legislation, as well as through specific Executive Orders and Homeland Security Presidential Directives.
Strategy and Structure	That each House of Congress establish a separate authorizing committee and related appropriation subcommittee with jurisdiction over Federal programs and authority for Combating Terrorism/Homeland Security				X	Three new committees have been established in the Congress for oversight and appropriations: the House Select Committee on Homeland Security, the House Appropriations Committee, Subcommittee on Homeland Security, and the Senate Committee on Appropriations, Subcommittee on Homeland Security. These committees commenced operations in 2003. In addition, the House Armed Services Committee created a special oversight panel on terrorism and the House Permanent Select Committee on Intelligence created a subcommittee on Terrorism and Homeland Security.

APPENDIX L—SIDE-BY-SIDE COMPARISON OF ALTERNATIVE STRATEGIC VISIONS

Key Dimensions	Strategic Vision			
	Complacence	**Reactive**	**Fortress America**	**The New Normalcy**
Civil Liberties	Concerns regarding the potential infringement on civil liberties by government counterterrorism efforts have waned in the absence of terrorist events – which itself has diminished government efforts to adapt the existing legal system to be more responsive to the terrorism threat.	Each terrorist attack is followed by a heated debate over whether more restrictive laws and regulations are needed, some of which could be construed as producing a threat to basic civil liberties. At the same time some argue that, in the clear absence of an effective long-term solution to the terrorism problem, those laws and regulations promulgated in the wake of 9/11 that could produce an infringement on civil liberties should be repealed.	Each attack is followed by a move to produce more restrictive terrorism-related laws and regulations, generating a heated debate as to whether fundamental American rights should be put at risk as a response to the continued terrorism attacks. Highly controversial legislation has been passed in the wake of several of the more severe attacks, with tests of the constitutionality of the new laws following shortly thereafter. Some of the legislation has failed in the federal courts, including at the level of the Supreme Court.	Through a process of often intense national debate – and some significant changes in the initial legal framework to combat terrorism enacted in the aftermath of 9/11 – Americans are again comfortable with the laws of the land as regards the protection of civil liberties in the face of the security threat presented by terrorism. A major contributor to this new environment has been the independent, bipartisan civil liberties oversight board established by the President to provide advice to the nation on any change to statutory or regulatory authority or implementing procedures for combating terrorism that has (or may have) civil liberties implications (even from unintended consequences). The actions of that board have been key to the resolution of several important issues in the overall national debate on the civil liberties issue.

Key Dimensions	Strategic Vision			
	Complacence	**Reactive**	**Fortress America**	**The New Normalcy**
Intelligence and risk assessment (threat plus vulnerability)	Efforts at producing a useful terrorism threat assessment are maintained in the face of the continued difficulty of obtaining good intelligence on terrorist capabilities and the absence of attacks; most view the strategic terrorism threat as significantly diminished. The challenge of producing actionable warning of near-term or imminent terrorist attack, always difficult, is given a low priority vis-à-vis other intelligence problems.	Efforts at producing a useful terrorism threat assessment are maintained in the face of the continued difficulty of obtaining good intelligence on terrorist capabilities and the episodic nature of terrorist attacks whose unpredictability bears testimony to the continued difficulty of the threat assessment task. The inability to generate actionable warning of potential near-term or imminent terrorist attack continues to frustrate federal and state and local officials, further contributing to the reactive nature of the U.S. posture vis-à-vis terrorism.	Intensive effort is being devoted to producing a useful terrorism threat assessment, but with only modest success in the face of the continued difficulty of obtaining good intelligence on terrorist capabilities and the diverse nature of the terrorism threat. Actionable warning of potential near-term or imminent terrorist attack is still not forthcoming and a continuous source of frustration at the state and local level as damaging terrorist attacks continue to take place.	Federal efforts in collection, analysis, and dissemination of terrorist threat information are increasingly mature under strong and effective DHS coordination and leadership. The intelligence community has developed an unprecedented level of expertise on terrorist threats, including matters related to health and medical factors. The TTIC (with broad federal government and state/local staff representation) is seen as increasingly successful in integrating overseas and domestic intelligence to provide a comprehensive terrorism threat assessment covering potential perpetrators, capabilities, and objectives. While uncertainties remain, the TTIC assessments are sufficiently bounded to be very useful for planning purposes at all government levels and in the private sector. Effective Executive Branch and Congressional oversight mechanisms have stabilized. Vulnerability assessments for critical infrastructures and other possible targets are also vastly improved with a commensurate effort to reduce existing vulnerabilities and limit the emergence of new problems. The improvements in threat and vulnerability assessments have enabled DHS to produce national risk assessments for critical target sets (e.g., infrastructures and national icons) and to aid state and local governments in high-risk target areas in performing site- and community-specific risk assessments, including geographic specific real-time assessments that respond to new actionable intelligence. There have been several instances in which actionable warning has been available in real-time and contributed substantially to reducing the impact of terrorist attacks. For planning purposes, however, it is still assumed that such warning will not be available.

Key Dimensions	Strategic Vision			
	Complacence	**Reactive**	**Fortress America**	**The New Normalcy**
Information Sharing	Terrorism-related cooperation on information sharing within the federal government, between the federal government and state and local entities, and between government and the private sector diminishes as society focuses on other problems.	Terrorism-related cooperation on information sharing within the federal government, between the federal government and state and local entities, and between government and the private sector continues but in fits and starts consistent with the episodic nature of the attacks.	Government and private sector cooperation in terrorism-related n information sharing has substantially increased with occasional successes in thwarting terrorist attacks, albeit in a general environment where none of the nation's efforts is viewed as very successful in the light of the continually effective terrorist attacks.	Information sharing on every aspect of combating terrorism—from risk assessments to best practices for responding to specific threats—has vastly improved within the federal government, between the federal government and state and local entities, and between governments and the private sector. In particular, the Intelligence Community has developed a new classification system and a series of unclassified limited distribution products that allow dissemination to a wider audience with specific products available for public health and law enforcement officials. Noteworthy is the improvement in information sharing between the government and the owners and operators of critical infrastructures, made possible by major changes in laws and regulations regarding freedom of information and restraint of trade. The federal government has also led the development of a comprehensive pre- and post-event risk communications strategy for educating the public on terrorism threats and consequences. A substantially improved Health Alert Network, aided by other improved health-related secure communications systems that generate surveillance, epidemiological, and laboratory information, is now being utilized with high reliability by all of the medical and health communities. In border control, there is now a well-established, comprehensive database and information technology systems internal to the border agencies under DHS and those of other Federal agencies, state and local entities, private sector operators, and cooperating foreign governments.

Key Dimensions	Strategic Vision			
	Complacence	**Reactive**	**Fortress America**	**The New Normalcy**
Coordination with State, local and private sector (including burden sharing)	Investments made since 9/11 have produced some still intact counterterrorism capability, but for the most the nations' ability to respond to a major terrorist attack is embodied in the federal, state, and local preparedness for natural disasters.	The lurching investments made over the ten years subsequent to 9/11 (with a heavy emphasis on dual use) have produced significantly improved counterterrorism capability in some jurisdictions and against some threats. However, for the most part the nations' ability to respond to a major terrorist attack remains embodied in the ongoing federal, state, and local preparedness for natural disasters.	The increasing investment in homeland security and other facets of counterterrorism has produced significantly improved counterterrorism capability in some jurisdictions and against some threats. The impact of some terrorist attacks has been markedly decreased as a consequence of these investments which have strongly emphasized dual use as part of an effort to improve overall national disaster preparedness.	A consistent federal government program of financial support for state and local government efforts to combat terrorism has played a major role in sustaining additional state and local investments and coordination in federal, state, and local preparedness planning. Of particular significance has been the sustained funding to strengthen preparedness and coordination within the public health system. Formula grants now fund preparedness programs based on continuing risk assessments where population is only one measure of vulnerability. DHS has led the development and implementation of a comprehensive process for State and localities, and appropriate entities in the private sector, to assess and articulate potential requirements for all-hazards Federal support. This process has vastly improved the allocation of Federal resources based on a prioritization of capabilities for potential support. Most important, the Federal government has developed and provided financial support for a nationwide system for the implementation of a comprehensive, integrated, overlapping network of mutual aid for all-hazards response—a "matrix" of intrastate multijurisdictional and interstate supporting capabilities that has helped to ensure responsiveness anywhere in the country.

Key Dimensions	Strategic Vision			
	Complacence	**Reactive**	**Fortress America**	**The New Normalcy**
Exercising, Training, Equipment, Standards	The effort to establish performance standards for federal, state, and local entities with counterterrorism responsibilities withers for lack of interest. The post-disaster/event communications interoperability challenge continues to be a subject of interest and effort, but with no added impetus from the terrorism threat. Government-led all-hazards training continues at local and state levels but with training for responding to terrorist attacks a low priority vis-à-vis other potential disasters and private sector participation minimal. There is no significant joint counterterrorism training of federal, state, and local officials for potential major terrorism events.	Efforts to establish performance standards have been frustrated by the episodic nature and varied character of the terrorist attacks, diminished concern between events, and a lack of the sustained support that would be required to achieve desired standards (and associated testing and evaluation). Improving communications interoperability is continually emphasized in the terrorism event experience and infrequent training sessions, but without the impetus to undertake the changes needed to genuinely improve interoperability. All-hazards training continues at local and state levels with no high priority for counterterrorism training. Some intergovernmental training for terrorism takes place, but with decreased interest between attacks.	An ongoing effort to establish performance standards has been frustrated by the highly varied character of the terrorist attacks. While efforts continue, the level of standards (and the testing and evaluation thereof) that is clearly sought has not yet been achieved. Major efforts to improve communications interoperability are well underway but the needed level of interoperability is still some years away in many venues. All-hazards training continues with responding to terrorist attacks given a high priority and private sector participation improving. Intergovernmental is ongoing and steadily improving the ability of these government levels to work effectively in terrorism response contexts.	DHS now leads a Federal interagency coordinating entity for homeland security grants that has streamlined the grant application and decision process throughout the government and eliminated unnecessary program redundancies. DHS has now established training standards for first responders that outline the tasks, conditions, and standards of performance for individuals and units. In addition, a DHS-supported program of all-hazards exercises, with an emphasis on evaluating terrorism preparedness, continues to expand at the state and local level and with private sector participation. A joint exercise program for potential major CBRN attacks has also been institutionalized and implemented nationwide. The sustained level of government funding for terrorism preparedness has facilitated the establishment of standards and proficiency tests associated with measuring terrorism preparedness. A successful national effort to improve communications interoperability through the promulgating of national equipment standards, facilitated by substantial Federal and private sector investment in RDT&E, is finally going forward. Best practices in all aspects of combating terrorism, informed by lessons learned from exercises and actual events, is available through a significantly improved national database and seen as particularly useful in assisting states in addressing surge capacity and associated resource allocation issues.

Key Dimensions	Strategic Vision			
	Complacence	**Reactive**	**Fortress America**	**The New Normalcy**
Role of the Military				Statutory authority and regulations for use of the military inside the homeland—for both homeland defense and civil support missions—have been clarified. Extensive public education has greatly improved the understanding about legal authority for using the military. Specific attention has been focused on defining the parameters and capabilities and limitations of homeland defense and its distinctions from civil support. Clear rules of engagement exist to govern the military's actions inside the United States in situations where it is unclear if the foe is a combatant or a criminal. A comprehensive requirements identification process for responding to major attacks has been developed by DHS. This and other aspects of the potential civil support role of the military in the event of a terrorist attack has been refined through a continued program of training and exercises involving NORTHCOM, other military entities, and state and local cohorts. NORTHCOM now maintains dedicated rapid-reaction units with response capabilities relating to detection and attack assessment, emergency medical support, isolation and quarantine, and communications support. The National Guard has been given a major homeland security mission with a comparable increase in funds for civil support planning, training, exercises, and operations. Some Guard units are trained for and assigned homeland security missions as their primary or exclusive missions. With authorizing legislation, the Department of Defense has established a collaborative process for deploying National Guard units in Title 32 duty status including authority to employ the Guard on a multi-state basis for homeland security missions.

Key Dimensions	Strategic Vision			
	Complacence	**Reactive**	**Fortress America**	**The New Normalcy**
Research and Development and Related Standards	Research and development specifically dedicated to terrorism has waned with some collateral benefits from the continued Department of Defense efforts to prepare to deal with adversaries potentially equipped with chemical, biological, radiological, or nuclear weapons.	Research and development specifically dedicated to terrorism is very modest with little support for R&D efforts that do not promise to curtail or mitigate the effects of the episodic terrorist attacks that the nation continues to suffer.	Research and development specifically dedicated to terrorism is growing steadily with the realization that terrorism presents a long-term problem that needs to addressed with long-term as well as short-term investments.	The federal government is providing sustained funding for a wide-ranging R&D program that is seeking major improvements in the ability to detect and analyze terrorism-related materials or devices both at the borders and in transit within the country. The National Institute for Mental Health has undertaken a long-term research program examining the most effective ways to both prepare the public mentally for possible terrorist attacks and to treat people with mental and emotional problems following such attacks. The Congress has expanded incentives under Bioshield to encourage industrial production and development of biological and chemical defense pharmaceuticals. NIAID, in collaboration with industry, has launched a major research effort in the area of vaccine development in anticipation of possibly facing threats from natural and genetically modified biological agents. The challenge of improving cybersecurity is being addressed through a comprehensive government-industry R&D partnership that has developed not only improved defensive tools and procedures but also industry standards for ensuring that improved protective techniques and tools are implemented on a continual basis.

Key Dimensions	Strategic Vision			
	Complacence	**Reactive**	**Fortress America**	**The New Normalcy**
Enhanced Critical Infra-structure Protection	The efforts to combat terrorism following 9/11 have produced some legacy capability of terrorism defenses and programs directed to reducing vulnerabilities (e.g., in the air transport industry). Because of the decrease in concern about terrorism, the general population is psychologically untouched, if not desensitized to the threat of terrorism, leading to an across-the-board decrease in counterterrorism vigilance and the ability to respond quickly and coherently in the face of a future terrorism attack.	The country continues to make improvements in defenses against the kinds of terrorist attacks that do episodically take place (e.g., akin to the post-9/11 efforts to reduce vulnerabilities in the air transport industry) but the changing character of the attacks has produced a feeling of continued high vulnerability throughout the country. The general population is psychologically affected by terrorist events when they do happen with the expected finger pointing and frustrations at the nation's inability to curtail the attacks.	The country works hard to improve defenses with efforts akin to the post-9/11 air transport efforts across society – generating a "fortress America" sentiment and posture - to the frustration of allies and economic partners who find this inward-turning U.S. trend troubling and a threat to U.S. involvement in pressing international security problems. The population is psychologically affected by terrorist events when they do happen with broad concerns about the long-term impact on the traditional American way of life and values.	Major improvements in infrastructure protection include mandated screening of all baggage and cargo for passenger and commercial aircraft and the equipping of U.S. seaports and international airports with extensive suites of detection and monitoring equipment. In energy, chemicals, and telecommunications, there are now well-established means for evaluating system and facility vulnerability and protective measures. Energy especially has benefited from new process actions and redundancies. At the borders, there are now pre-entry identification requirements and commercial shipment regulations that have dramatically improved prospects of preventing terrorists and related materiel from entering the United States - at minimal economic impact. In medical/health there is a renewed emphasis on all hazards/dual use capabilities, well defined health care requirements for specific bioterrorism contingencies, and vastly improved public-private coordination at all levels. The national CBRN medical/health response teams have been updated and unified, with a focus on bioterrorism preparedness. In addition a campaign to improve U.S. psychologically readiness for terrorism is underway. The cyber threat to critical infrastructures (especially interdependency and cascading effect problems) is of continual concern with new protective tools and practices building confidence regarding the cyberspace vulnerability. In agriculture and food risk assessments and responses are now coordinated by an intra-governmental effort that includes joint education and training programs, more funds for veterinary education, and a program of compensation for losses in the event of a successful attack on agriculture. Specially designated laboratories now perform tests on foreign agricultural diseases.

APPENDIX M—TESTIMONY OF SECRETARY OF AGRICULTURE ANN VENEMAN, SEPTEMBER 9, 2003

United States Department of Agriculture

Office of the Secretary
Washington, D.C. 20250

Statement by Secretary Veneman
Submitted for the Record to the Gilmore Commission
September 9, 2003

Chairman Gilmore and distinguished members of the Commission, thank you for the opportunity to share the Department of Agriculture's (USDA) role in protecting our country from terrorism with the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction.

When the Gilmore Commission was established four years ago, few Americans foresaw the profound way that terrorism could affect us, and very few understood the potential impact of weapons of mass destruction. This Commission, however, has been on the forefront of both of these issues, which are now central not only to American foreign policy, but also to the work of every department within the Federal government. I commend the Commission for its role in heightening awareness of these issues, for bringing more accountability to the government and for its recommendations for improving homeland security.

In its latest report, the Commission considers the economic impact of a significant attack against American agriculture and finds that, "the downstream effect of a major act of terrorism against this highly valuable industry would likely be enormous."[202] Indeed, with one in eight American jobs directly involved in, or dependent upon agriculture, the economic impact of an attack on this sector could be the most important threat we face.

I want to commend the Commission, too, for observing that because agriculture was not recognized as a critical infrastructure when critical infrastructures were initially identified, agriculture did not benefit from the heightened awareness of terrorist threats that were paid to other sectors. As you further note, though, the Bush Administration has recognized this oversight, designated agriculture as a critical infrastructure in its *National Strategy,*[203] and has taken strong steps toward protecting it. Addressing the new threat requires extraordinary vision, new thinking and the ability to look at the much larger issue – the protection of our citizens against potential threats.

We have seen the devastation, destruction and loss of lives – to say nothing about the damage to our economy – caused by the events of that horrible day, September 11, 2001. It is something that nobody wants to see repeated. It is why all of us are considering the important issues of homeland security and

---

[202] RAND, *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: Chapter VII, Implementing the National Strategy*, December 15, 2002, p. 68.
[203] The White House, Office of Homeland Security, *The National Strategy for Homeland Security,* July 16, 2002, p. 30.

how we can best prepare for and prevent future attacks. However, preparedness also requires us to consider how we can best ready this nation – and the infrastructure which supports it – to respond in the event of another attack.

Background – Post September 11, 2001

Over the last two years, our mission at USDA has evolved and expanded to include homeland security. In the past, our focus was on preventing and deterring the unintentional introduction of pests and diseases into our country and ensuring a plentiful food supply that is safe from unintentional contamination.

Shortly after the events of September 11, USDA undertook a top-to-bottom review to see how best to grapple with potential terrorist threats. I immediately formed a Homeland Security Council to develop a Department-wide plan concerning homeland security. USDA's homeland security efforts are focused upon three key areas: agricultural production and the food supply, USDA facilities, and USDA staff and emergency preparedness. Forming the Homeland Security Council was the first step in a series of organizational changes aimed at improving the Department's ability to perform homeland security-related activities.

I also established a Homeland Security Staff to coordinate Department-wide activities. The mission of this staff is to provide overall leadership, to coordinate programs, and to plan for, and respond to, major natural and terrorist emergencies and threats. This staff coordinates policy formulation, response plans, and reporting and action assignments for the mission areas. The staff leads the activation of USDA's incident management system and its Federal Response Plan duties in the event of a major incident and oversees USDA's nationwide homeland security policies and procedures. The staff also coordinates the Department's homeland security activities with the White House's Homeland Security Council, the Department of Homeland Security (DHS), other federal agencies, and public and private organizations; collaborates with many White House offices, USDA agencies, and other federal partners on the development and submission of a coordinated budget request for homeland security; and provides staff support to the Homeland Security Council. Many USDA agencies have also created offices or enhanced existing offices to serve a similar function within the agency and work in close coordination with the USDA Homeland Security Staff.

In addition, USDA has worked closely with the rest of the Administration and Congress during the creation of the new DHS. USDA will also continue to improve its prevention, surveillance, communications and response efforts.

Protecting Agricultural Production and the Food Supply

Agricultural Production

To ensure the security of our animals and plants, USDA has utilized its personnel, many of whom are stationed throughout the nation, as a first line of defense. We have worked with our Federal partners to ensure that strong laws and regulations are in place to deter terrorists. In addition to fortifying our first line of defense, we are enhancing the surveillance capabilities of the nation's plant and animal health laboratories. Lastly, USDA is working closely with its partners at the Federal, State, and local levels, in the private sector, and consumers, to ensure that they are educated and are equipped to aid in the defense of our agricultural production.

Personnel
Since September 11, 2001, USDA has increased its safeguarding personnel, such as border inspectors, wild-land firefighters, and veterinarians – those on the front lines of homeland security. Congress recognized the importance of USDA's border inspection personnel to homeland security programs in the Department of Homeland Security Act of 2002, which created DHS. As mandated by the Act,

approximately 2,600 members of the USDA border inspection force have been transferred to the new department. These individuals enhance prevention efforts to keep foreign agricultural pests and diseases from entering the United States. USDA will continue to work in close consultation with DHS to train these inspectors and set policy for plants, animals and commodities entering the nation.

In addition to the transferred personnel, USDA maintains National Forest Service enforcement personnel along the hundreds of miles of continuous Forest Service land on both our northern and southern borders. The Department has also added 18 new veterinarian positions to the agricultural quarantine inspection staff at borders, ports of entry, and on farms to ensure that strong preparedness programs are in place. Furthermore, USDA has added 20 new food import surveillance officers to ports of entry.

Regulations
One of the most important steps taken to secure American agricultural production and the food supply was the "Select Agents Rule" mandated by the Agriculture Bioterrorism Protection Act of 2002. USDA and the U.S. Department of Health and Human Services (HHS) issued complementary regulations that established new safeguards for the possession, use, and transfer of certain toxins and biological agents. These safeguards reduce the chance of terrorists acquiring dangerous pathogens and toxins.

Laboratories
In its December 2002, report, the Commission urged the expansion of laboratory capacity, noting that in the event of a terrorist attack, our laboratories would likely be overwhelmed.[204] USDA concurs with this assessment, and is in the process of creating networks that will increase laboratory capacity.

In addition, USDA has begun a pilot version of a National Animal Health Laboratory Network (NAHLN), a network of Federal and State resources intended to enable a rapid and sufficient response to animal health emergencies, including foot and mouth disease and other foreign animal diseases. The NAHLN reconfigures the nation's animal health diagnostic services by positioning the National Veterinary Services Laboratories in Ames, Iowa, to be the lead animal health laboratory and allowing certain laboratories operated by States and universities to cooperate in foreign animal disease surveillance and related services. Such an arrangement will enhance the nation's animal health diagnostic services, speed response efforts should a foreign animal disease be detected in the United States, and lend greater credibility to our animal health export certifications. A similar effort is underway to build a laboratory network for plants.
Communications
To ensure the protection of our nation's agriculture, USDA has worked with its partners at the State and local levels and the private sector to ensure they are informed of, and have the tools necessary to both prevent and respond to an attack. USDA-sponsored guidance documents, security upgrades and partnerships are essential to a robust communications system.

Guidance documents provide helpful information to industry, consumers, and State and local partners. The voluntary nature of the guidance has enabled USDA to share recommendations and information.. USDA has developed guidance documents for distribution to farmers and ranchers to remind them of steps they can take to secure their operations. Information was posted on the USDA website and distributed through the USDA Extension system to reach constituents in every county in the nation.

Strong security systems in the field enhance communication. They enable USDA headquarters and field offices to share information quickly, securely, and reliably. USDA has upgraded the security systems at its State and county offices. This upgrade included establishing a web-based tracking system for disaster reporting, maintaining databases of fertilizer, food, feed and seed listings, and coordinating with State and county emergency boards for assistance during an emergency.

[204] RAND at p. 74.

Training and seminars are also key components of a communications strategy. For this reason, USDA has, and will continue to conduct, on-going Foreign Animal Disease Awareness Training seminars for Federal and State veterinarians. In addition, the Department has conducted, and continues to conduct, satellite seminars to share vital emergency preparedness information with Federal and State veterinary officials and emergency planners, military representatives, and academia. As part of this effort, USDA has developed a CD-ROM to help practitioners better identify and diagnose animal diseases and distributed it to State and Federal veterinarians, veterinary schools, and associations.

USDA has also partnered with States, universities and tribal lands to increase their homeland security prevention, detection and response efforts. USDA provided funding for those efforts and is currently developing rapid tests for agents that pose the most serious threats to our agricultural system. Some examples of these threats include foot and mouth disease and rinderpest.

While this is an overview of what we are doing to protect agricultural production, USDA is just as active in protecting the food supply.

Food Supply

As with agricultural production, USDA now must consider how to prevent, and respond to, intentional threats to the safety of the food supply. Historically, USDA has been responsible for ensuring the safety of meat, poultry, and egg products from unintentional contamination. Over the years, USDA has faced tampering and intentional contamination of the food supply, but on a small scale. The tragic events of September 11, 2001, now require us to seriously consider the possibility of a large-scale attack on the food supply.

As with agricultural production, USDA has relied upon our greatest asset, our field personnel, as we adjust to the new threats. In addition to personnel, the keys to protecting the food supply lie in a coordinated effort, a strong understanding of the threat and our vulnerabilities, an enhanced laboratory system, and communications between all sectors.

Personnel

USDA has approximately 7,600 personnel at federally inspected food establishments nationwide. These individuals are trained to look for signs that may suggest intentional contamination and adulteration of meat, poultry, and egg products. This workforce is comprised of consumer safety inspectors, consumer safety officers, compliance officers, and veterinarians.

Coordination

USDA has participated in several drills at the Federal and State levels to test and improve response procedures. These drills have proven valuable in identifying vulnerabilities and assisting with interagency coordination.

Vulnerabilities and Threats

To ensure that we are taking the right steps to protect the food supply, we first needed to understand its vulnerabilities and the threats posed by terrorists. In the months following the attacks, USDA conducted vulnerability assessments for domestic and imported food and conducted threat assessments to ensure the security of food. The assessments also addressed food purchased by USDA for Federal feeding programs, as well as shipping procedures and storage. Based on the assessments, USDA developed a food security plan and training sessions for employees in preparedness activities.

These assessments also played a vital role in developing a plan for USDA's role within Liberty Shield, the Administration-wide strategy for protecting the homeland from terrorist attacks during the war in Iraq. USDA's measures included increasing the number of agents tested for in the food supply and increasing the frequency of testing.

Enhanced Laboratories' Capabilities
Food regulatory laboratories are essential surveillance and response tools. One of the most important steps USDA has taken is to enhance security at its three food regulatory laboratories and increase their capacity to test for products, hazards and biological agents. This is consistent with the Commission's recommendation to improve laboratory capacity, addressed above.

Communications
USDA prepared and distributed food security guidance documents for the processing, distribution, and transport of meat, poultry and egg products. USDA has also developed information on biosecurity and the food supply for constituents and processors. To ensure that consumers have an opportunity to provide critical information, USDA implemented the national Consumer Complaint Monitoring System, a surveillance and sentinel system that monitors and tracks food-related consumer complaints.

Protecting USDA Laboratory Facilities

Addressing the concern that foreign terrorists might seek access to laboratory facilities and the pathogens stored there for research and testing, USDA issued two Departmental Manuals addressing policies and procedures for pathogen control, physical security, human reliability, cybersecurity, and incident response plans. Additionally, USDA developed departmental policies for the sponsorship of non-citizen scientists working in USDA facilities, including a tracking system for these workers. Furthermore, background checks are being conducted for non-citizen workers. In addition, all positions at USDA labs are being examined for personnel reliability and the appropriate background investigations are being conducted, beginning with the Bio Safety Level 3 (BSL-3) locations.

Protecting USDA Staff and Emergency Preparedness and Response

As our first line of defense, USDA employees play a vital role in protecting the nation's agricultural production and food supply. Therefore, employees that are knowledgeable and well trained in emergency preparedness and response are key to this effort. To ensure that our critical infrastructure is protected and employees are safe, USDA developed additional security procedures for use when the threat of terrorist attacks, as determined by the Homeland Security Advisory System, increases. This approach was integrated with Liberty Shield.

A coordinated workforce is also essential to carrying out prevention and response activities. Guidance for a coordinated, prepared workforce can be found in the National Incident Management System (NIMS) and National Response Plan (NRP).

USDA is now implementing a Department-wide NIMS based on the successful system currently utilized by USDA's Forest Service. The NIMS has systems for command and control, coordination, training and qualification, and publication management. This effort is consistent with Homeland Security Presidential Directive 5, which called for a single, comprehensive approach to domestic incident management.

USDA is working with DHS to draft the NRP and NIMS documents. Various aspects of agricultural production and food will be addressed in the new plan, including animal and plant health, food safety, nutrition, and wild-land firefighting. Since the NRP will integrate the Federal government's domestic prevention, preparedness, response, and recovery plans into a single all-discipline, all hazards plan, we believe it will address the Commission's concerns that agricultural production and food be adequately represented in current national response plans.

Next Steps

Our work to date is just the beginning. We have begun to develop the foundation for an agricultural production and food security program. While we carefully consider the next steps, we must continue our ongoing efforts because the agricultural production and food sectors are still vulnerable to attack. Therefore, USDA will continue to build upon its accomplishments thus far, as reflected in the recent budget request that calls for bolstering ongoing initiatives. These initiatives fall into four categories: prevention and preparedness, surveillance, communications, and response.

Prevention and Preparedness

USDA is seeking new funding to expand laboratory networks, strengthen laboratory security measures, conduct research on emerging animal diseases, and develop new vaccines. The Department will continue to develop the NAHLN, as mentioned above, train more personnel, expand standardized rapid/sensitive testing capabilities, increase BSL-3 laboratory capacity, assure quality standards and proficiency testing, and improve communications for data sharing. USDA will also expand the plant laboratory network, by establishing national standard operating procedures for diagnostics, sampling, and reporting, by providing inter-regional communication, and by creating a national database for monitoring disease and pest outbreaks.

Surveillance

USDA employees in our nation's food processing facilities and on the farm are our first line of defense and have a unique ability to serve as a surveillance tool. Therefore, staffing these positions is essential to the Department's homeland security efforts. USDA has set a staffing level goal of 7,680 food inspectors, an increase of 80 inspectors, who are on the front line in our nation's food facilities looking for unintentional and intentional threats to food safety. In addition, USDA is examining ways to expand the role of its Extension Service and other on-site employees to include homeland security responsibilities.

USDA employees on the farm also serve as a surveillance tool. USDA has set goals to increase on the farm inspections, expand the availability of foot and mouth disease vaccines, provide protection against chronic wasting disease and poultry diseases, and expand diagnostic and other scientific and technical services.

Research is key to a strong surveillance program. USDA is researching remote sensing technology that would detect the introduction of foreign pests and plant and animal diseases and has requested funding for the National Research Initiative, a USDA grants program funding research on a peer-reviewed, competitive basis in the biological, environmental, physical, and social sciences relevant to agriculture, food, and the environment.

Communications

Two of our highest homeland security priorities at USDA are the improvement of communications channels between the Department and the intelligence community, and the creation of a more sophisticated way of communicating sensitive information to the private sector so that when there are incidents, warnings or threats, the private sector can assist us in preventing or mitigating a problem. USDA is working with DHS to coordinate our communications programs to better protect agricultural production and the food supply. One such joint effort is the DHS-USDA-HHS project to organize the food and agriculture sectors. An organized sector can provide assistance to the industry. For example, this sector could suggest guidelines and best practices, and provide a means for sharing information.

Response

As mentioned above, USDA is working with DHS to write and implement the NRP and NIMS documents. As part of this effort, USDA will implement NIMS throughout the entire Department, starting this year with online training and other forms of training and certification.

Conclusion

In conclusion, USDA has acted decisively and aggressively since September 11, 2001, to establish a national strategy to keep American agricultural production secure from intentional harm and to maintain a secure and reliable food supply. We have done this through a top-to-bottom review of our organization, thorough assessments of our vulnerabilities, simulating attack scenario exercises, increased surveillance, more targeted and expedited communications, and a more robust response strategy.

While I cannot tell you that we have mitigated all of the threats to American agriculture, I can state that we are much better off today than we were two years ago and that we are aggressively pursuing new programs and policies to better protect agricultural production and the food supply.

Finally, I want to thank the Commission for its work, which has brought attention to the threats that terrorism presents and a specific focus to the threat posed to agriculture and food.

APPENDIX N—STATEMENT BY C. MICHAEL ARMSTRONG, THE BUSINESS ROUNDTABLE

Statement by C. Michael Armstrong
Chairman, Security Task Force, The Business Roundtable

Before the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction

September 3, 2003

Thank you, Governor Gilmore and Members of the Advisory Panel.

My name is Mike Armstrong, and I am Chairman of Comcast Corporation and Chairman of The Business Roundtable's Security Task Force. I appreciate the opportunity to express the views of The Business Roundtable with respect to how the private sector can assist government in disaster response and recovery efforts.

Before I begin, let me take this opportunity to recognize Governor Gilmore and the distinguished members of this panel for their leadership in terrorist response and recovery efforts. Your work is vital to the ability of this nation to prepare for and protect against future threats.

The Business Roundtable is an association of 150 chief executive officers of leading corporations with a combined workforce of more than 10 million employees in the United States, $3.7 trillion in annual revenues, and a presence in every state in the nation. The chief executives are committed to advocating public policies that foster vigorous economic growth and a dynamic global economy.

Following the September 11th terrorist attacks, the Business Roundtable created a Security Task Force to address ways that the private sector could improve the security of our employees, their communities and our companies.

The Roundtable believes that the business community has an important role in disaster response and recovery, and must be a partner in a coordinated effort with federal, state and local governments. We believe that the government cannot face these challenges alone, because more that 85 percent of the critical infrastructure in the country – the power grid, financial services, information services, railroads, airlines and others – is controlled by the private sector, not the government.

Businesses are committed to protecting their employees, customers, facilities and communities. We accept this responsibility and have moved forward on strengthening our security. The private sector is ready and willing to partner with government in disaster response and recovery in significant ways. For example, following the September 11th attacks, companies from across New York and across the country responded with respirators, boots and other materials for rescue personnel. The private sector also helped restore phone service and power, and helped get institutions such as the New York Stock Exchange ready to reopen.

The terrorist attacks on our nation revealed that America needed a way for government and business leaders to exchange information in times of crisis. Coordinated security efforts by government and business will lead to better protection for our citizens, facilities, communities and nation.

THE BUSINESS ROUNDTABLE HAS DEVELOPED WAYS FOR GOVERNMENT AND THE PRIVATE SECTOR TO WORK TOGETHER TO PROTECT AMERICA.

In the months since September 11th, the Business Roundtable's Security Task Force has been working closely with the Bush Administration, including the new Department of Homeland Security (DHS), to collaborate and coordinate improved security and responses to terrorist attacks. The hallmark of the Business Roundtable's efforts is the development and implementation of CEO COM LINK℠, a secure telecommunications bridge that enables senior federal officials and CEOs to exchange timely information in the event of a terrorist threat or a crisis.

CEO COM LINK℠ enables CEOs to get the information they need in order to respond to terrorist threats and recover after an attack. The capability equally serves the government by offering real-time access to the nation's business resources. We have expanded CEO COM LINK℠ to include representatives from the banking, chemicals and water industry sectors. We are in the process of adding other critical infrastructure sectors as well.

As we further develop CEO COM LINK℠, we work closely with the Department of Homeland Security (DHS) and other security officials throughout the federal government. We are now working with them to refine CEO COM LINK℠ so that calls can be made to appropriate industries in response to a specific sector threat. In May, the BRT brought together a number of company security officials to get their ideas for enhancing CEO COM LINK℠ and improving the security alert system. We continue to seek ways to enhance CEO COM LINK℠ and are working with DHS on setting up a 7x24 real-time system that would be used in an on-going basis by the public and private sectors to coordinate response and recovery.

IMPROVING COMPANY SECURITY PROCEDURES

The Business Roundtable is also providing best practices and ideas to improve company security procedures. These efforts concentrated in five areas.

First, the Roundtable made a series of recommendations that strengthen corporate governance procedures to bring security under board review. Specifically, the Roundtable is urging boards of directors to designate management responsibility for business resiliency and to periodically review management's plans as part of their oversight function. The Roundtable added this new security component to its Principles of Corporate Governance, a set of best practices designed to guide corporate governance practices and advance the ability of U.S. companies to compete, create jobs and generate economic growth.

In today's world, America's security is inexorably linked to our nation's economic growth. It is more vital today than ever before that corporate boards review management's security plans and procedures.

Second, the BRT has developed a Crisis Communications Toolkit that offers best practices for communicating with employees, customers and neighbors during a crisis. We have shared this with other business groups, such as the National Association of Manufacturers, the U.S. Chamber of Commerce, the Small Business Association, and the National Federation of Independent Businesses. A copy of the Crisis Communications Toolkit can be found in the security section of www.brt.org.

Third, the Roundtable's Security Task Force is developing a risk assessment toolkit. Business enterprises face many threats and vulnerabilities in the global environment, as terrorists can target any number of business assets. We cannot afford to build fences or moats around our employees and facilities. Performing a current risk assessment on threats and vulnerabilities is one way that businesses can manage the evolving threat environment. Similar to the Crisis Communications Toolkit, this risk assessment

material offers important templates and procedures for both business and government executives that manage critical infrastructures.

Fourth, the Business Roundtable has also made recommendations on security regulation by government in a regulation white paper that was released in July. Industry is willing to accept greater costs and additional security regulation, but we strongly believe that security regulations must be based on rational and open processes. The best security solutions will come from government policies that encourage greater business participation and are based on collaborative efforts that favor flexible and focused private-sector initiatives.

Finally, to better understand how CEO COM LINK[SM] could add value, leaders of major U.S. businesses and government agencies engaged in a two-day wargame simulation on April 8-9, 2003, in Washington DC. The war game – conducted by the Business Roundtable and Booz Allen Hamilton – simulated a catastrophic cyber failure in the accounting systems of two major U.S. banks in New York City and, simultaneously, an outbreak of pneumonic plague at the Chicago Stock Exchange.

The wargame established the critical importance of crisis communication and collaboration mechanisms between the public and private sectors to foster economic and societal resilience in the face of asymmetric attacks. It showed that CEO COM LINK[SM] saved hundreds of thousands of lives due to the ability for the public and private sector to communicate and respond. Going forward, government and industry together have a critical role to play and a unique opportunity to enhance public-private sector interaction. Their crisis response must encompass new decision models, communications capabilities, and dynamic organizations and structures, with CEO COM LINK[SM] serving as an important element.

Leveraging these lessons can help shape the U.S.'s ability to respond to and recover from crises that could otherwise jeopardize our national, homeland and economic security.

The CEO COM LINK[SM] wargame showed that in times of crisis, we must be able to communicate real-time to respond to events through 7x24 capability to interface with a national command and control center.

A summary of the CEO COM LINK[SM] wargame report is included as part of this testimony.

PROGRESS HAS BEEN MADE BUT MUCH LEFT TO DO

The efforts of the Business Roundtable and DHS to include businesses in response and recovery efforts have been significant. CEO COM LINK[SM] has been utilized successfully several times when the terror threat level changed. The Department of Homeland Security is including the Business Roundtable and member companies as part of its Crisis Action Team (CAT). We are working with DHS to identify company experts on a variety of issues who can be called upon by the government in the event of an attack.

The Gilmore Commission's decision to invite the Business Roundtable to testify is recognition of the role that the business community can play. We acknowledge that involving the private sector in disaster response and recovery is new and uncertain territory for many of you, and we appreciate this opportunity.

However, while the business community is making progress in some areas, the private sector is not yet adequately integrated in disaster response planning and activities. For example, the Roundtable and other private sector organizations were not fully part of TOPOFF II, the wargame this past spring on disaster response by government. Roundtable representatives were at TOPOFF II, but only as observers, not participants.

In addition, while the governors and Roundtable CEOs are both briefed by the Department of Homeland Security when the terror threat levels are raised, there is no mechanism for governors and CEOs to coordinate their efforts. It is essential that we address this national, public-private deficiency. In the event of an attack, for example, it is imperative that the decisions by businesses on whether to send thousands of workers home be coordinated with state officials and local responders who may need to use the same roadways. There are many other issues that senior principals in state and local government and the business community should address as part of a well-exercised process – whether locally, at the State level, within a region, or as a national matter.

BUILDING A PARTNERSHIP FOR A SECURE AMERICA

The Business Roundtable is encouraged by the progress that has been made to involve our companies in matters of homeland security, response and recovery. Yet there is much more left we can do to build on this foundation of cooperation and partnership – tasks that will benefit America during a time of crisis.

I would encourage Governor Gilmore and every member of the Panel to consider the nation's business community and its important role in response and recovery efforts.

The Business Roundtable believes that recommendations to Congress by this panel would be an effective means to strengthen public-private partnerships. These recommendations should encourage more robust and targeted private sector roles in homeland security planning and disaster response and recovery – at all levels of government, including regional and national in scope. It should also clarify roles, responsibilities and systems in disaster response and recovery, and include the private sector at all levels. Specifically, we recommend exploring partnerships between business groups such as the Business Roundtable with states and local governments, possibly through the National Governors Association or the National Emergency Managers Association, as warranted.

We also believe that CEO COM LINK^{SM} should be integrated into our national response and recovery. At the federal level, the Administration has embraced the capability, tested its use, and we will continue to enhance its capability. However, with regard to state and local entities, there is no link, whether in terms of agreed upon processes or technological support. In addition, it is critical that a single home be found for CEO COM LINK^{SM} and disaster response – and to hard wire this capability. This would include configurability as well as supporting real-time bridge capacity on a 24x7 basis.

Finally, the private sector has taken responsibility in protecting the security of our employees, facilities, customers and communities. We have expressed that in a security component of the Business Roundtable's Principles of Corporate Governance. We would appreciate the Gilmore Commission's endorsement of the Business Roundtable's corporate governance principles for security for all of the nation's businesses. We would also challenge government entities to develop similar governance principles for security.

In conclusion, we believe that the business community, working in close partnership with federal, state and local governments, is the best way to plan for and mitigate the effects of future threats to our homeland security.

The private sector is ready, willing and able to be a partner with government at all levels in disaster response and recovery. To have an effective national response system, the private sector much be involved in planning so that everyone understands roles and responsibilities.

Thank you again for the opportunity to share the business perspective on this issue. I appreciate the Panel's willingness to listen and am now available to take your questions.

# # #

CEO COM Link Wargame

Improving Response and Recovery

Executive Summary

Rapidly Linking the public and private sectors during a crisis can dramatically improve collaboration and effectiveness in enhancing homeland security. The CEO COM LINK[SM], developed by the Business Roundtable, is an essential tool that enables this collaboration prior to, during, or in the aftermath of a significant national crisis. To better understand how CEO COM LINK[SM] could add value, leaders of major U.S. businesses and government agencies engaged in a two-day exercise, the CEO COM LINK[SM] Wargame, on April 8 and 9, 2003, in Washington DC. The wargame simulated a catastrophic cyber failure in the accounting systems of two major U.S. banks in New York City and, simultaneously, an outbreak of pneumonic plague at the Chicago Stock Exchange.

The wargame established the critical importance of crisis communication and collaboration mechanisms between the public and private sectors to foster economic and societal resilience in the face of asymmetric attacks. Going forward, government and industry together have a critical role to play and a unique opportunity to enhance public-private sector interaction. Their crisis response toolkit must encompass new decision models, communications capabilities, and dynamic organizations and structures, with CEO COM LINK[SM] serving as an important element. Leveraging these lessons can help shape the U.S.'s ability to respond to and recover from crises that could otherwise jeopardize our national, homeland and economic security.

"In times of crisis we must figure out how we are going to expand traditional networks, how we are going to interface with the command and control center (Department of Homeland Security), and then we need to practice," said C. Michael Armstrong, Chairman of Comcast and Chairman of The Business Roundtable's Security Task Force, who participated in the exercise.

The Wargame

The Business Roundtable, an association of CEOs representing the nation's leading companies, co-sponsored the two-day exercise with Booz Allen Hamilton, a global management and technology consulting firm. Participants included more than 70 senior policymakers and business leaders. Representing government were officials from the White House, Department of Homeland Security, Department of Treasury, and the Federal Bureau of Investigation, as well as officials from city and state agencies. Business participants included CEOs and senior executives from a broad array of industries, including financial services, pharmaceuticals, high-tech, manufacturing, consumer products and telecommunications.

At the start of the game participants faced a potentially catastrophic scenario – an outbreak of pneumonic plague suspected to have originated at the Chicago Stock Exchange, and a software glitch that caused major discrepancies in the account balances of corporate and consumer customers of two of the largest U.S. banks. The situation resulted in a halt of payment and investment activity throughout the country. Six teams, representing government and business stakeholders, had to make choices, and live with the consequences of their actions. The teams then identified next steps to improve real-world communication and collaboration in response to the evolving scenario.

The intent of the wargame was not to assess the preparedness or responsiveness of specific groups. Instead, the wargame sought to increase awareness among all participants about the challenges in assuring homeland security, and to explore how to enhance public-private collaboration and to identify ways that CEO COM LINK[SM] could help improve crisis response and recovery.

Insights & Recommendations

The objective of the wargame was to better understand how CEO COM LINK[SM] could serve as a crisis communications network. Participants discovered that effective public-private collaboration is essential to fulfilling the homeland security mission, improving our response and recovery to national crises by filling the gaps between needs and capabilities.

For example, the Department of Homeland Security (DHS) served as the focal point during the wargame for mobilizing government and business resources in response to the biological attack. Consequently, DHS required input from the healthcare industry to identify additional resources and to increase production of pharmaceuticals. Participants leveraged CEO COM LINK[SM] to coordinate actions, which demonstrated that a centralized and flexible public-private collaboration mechanism can improve crisis response.

Based on this experience, participants concluded that effective public-private sector collaboration is built on three critical elements:

- *Dynamic Organization and Operations*: Observation of CEO COM LINK[SM] calls revealed the need to dynamically shift among multiple collaboration models, depending on the objectives and stage of the crisis. Creation of a "strategic architecture," Linking various collaboration models and response plans across the country, would enable rapid and informed crisis response. Inclusion of established criteria would enable decision-makers to determine quickly which model to use and who should participate.

- *Balanced Decision-Making*: During crises, there is rarely sufficient time and information to satisfy decision makers. Nevertheless, crisis management demands decisive and expedient responses to control cascading damages. Such decision-making must be balanced, considering risks, urgency of needs, information fidelity and availability.

- *Flexible Communications*: Throughout the wargame, participants stressed the need for timely, relevant, accurate, and clear communications. Clarity – in terms of objectives, language, decisions and action – is critical, and use of industry or agency-specific jargon and acronyms must be strongly discouraged. Communication must take place early in the crisis, with regular updates, to allow stakeholders to make decisions and take actions to resolve issues and mitigate impacts before the crisis spins out of control.

The wargame demonstrated that DHS provided an effective, single focal point to coordinate government and business response, speed decision-making and mitigate long-term impact. However, additional actions are required to enhance crisis preparedness, response and recovery. The wargame identified several key imperatives to enhance business and government collaboration moving forward:

- *Build operating models to guide government and industry in effective communication and collaboration*. Ensure that these models enable real-time establishment and modification of networks and incorporate appropriate decision rights and processes. CEO COM LINK[SM] should be leveraged as a key element, providing a strategic-level interface between business and government.

- *Develop integrated decision models for crisis response.* The decision model should help leaders establish criteria for rapidly assessing what collaboration is needed and what actions need to be taken, when, how and by whom. This will facilitate the crisis decision-making process, even in the absence of complete information.

- *Test – and refine – operating models, decision-making capabilities and CEO COM LINK[SM] through continuous practice and simulation.* Provide decision-makers with "experience" in simulated risk-free environments that enables them to better anticipate and resolve critical issues and potential stumbling blocks, and identify solutions in real-world crises.

- *Address the regulatory and commercial issues that might become roadblocks to effective public-private sector crisis collaboration and response*. Seek ways to creatively address issues that may result in government's or industry's inability to take action during a crisis. By understanding the implications of regulations and commercial issues in advance of a crisis and thinking through contingencies, participants can make more informed decisions.

Finally, participants identified insights and enhancements to ensure that CEO COM LINK[SM] continues to serve as an effective crisis response resource for business and government leaders:

- CEO COM LINK[SM] is most applicable for urgent, strategic level communications and decision making to enhance situational awareness and address cross-sector and cross-agency issues

- The ability to quickly transition from strategic decisions to operational implementation increases the value of CEO COM LINK[SM] in crisis situations

- Proactive call management – setting the agenda in advance, driving decision making, appointing a single leader for each call, assigning responsibility, and following-up – drives key decisions and action items

- The communications model (e.g., who is on the call) should be flexible and dynamic to address a variety of situations

- Stakeholders should develop a better understanding of each other's relevant and unique capabilities, concerns and challenges to mitigate potential communication gaps during a crisis

- Participation in CEO COM LINK[SM] calls should expand, as necessary, beyond the core CEO/senior official group, to include other relevant government and business stakeholders. However, the ability to designate

participants based on sector or geography is critical to ensure calls are managed efficiently and members are provided with relevant information

- Coordination with other communication mechanisms such as industry Information Sharing and Analysis Centers (ISACs) would provide expertise and help implement decisions

A Case for Enterprise Resilience

The wargame revealed that in addition to public-private sector collaboration, government and private industry organizations should take steps to improve their own enterprise resilience. The exercise revealed a set of risks that many companies have not considered: Today's heightened risk environment, increased business model complexity and interdependence have significantly altered the risk landscape of the extended enterprise. Boards and corporate leadership must now grow and protect their businesses by proactively managing risk and enhancing management focus and accountability through corporate-wide risk stewardship. They also must develop adaptive risk management capabilities. Wargame exercises such as this one are an effective means for regularly assessing crisis response and identifying solutions to enhance an organization's resilience.

Terrorism: Real Threats. Real Costs. Joint Solutions.
(The Business Roundtable, June 2003)

A full copy of this publication is available at www.brt.org

Executive Summary

Governments and businesses both have critical roles to play in improving security after September 11, 2001. However, determining which security measures to implement, how they should be implemented, and what should be the roles of business and government present significant challenges. The Business Roundtable's goal is to explore those challenges and encourage smarter regulatory decision-making. Our key conclusions:

Acting alone, neither business nor government can adequately assess and manage security risk. Both have roles to play in securing our nation, although both are subject to limited resources and other constraints. Collaboration, not regulation, presents the most effective approach to addressing security risk. Information-sharing is integral to effective collaboration.

We can never protect America lives and property against every possible threat, even with optimal public and private investment and ideal collaboration between business and government or among governmental entities.

Where government intervention is necessary, policymakers should avoid command-and-control regulation and instead favor deference to private initiative, incentives, flexibility, and careful priority-setting. Despite inherent uncertainties underlying terrorist threats, analytical tools such as risk-assessment, cost-benefit analysis, and cost-effectiveness analysis should be used and refined to maximize security enhancement per dollar invested. Public participation and transparency should be retained for security rulemaking.

Protection against terrorist acts is uniquely a governmental function. Any security mandates that lead to extraordinary additional costs on the private sector should be paid by the government.

Terrorism: Real threats. Real Costs. Joint Solutions examines the challenges and responsibilities in developing ways to improve the security of our nation, communities, employees and facilities. These include:

Refining our understanding of the terrorism risk and selecting security programs

Although the threat of terrorist attacks on the American homeland is very real, the risk of occurrence of a particular kind of attack in a specific place is far less certain, primarily due to the dearth of precise threat information. Despite this uncertainty, government tends to respond to public fears of terrorist attack. Regulating in response to fear will impose costly security regimes that may mitigate fear without increasing security. A rational approach to security regulation will achieve greater increases in security per dollar spent by both government and business.

Achieving trust between government and business

Because neither government nor businesses can manage security risks alone, effective security risk-management requires cooperation and for each to set aside suspicions that have often characterized their roles in other regulatory contexts. A key responsibility for the new Department of Homeland Security will be to instill trust and facilitate the flow of threat information to the private sector.

The business role. Businesses have multiple incentives for investing in security: ensuring the continued existence of the business maintaining profitability; legal obligations; and competitive benefits and patriotism. And businesses are usually in the best position to assess vulnerabilities, devise cost-effective protection, and respond flexibly to adverse events. Before mandating security schemes, government should defer to business security initiatives. However, businesses also have limitations in making security investment such as limited loss potential; limited resources, limited capacity to protect due to significant interdependencies, and uncertainty surrounding the terrorism risk.

The government role. Although government brings unique strengths to the security arena, there are also significant governmental limitations. The traditional governmental "one size fits all" approach is unwieldy for the fast-evolving security arena. Government is less sensitive to the problem of substitution risk. Government is likely to be more willing to direct resources in response to public fear, even where the security risk is smaller than the public perceives. Finally, government often fails to develop the most effective and efficient solutions. Nonetheless, the public will look to government to play a role in ensuring enhanced security for the private sector.

Ensuring procedural fairness, transparency, and rational decision-making

If government does step in to regulate to reduce security risks, it should guarantee the greatest participation of the private sector through open and deliberative processes. Transparency not only ensures that public debate refines

and improves policy, but also reinforces the public-private cooperation necessary to implement homeland security initiatives.

Risk assessments should be the first step in developing any security regime. Any allocation of resources should then be made pursuant to a coherent and cost-effective risk-management strategy that includes examining alternative methods of securing an asset using the traditional tools of rational regulation. Policymakers must decide how much security they will consider "adequate" for a particular site or sector (given that there is no perfect or impenetrable level of security), determine whether additional security is required, and be explicit about what assumptions they are making and the level of uncertainty in the terrorism risk analysis, and compare costs of alternatives. Performance standards, incentives, and market mechanisms should always be favored over command-and-control regulation for achieving security objectives.

Determining who pays for added security

A security program that provides a benefit to only a select few should ideally be paid for by those beneficiaries. The traditional responsibility of government to guard our borders suggests that security risks of national significance should be overseen – and paid for – by the government. The challenge of allocating the costs of security occurs between these two ends of the spectrum – and is complicated by the nature of the terrorist threat. Any newly implemented security program should include a close analysis of the question of funding. If the government mandates extraordinary additional costs to enhance homeland security against terrorism, these costs should ordinarily be borne by the government.

APPENDIX O—LIST OF ABBREVIATIONS

2-PAM (Pralidoxime Chloride)
ACEP (American College of Emergency Physicians)
AFGP (Assistance to Firefighters Grant Program)
AG (U.S. Attorney General)
AHA (American Hospital Association)
AIC (Akaike Information Criterion)
ANSI (American National Standards Institute)
APHIS (Animal Plant Health Inspection Services)
ARTEP (Army Training and Evaluation Program)
ATF (Bureau of Alcohol, Tobacco, and Firearms)
ATTF (U.S. Attorneys Anti-Terrorism Task Forces)
BJA (Bureau of Justice)
BSL (Bio-Safety Level)
BT (Bioterrorism)
BW (Biological Weapons)
CAPPS II (Computer Assisted Passenger Pre-Screening System II)
CB (Chemical/Biological)
CBIAC (Chemical and Biological Information Analysis Center)
CBP (Customs and Border Protection)
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)
CIA (Central Intelligence Agency)
CMI (Consequences Management Interoperability)
CNN (Cable News Network)
CONUS (Continental United States)
COPS (Community Oriented Police Services)
CT (Counter Terrorism)
CTC (Counter Terrorism Center)
CW (Chemical Weapon)
DARPA (Defense Advanced Research Projects Agency)
DCI (Director of Central Intelligence)
DHHS (U.S. Department of Health and Human Services)
DHS (U.S. Department of Homeland Security)
DMAT (Disaster Medical Assistance Teams)
DoD (Department of Defense)
DOE (Department of Energy)
DOJ (Department of Justice)
DOT (Department of Transportation)
EIA (Electronics Industries Association)
EMI (Emergency Management Institute)
EMPG (Emergency Management Performance Grants)

EMS (Emergency Medical Services)
EMT (Emergency Medical Technician)
ENA (Emergency Nurse Association)
EOC (Emergency Operations Center)
EP&R (Emergency Preparedness and Response)
EPA (Environmental Protection Agency)
Epi-X (Epidemic Information Exchange)
ER (Emergency Room)
ERTP (Emergency Response Training Program)
FBI (Federal Bureau of Investigation)
FCC (Federal Communications Commission)
FCRP (Federal Rules of Criminal Procedure)
FDA (Food and Drug Administration)
FEMA (Federal Emergency Management Agency)
FinCEN (Financial Crimes Enforcement Network)
FISA (Foreign Intelligence Surveillance Act)
FISC (Foreign Intelligence Surveillance Court)
FTE (Full Time Equivalent)
FWMDPPS (Federal Weapons of Mass Destruction Preparedness Programs)
GAO (U. S. General Accounting Office)
GP (Grant Program)
HAN (Health Alert Network)
HAZMAT (Hazardous Material)
HHS (Health and Human Services)
HIPAA (Health Insurance Portability and Accountability Act)
HRSA (Health Resources and Services Administration)
HSC (Homeland Security Council)
HUD (Housing and Urban Development)
IAB (Interagency Board)
IAIP (Information and Infrastructure Protection Directorate)
ICS (Incident Command System)
IED (Incendiary Explosive Device)
IMS (Incident Management System)
INS (U.S. Immigration and Naturalization Service)
IOM (Institute of Medicine)
IRP (Improved Response Program)
IRS (Internal Revenue Service)
ISO (International Organization for Standardization)
JTTF (Joint Terrorism Task Forces)
LEAA (Law Enforcement Assistance Administration)
LEPC (Local Emergency Planning Committee or Commission)
LHD (Local Health Departments)
MMRS (Metropolitan Medical Response System)
MOU (Memorandum of Understanding)

MTSA (Marine Transportation Act)
MIPT (Memorial Institute for the Prevention of Terrorism)
NACCHO (National Association of City and County Health Officials)
NAEM (National Association of Emergency Managers)
NAHLN (National Animal Health Laboratory Network)
NCTC (National Counter Terrorism Center)
NDLEA (National Directory of Law Enforcement Administrators)
NDPO (National Domestic Preparedness Office)
NEA (National Endowment for the Arts)
NEIC (National Enforcement Investigation Center)
NFA (National Fire Academy)
NFPA (National Fire Protection Association)
NIAID (National Institute of Allergy and Infectious Diseases)
NIJ (National Institute of Justice)
NIOSH (National Institute for Occupational Safety and Health)
NIST (National Institute for Standards and Technology)
NORTHCOM (U.S. Northern Command)
NPSIB (National Public Safety Information Bureau)
NRC (Nuclear Regulatory Commission)
NSA (National Security Agency)
NTIA (National Telecommunications and Information Administration)
NWCG (National Wildlife Coordinating Group)
ODP (Office of Domestic Preparedness)
OEM (Office of Emergency Management)
OEP (Office of Emergency Preparedness)
OES (Office of Emergency Services)
OHS (White House Office of Homeland Security)
OJP (Office of Justice Programs)
OSHA (Occupational Safety and Health Administration)
OSLDPS (Office for State and Local Domestic Preparedness Support)
PPE (Personal Protective Equipment)
R&D (Research and Development)
RDT&E (Research, Development, Test, and Evaluation)
RFPA (Right to Financial Privacy Act)
ROE (Rules of Engagement)
RRIS (Rapid Response Information System)
S&T (Science and Technology)
SARS (Severe Acute Respiratory Syndrome)
SBCCOM (U.S. Army Soldier and Biological Chemical Command)
SCBA (Self Contained Breathing Apparatus)
SLATT (Anti-Terrorism State and Local Training Grants)
SOP (Standard Operating Procedure)
TANF (Temporary Assistance to Needy Families)
TIA (Telecommunications Industry Association)

TSWG (Technical Support Working Group)
TTIC (Terrorist Threat Integration Center)
USACLMS (U.S. Army Chemical School)
USAI (Urban Areas Security Initiative)
USC (United States Code)
USCG (U.S. Coast Guard)
USDA (United States Department of Agriculture)
USFA (United States Fire Administration)
UMTA (Urban Mass Transportation Administration)
WMD (Weapons of Mass Destruction)

APPENDIX P—PANEL ACTIVITIES—CALENDAR YEAR 2003

During the past year, the panel held five formal meetings:

March 20-21, 2003, RAND Washington Office, Arlington, VA
April 30-May 1, 2003, RAND Washington Office, Arlington, VA
June 16-17, 2003, RAND Washington Office, Arlington, VA
September 3-4, 2003, Headquarters, California Office of Emergency Services, Sacramento
November 17-18, 2003, RAND Washington Office, Arlington, VA

During the course of those meetings, panel members received presentations or engaged in categorical discussions as follows:

The Honorable Tom Ridge, Secretary of Homeland Security

The Honorable John Ashcroft, Attorney General of the United States

The Honorable Ann Veneman, Secretary of Agriculture (submitted written testimony)

The Honorable Robert Mueller, Director, Federal Bureau of Investigation, FBI organizational and mission restructuring (classified and unclassified)(two appearances)

The Honorable James Loy, Transportation Security Administration, Passenger Identification Technology

John Brennan, Director, Terrorist Threat Integration Center (classified)

John Poindexter, Defense Advance Research Projects Agency, Information Technology for Counterterrorism (classified)

Greg Saathoff, Critical Incidents Analysis Group, University of Virginia, Shielding Discussion

Mike Armstrong, Business Roundtable, Private Sector Discussion

Joe Samuels, International Association of Chiefs of Police

Ernie Mitchell, International Association of Fire Chiefs

Glen Woodbury, National Emergency Management Association

Steven Charvat, International Association of Emergency Managers

Bill Webb, Congressional Fire Services Institute

Mike Selves, National Association of Counties

James Ferguson, International Association of Fire Fighters

John Roquemore, National Association of Emergency Medical Technicians

Ted Macklin and Corey Gruber, Office of Domestic Preparedness, Department of Justice – Briefing on TOPOFF II

Sergeant John Sullivan, Los Angeles County Sheriff's Department, Terrorism Early Warning Group

Major General Paul Sullivan and Colonel Peter Alyward, National Guard Bureau

Armond Mascelli and Scott Conner, American Red Cross

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/nsrd/terrpanel. Unclassified minutes of the panel meetings are posted to that web page as soon as the panel has approved them.

The Advisory Panel also accepts written testimony and public comment. Written testimony and comments are also posted to the panel web site.

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 Q—RAND STAFF PROVIDING SUPPORT TO THE ADVISORY PANEL

Executive Project Director

Michael Wermuth

Co-Project Director

Jennifer Brower

Research Staff for the Report

Justin Adams	Bruce Don	Renee Labor	John Parachini
Gabrielle Bloom	Can Du	Francis Lacroix	Negeen Pegahi
Susan Bohandy	Ron Fricker	Josephine Levy	Kevin Jack Riley
Irene Brahmakulam	Michael Geruso	Michael Lostumbo	Heather Robertson
David Brannan	Bruce Hoffman	Nicole Lurie	William Rosenau
Robert Button	Susan Hosek	Lou Mariano	Paul Steinberg
Gary Cecchine	David Howell	Scott McMahon	Suzanne Spaulding
Peter Chalk	Brian Jenkins	Charles Meade	Michael Stoto
Kim Cragin	Felicia Joshua	Roger Molander	Terri Tanielian
Sara Daly	Seth Jones	Sarah Myers	Gregory Treverton
Teresa Dausch	Terrence Kelly	Sarah Cotton Nelson	Jeffrey Wasserman
Lois Davis	Jacob Klerman	Jennifer Pace	Barbara Wynn

Principal Administrative Support

Hillary Peck	Nancy Rizor	Michael DuVal	Elizabeth Whitaker

Other RAND Staff Providing Support

Kimberly Alldredge	Steven Drew	Barbara Lacy	Shirley Ruhe
Charles Allen	David Egner	Tom LaTourrette	Kimberly Sadler
Carole Berkson	Karen Echeverri	Lee Meyer	Irene Sanchez
Nurith Berstein	Leanna Ferguson	Phillip Mazzocco	Dan Sheehan
Stephen Bloodsworth	Dorothy Gardner	Ryan McKay	Dan Solosan
Roger Castle	Evelyn Gonzalez	Vanessa Miller	Diana Thornton
Bob Cheng	Monica Granados	Kathy Mills	Sandra Wade-Grusky
Christel Chichester	Hunter Granger	Paige Parham	Sophia Washam
Patricia Clark	Tyrone Greene	D.J. Peterson	Stephen Watkins
Leo Cloutier	Allison Hill	Joanna Polak	Deanna Webber
Tania Coderre	Candace Hoffman	Luetta Pope	Elwood Whitaker
Molly Coleman	Peter Hoffman	Monica Rodriguez	Patricia Williams
Ethan Collins	Douglas Kim	Carolyn Rogers	Ralda Williams
Linda Daly	Jessica Kmiec	Amy Rudibaugh	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

State and Local Empowerment

- Combine all departmental grant making programs into a single entity in DHS (DHS)
- Establish an interagency mechanism for homeland security grants (President)
- Develop a comprehensive process for establishing training and exercise standards for responders (DHS)
- Revise the Homeland Advisory System to include (1) a regional alert system (2) training to emergency responders about preventive actions; and (3) specific guidance to potentially affected regions (DHS)
- Establish sustained funding to enhance EMS response capacity for acts of terrorism (Congress)
- Reestablish a Federal office specifically to support EMS operational and systems issues (Congress)
- Establish a "Matrix" of Mutual Aid in coordination with local, State, and other Federal agencies, for a nationwide system of mutually supporting capabilities (DHS)

Private Sector Engagement

- Adopt the Business Roundtable's Principles of Corporate Governance security component (DHS and private sector)

Intelligence and Information Sharing

- Establish the Terrorist Threat Integration Center as an independent agency and require TTIC to have permanent staff from representative State and local entities (Congress)
- Develop and disseminate continuing comprehensive strategic threat assessments (Intelligence Community and DHS)
- Designate one or more security clearance-granting authorities, which can grant clearances Federal government wide that are recognized by all Federal agencies (President)
- Develop a new regime of clearances and classification of intelligence and other information for dissemination to States, localities, and the private sector (President)
- Develop a training program for State, local, and private sector for interpreting intelligence products (DHS)
- Establish comprehensive procedures for sharing information with relevant State and local officials (DHS)

Research and Development and Related Standards

- Establish a Federal Interagency Homeland Security Research and Development Council (President)

Psychological Preparedness

- Implement IOM Committee's recommendations on psychological preparedness (DHS and DHHS)
- Provide increased funding and DHS and DHHS monitor State and local compliance of incorporating in plans an appropriate focus on psychological and behavioral consequence preparedness and management (Congress, DHS and DHHS)
- Create a Federal task force on psychological issues, jointly led by DHHS and DHS (President)

Agroterrorism

- Designate DHS as the lead and USDA as the technical advisor on food safety and agriculture and emergency preparedness (President)


Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction
E PLURIBUS UNUM
1999-2001