



# Beyond the Beltway: Focusing on Hometown Security

---

## Recommendations for State and Local Domestic Preparedness Planning A Year After 9-11

*A Report of the  
Executive Session on Domestic Preparedness  
John F. Kennedy School of Government  
Harvard University  
September 2002*



## Introduction

---

September 11, 2001 awakened the United States to the threat of terrorism on American soil. Over this year, as both a memorial to those who died and an effort to prevent further attacks, there has been significant activity at all levels of government – federal, state and local – to buttress domestic preparedness and security. Due in part both to politics and the nature of the terrorist threat, however, there has been a tremendous focus on what the federal government is, or should be, doing. As we approach the one-year anniversary of 9/11, therefore, most attention has centered on a plan for reorganization within the Beltway.

Since the President announced a proposal this spring to create a Department of Homeland Security (DHS), there has been an almost endless fascination - some might say obsession - with the contours of a new Department that many hope will consolidate a variety of agencies and programs in order to give one central locus to domestic preparedness planning. However, few expect the DHS to be effective or even operational in the near future as the very action of moving so many pieces and people into place will inevitably disrupt before it unifies. It is a mistake, therefore, to expect that the creation of a DHS will resolve all of America's domestic preparedness deficiencies. As a nation, we risk sitting back, twiddling our thumbs, and waiting for the great federal fix while the clock ticks toward the next possible terrorist attack.

How we came to this point is not entirely clear. In the days after September 11, 2001, it seemed that the entire nation recognized that enhancing local and state capacities, or providing support for first responders, was instrumental in our fight against internal threats, whether it be a burning building or an odorless, invisible biological agent. Giving first responders a sense of the priorities they must set, the threats they may confront, and even the money to achieve preparedness appeared to be the real lesson of 9/11. Over the course of the year, however, as the federal government's deficiencies in preventing the attacks on 9/11 were disclosed, all attention focused on D.C.

This Report seeks to bring us back to the hometown, back to the ground level of preparation and planning that remains essential in our overall efforts. Looking beyond the top-down approach taken by the Department of Homeland Security, this report stems from a bottom-up perspective. Simply put, domestic preparedness requires action and emergency planning focused in our hometowns and not simply in our Nation's Capitol.

The dangers of an “inside-the-Beltway” focus on domestic preparedness are myriad. For example, states may be inclined to wait for cues provided by Congress before taking action. As a result, they may seek simply to mimic whatever federal reorganization plan emerges, with each attempting to create their own state Departments of Homeland Security. Effective domestic preparedness action, however, is not a one-size fits all venture. States and local capacities and resources do not mirror those of the federal government. The roles of state and federal governments in guarding against, and responding to, terrorist attacks also differ. Indeed, the variation in the size of states, as well as the potential targets within them, necessitate a more tailored domestic preparedness strategy.

Similarly, an “inside-the-Beltway” focus may lead the federal government itself to devote too much time and energy towards getting its own house in order. A successful national domestic preparedness policy, however, must be one that integrates state and local agencies and actors into the counterterrorism effort. Federal resources, whether monetary or technical, must be deployed to assist state and local preparedness efforts. However necessary, a new department in Washington, standing alone, will not suffice as a federal response.

*Beyond the Beltway: Focusing on Hometown Security*, therefore, is designed to spur federal, state and local officials to work together to ensure that the first line of defense on the homefront is not forgotten. To that end, this report focuses attention on the most urgent local and state needs and offers a blueprint for taking the kind of action that would address them. Out of the events of September 11 and the subsequent anthrax attacks, a consensus has emerged on some of the best practices, most needed capabilities, and broader lessons for meaningful domestic preparedness at the state and local levels. This

paper highlights these practices, needed capabilities, and lessons, offering concrete suggestions for implementation.

*Beyond the Beltway* contains a variety of recommendations that range across diverse fields, from public health to regional planning. Three broad themes, however, are consistent throughout.

First: plan, then act. Since September 11, even those who operate full-time in the field of domestic preparedness have found it difficult to keep track of the money, the programs, and the policies enacted in the flurry of activity. Although this haste is understandable in hindsight, there has been a lack of big-picture thinking about strategies and priorities for the best and most sustainable domestic preparedness planning. Thus, the report stresses the need for states and localities to develop comprehensive plans rather than piecemeal solutions. Time spent on planning for domestic preparedness, notwithstanding the urgency of the moment, is time well spent.

Second: act, then verify. There is no benefit to adopting new programs, despite the inevitable political incentives to do so, if they do not work when put to the test. New plans of action, therefore, must include mechanisms for systematic evaluation of their effectiveness over time. The terrorist threat is real, and it also is likely to be with us for some time. Unless some means of determining what is working and what is not are in place, states and localities run the risk of confusing action with success.

Third: act, but only if necessary. The report confirms the wisdom of the adage: “Do not reinvent the wheel.” There is no benefit, and potentially much harm, in adopting new programs when old ones will do. Although the terrorism threat is evolving continuously, many of the existing practices and policies of first responders can be utilized to assist in homeland security. For example, for years, local police departments have used community policing techniques against crime and have engaged their communities in those efforts. Those same tactics can be transferred to the terrorist threat. Adding new structures may only lead to difficult problems of coordination and the depletion of resources that would have been better spent on leveraging the capacities of first-responders that are already in place.

The report includes nine chapters. Each focuses on one substantive area of hometown domestic preparedness that has, as of yet, received far too little consideration. The Executive Session previously released a study on the issue of state and local communication interoperability, which concerns the ability of first responders to maintain radio contact during an emergency (see “Emergency Communications: The Quest for Interoperability in the United States and Europe,” by Viktor Mayer-Schönberger at [www.esdp.org](http://www.esdp.org)). This report brings attention to issues that have been far less well studied, but are no less critical. The nine areas are: personnel shortfalls, management of the psychological impact of terrorism, public health coordination, law enforcement planning, private sector engagement, regional preparation, domestic military efforts, public affairs, and the problem of sustaining domestic preparedness efforts.

The individual authors are all staff, members, or observers of the John F. Kennedy School of Government’s Executive Session on Domestic Preparedness (for a complete list of ESDP members, see [www.esdp.org](http://www.esdp.org)), a standing task force of leading practitioners and academics in homeland security. Many of the authors have primary responsibilities as managers of first-responder agencies, and all bring expertise to their topics. They have been part of a continuing series of roundtable discussions on homeland security since 1998, and thus they have been thinking, planning, and writing about domestic preparedness before the September 2001 attacks. The recommendations have benefited from these continuing conversations, publications, and the Kennedy School’s efforts in this urgent arena.

Our goal with this paper is to offer strategic recommendations for state and local planners based both on long experience and the perspective gained from the events of September 11, 2001.

Juliette N. Kayyem  
Executive Director

Arnold M. Howitt  
Director

Executive Session on Domestic Preparedness  
John F. Kennedy School of Government  
Harvard University

## Executive Summary

---

The importance of state and local domestic preparedness planning has been neglected as a result of the recent attention devoted to debates over the proposal to create a new federal Department of Homeland Security (DHS). An effective national domestic preparedness strategy must look beyond DHS to the needs and roles of responders in our hometowns. A bottom-up perspective is therefore critical. The following points suggest often simple, but extremely important, security measures that state and local governments can take to better prepare their own communities, and therefore the nation.

- **Avoid the Problem of Two-Hats:** Many first responders hold a variety of jobs in domestic preparedness efforts, from serving the National Guard to working as a voluntary firefighter. First responders who have multiple functions and responsibilities will thus wear “two hats.” Without a jurisdiction’s strategic assessment of off duty commitments, many localities will find that their domestic preparedness plans are ill-formed. Based on efforts in the Atlanta, Georgia, metropolitan area, this report provides a game plan for addressing the “two-hat” problem.
- **Involve Local Mental Health Personnel:** As was clear post 9/11, the psychological impact of terrorism has not been adequately addressed. Although the federal government may recognize the need for mental health care, responsibility for the mental health repercussions of rescue workers, for example, is not part of federal policy. Localities will need to think creatively about addressing those needs. By crafting roles for victims and bystanders, such as letting them volunteer or assist aid workers, the mental impact of terrorism can be diminished by giving the public a sense of control over a traumatic situation.
- **Look Beyond the Centers for Disease Control:** After the anthrax attacks, public health officials have been overwhelmed with trying to fix a public health system that has been neglected for decades. Congress has dedicated significant amounts of money to the cause, but local and state officials rarely set a vision for appropriate preparedness before they spend the money. Both within and between states, operational teams can be formed with the appropriate public health and safety officials to evaluate grant initiatives and, more importantly, to eliminate weak ideas.

- **Rely on Neighborhood Cops:** There has been tremendous discussion of the Federal Bureau of Investigation's law enforcement efforts before and after 9/11, but there has been too little assessment of actions that local and state police can take when facing an immeasurable threat such as terrorism. For years, local police have been practicing community policing skills to become better engaged with the people they seek to protect. By utilizing community policing skills from lessons learned in Charlotte, North Carolina, we can better engage local police efforts against the next threat.
- **Engage Hometown CEOs:** Domestic preparedness planning is not simply a government effort. Most people spend a significant part of their day within private institutions, each with their own communication, transportation and security systems. Federal efforts to coordinate with the private sector are often too geographically and industry diverse to be effective. Based on efforts in the city of Washington D.C., "low key" approaches to engaging businesses, such as linking first responders with a corporation's head of security, can be the foundation of important planning and partnerships.
- **Work Together as a Region:** A single jurisdiction cannot fight terrorism, nor will terror remain within a town's borders. Since 9/11, the need for real regional cooperation has never been more apparent, even though federal planning tends to focus solely on state and local boundaries. Efforts in Los Angeles, California, show that by creating benefits that encourage regional cooperation, and reducing the legal and operational risks of collaboration, local jurisdictions can find that working across boundaries lowers the cost of homeland security.
- **Embrace the Soldiers at Home:** The Department of Defense has, since 9/11, enhanced its own role in homeland security. These enhancements pose significant operational, and legal, concerns. Local domestic preparedness planners, however, need not look to the federal military for the ultimate solution. By learning from our nation's history with the "war on drugs," each state's National Guard may already prove to have the necessary capabilities and capacities.
- **Educate Local Media:** The sense of security felt by members of the mass media themselves will have a tremendous impact on the public's sense of safety. The national media will focus on threats and domestic preparedness policy at the national level. Local media can play a key role in defining the particular threat for a community as well as suggest steps to take at home to prepare for it. Indeed, a reporter's own sense of safety will inevitably impact her telling of the news. Local responders can easily



provide the media with training in hostile and hazardous environments, as is so often done for other dangerous assignments.

- **Don't Specialize, Generalize:** In the absence of another successful terrorist attack since the fall of 2001, the public's perception of the risk will diminish. Political interest may then wane. Sustaining a long term and successful preparedness program for each state and locality will be difficult because of this "boom or bust" prioritization. Domestic preparedness is sustainable the less a jurisdiction focuses on terrorism specialties, and the more it subsumes domestic preparedness planning into an overall all-hazards approach.

These issues are as urgent and necessary as any federal reorganization plan. Indeed, while the federal government plays the primary role in preventing terrorism (through military action, intelligence gathering, or controlling our borders through immigration), once a terrorist attack occurs, it is the first responders who will be prominent again. In the midst of flowcharts and puzzle pieces, we simply cannot afford to be distracted.

September 3, 2002

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

## Contents and Chapter Authors

---

<i>Introduction.....</i>	<i>i</i>
<i>Executive Summary.....</i>	<i>v</i>
<i>Contents and Chapter Authors .....</i>	<i>viii</i>

<i>CHAPTER 1 — The “Two-Hat Syndrome”: Determining Response Capabilities and Mutual Aid Limitations .....</i>	<i>1</i>
<b>Rebecca F. Denlinger with Kristin Gonzenbach</b>	

**Rebecca F. Denlinger** is Chief of the Cobb County, Georgia, Fire Department and is a member of the Executive Session on Domestic Preparedness (ESDP).

**Kristin Gonzenbach** is a Managing Partner at Callahan Management Strategies, LLC.

<i>CHAPTER 2 — After the Attack: The Psychological Consequences of Terrorism .....</i>	<i>6</i>
<b>Robyn Pangi</b>	

**Robyn Pangi** is a Research Associate with the Executive Session on Domestic Preparedness.

<i>CHAPTER 3 — Local and State Public Health Planning.....</i>	<i>11</i>
<b>Ralph Timperi</b>	

**Ralph Timperi** is Assistant Commissioner of the Massachusetts Department of Public Health (DPH), and Director of the DPH State Laboratory Institute. He is a member of the Executive Session on Domestic Preparedness.

<i>CHAPTER 4 — The Policing Challenge .....</i>	<i>15</i>
<b>Darrel W. Stephens and Francis X. Hartmann</b>	

**Darrel W. Stephens** is Chief of the Charlotte-Mecklenburg Police Department, North Carolina, and is a member of the Executive Session on Domestic Preparedness.

**Francis X. Hartmann** is Executive Director of the Malcolm Wiener Center for Social Policy, Senior Research Fellow of its Program in Criminal Justice Policy and Management, and Adjunct Lecturer in Public Policy at the John F. Kennedy School of Government, Harvard University. He is a member of the Executive Session on Domestic Preparedness.

<b>CHAPTER 5 — Engaging the Private Sector.....</b>	<b>23</b>
<b>Juliette N. Kayyem and Patricia E. Chang</b>	
<b>Juliette N. Kayyem</b> is Executive Director of the Executive Session on Domestic Preparedness at Harvard University’s John F. Kennedy School of Government. She served on the National Commission on Terrorism from 1999–2001.	
<b>Patricia E. Chang</b> is a Research Assistant with the Executive Session on Domestic Preparedness.	
<b>CHAPTER 6 — Promoting Regional Collaboration.....</b>	<b>28</b>
<b>Arnold M. Howitt</b>	
<b>Arnold M. Howitt</b> is Director of the Executive Session on Domestic Preparedness, and Executive Director of the Taubman Center for State and Local Government at the John F. Kennedy School of Government, Harvard University.	
<b>CHAPTER 7 — The “Local” Military .....</b>	<b>32</b>
<b>Major General Philip Oates</b>	
Major General <b>Philip Oates</b> is Adjutant General of Alaska, Commissioner of the Alaska Department of Military and Veterans Affairs and Emergency Services, and the Governor of Alaska’s point of contact for Homeland Security. He is a member of the Executive Session on Domestic Preparedness.	
<b>CHAPTER 8 — Utilizing the Mass Media .....</b>	<b>35</b>
<b>Peter Van D. Emerson</b>	
<b>Peter Van D. Emerson</b> is President of the consulting firm of Emerson Associates International. He is a recent graduate of the John F. Kennedy School of Government and is an observer of the Executive Session on Domestic Preparedness.	
<b>CHAPTER 9 — Sustaining Preparedness .....</b>	<b>38</b>
<b>David Grannis</b>	
<b>David Grannis</b> is Senior Policy Advisor to Congresswoman Jane Harman (D.-Calif.) on terrorism, intelligence, and defense issues. He worked as a Research Assistant for the Executive Session on Domestic Preparedness in 1999 while a student at the John F. Kennedy School of Government.	
<b>Conclusion .....</b>	<b>43</b>
<b>Endnotes.....</b>	<b>44</b>

*Thanks are owed to Rebecca Storo, Assistant Director of the Executive Session on Domestic Preparedness, for her tremendous support, and to consulting editor Teresa Lawson.*

*This project was supported by Grant No. 1999-MU-CX-0008 awarded by the Office for Domestic Preparedness, Office of Justice Programs, U.S. Department of Justice. The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program offices or bureaus: the Bureau of Justice Assistance, the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.*

## **CHAPTER 1 — The “Two-Hat Syndrome”: Determining Response Capabilities and Mutual Aid Limitations**

---

*Rebecca F. Denlinger with Kristin Gonzenbach*

Whenever a large-scale emergency occurs, there is a corresponding surge in the number of activities requiring the services of first-responder agencies, a vast group that includes police, fire, emergency medical services (EMS), 911 communications, public health, emergency management, and sheriffs’ agencies. Many first responders are public safety employees, but a significant number are private providers, especially in Emergency Medical Services (EMS) and police services. Emergencies that cause a surge lasting days, weeks, even months or years are unusual, but they have now become more likely with the rising incidence of terrorism and the threat of deadlier, more powerful attacks. Thus, in order to deliver and sustain operations at an increased level of service, first-responder employers must have a “surge capacity” of personnel that may respond to such events.

Many first-responder employers have therefore developed call-up plans designed to increase the number of personnel available to perform the agency’s mission during a disaster. Call-up plans generally assume that off-duty personnel will report to work when contacted in order to expand the agency’s capability. However, many emergency workers, particularly fire and rescue employees, work at more than one first-responder agency. We describe this as the “two-hat syndrome.” In a large-scale emergency, these workers might be called upon to perform both jobs, that is, to wear both hats. When called up, many of the off-duty employees may be at work on their second jobs at these other agencies. Calling them in means they would have to abandon assigned duties at private ambulance services, local hospitals, or neighboring fire departments. Thus it narrows the pool of personnel for nearby volunteer fire departments, because in reality, each employee would be able to fill only one position.

First-responder agencies must therefore identify which employees wear more than one hat, gauge how critical each of those hats is to each employer, and consequently assess the region’s ability to manage a disaster. In order to successfully manage personnel

during a disaster, leaders of first-responder agencies must gather and share this information. This information is crucial to a reliable call-up plan, which must be tested and implemented.

### **Recommendations**

1. Assess Off-Duty Commitments
2. Determine Impact on Call-up Personnel
3. Share Information across Borders
4. Develop Alternative Personnel Solutions
5. Test and Implement

#### **1. Assess Off-Duty Commitments.**

First-responder agencies and employers should, first, conduct a survey of their workers to reveal how many have secondary employment at another first-responder agency. Of particular concern is that extended breaks between long shifts has allowed many first responders, especially firefighters and EMS personnel, to make significant commitments to more than one agency. The “secondary” employer is likely to depend upon the employee as much as the “primary” employer. The “Two-Hat Project Survey,” conducted in fourteen counties in the Atlanta metropolitan area, found, for example, that among sixteen fire departments, an average of 22.2 percent of employees hold two or more first-responder positions. Moreover, a significant percentage of the public safety workforce has commitments to the military reserve or National Guard. The survey revealed that a military call-up would affect police and sheriff agencies even more than fire and rescue agencies. One law enforcement agency reported that 13 percent of its personnel have military obligations.<sup>1</sup> The Two-Hat Survey showed that communities might not have a firm grasp of what personnel will be available in a disaster. Agencies might be hard-pressed to identify the number of employees who wear two or more hats, where else these people work, or how this might affect disaster response plans. The fact that more than one responder agency may rely on the same employee may critically affect both agencies’ effectiveness in time of disaster.

## **2. Determine Impact on Call-Up Personnel.**

It is crucial to plan who will wear which hat in a disaster. Interviews revealed that even many chief officials of public safety agencies fit the two-hat profile, but had not considered the problem or their own limitations when planning for disaster. The smaller the agency, the greater the impact if those wearing two hats cannot fulfill both duties during a disaster. In the case of large jurisdictions, a disastrous incident is likely to magnify the impact of overworked personnel or those with duplicate commitments. Plans must be in place to determine who will fill these roles should it be necessary to staff more than one commitment during a crisis. In addition, should agencies lose employees to military commitments, plans should address who will back up any critical positions left vacant.

## **3. Share Information Across Borders.**

The information and analysis resulting from such surveys must be shared with other agencies and jurisdictions that may be relying on the same personnel. For example, the nationwide shortage of health care workers has meant that a growing number of firefighter emergency medical technicians and paramedics are recruited for part-time and full-time employment in local hospitals. This raises questions about how many EMS workers are actually available in a given area, should these employers need to expand service. Private entities, such as ambulance contractors that transport patients, often employ significant numbers of off-duty firefighters and EMS workers. In one case in Cobb County, Georgia, 33 percent of an ambulance company’s workforce consisted of off-duty firefighters. Other conflicts arise when career fire and rescue personnel volunteer in considerable numbers at fire and rescue departments agencies in other jurisdictions. If these personnel respond to their primary employers, fewer will be left available to serve volunteer fire departments. Thus sharing of “two-hat” information among agencies is crucial.

## **4. Develop Alternative Personnel Solutions.**

Since there may be significant personnel deficiencies in call-up plans, both innovation and flexibility are necessary. For example, when Cobb County Fire and Emergency

Services became aware of the fact that its employees constitute one-third of the workforce of one of its ambulance providers, it realized that a personnel call-up might have a crippling effect on the ambulance company's ability to transport patients. In a disaster, the community's interests require both an effective fire department and an effective ambulance service. Thus, disaster plans now call for ambulance company managers to work with officials in the county emergency operations center to staff and dispatch ambulances from fire stations until personnel issues stabilize. Another solution may include holding some staff in reserve to provide a sustained response. The Arlington County, Virginia Fire Department made a number of policy and procedural changes in its disaster plan after the 9/11 Pentagon incident. It has changed its call-up strategy to add the ability to build up its force incrementally, rather than calling in all off-duty personnel at once. The department has also begun utilizing an automated telephone system for notifying personnel, thereby removing this critical and staff-intensive assignment — a sort of second hat — from its dispatch center. Chief Plaugher and his staff prefer not to have to rely on the media to notify personnel, as they did in the Pentagon incident.<sup>2</sup>

## **5. Test and Implement.**

In order to create a call-up plan to manage personnel successfully during a disaster, agencies must plan to rotate personnel on and off shifts to maintain a strong and alert work force, and take into account the off-duty obligations that some employees have. Second, agencies must communicate to personnel how these call-up plans work, in order to manage employee expectations, as well as to train employees in the plan's use before a disaster occurs. Third, agencies must practice the call-up plan, and factor in contingencies such as reasonable travel time. This will help reveal any problems, including those that result from the two-hat syndrome, and will allow agencies to develop solutions for those problems. Activation plans should be practiced to determine their true feasibility and allow for necessary adjustments, and agencies must then review and modify the plans if necessary. After gathering, analyzing, and sharing information, and developing, selecting, testing, and reviewing a plan, implementation of the agency call-up plan requires publishing and distributing the plan to all personnel, and making sure that neighboring first responders are aware of its status and content. This cycle of activity should be



repeated as circumstances change, and information regarding personnel becomes obsolete.

## CHAPTER 2 — After the Attack: The Psychological Consequences of Terrorism

---

*Robyn Pangi*

History suggests that there may be even more psychological victims than physical victims in a terrorist attack. This is evidently true for a conventional attack, such as the use of hijacked aircraft to destroy high-occupancy buildings: while the 2001 attacks on the World Trade Center and the Pentagon resulted in thousands of deaths and physical injuries, the psychological casualties numbered in the tens to hundreds of thousands. An attack using a weapon of mass destruction (WMD) — a biological, chemical, nuclear, or radiological device — might produce even more extreme numbers. Psychological casualties easily outnumbered physical casualties due to the anthrax attacks in the United States in 2001: they resulted in 23 illnesses and five fatalities, but they affected millions. Likewise, the sarin attacks in the Tokyo subway system in 1995 engendered thousands of psychological casualties, in addition to a dozen fatalities and hundreds of injuries. Indeed, these psychological effects are integral to the “success” of the terrorist actions.

“Fear management” comprises the programs that reduce the incidence of adverse psychological effects following a disaster. Fear management is, technically, “the mitigation of panic and the management of public response following a WMD or other mass casualty incident,” but should not be limited to waiting for the next attack.<sup>1</sup> Effective fear management is built upon an understanding of the potential psychological effects of a WMD terrorist attack. It is critical to anticipate victims’ reactions so that first responders can plan accordingly. In other words, panic and shock would affect response operations and must be anticipated. On the other hand, if — as studies indicate — panic is relatively rare, first responders need to plan for more likely scenarios such as an influx of the “worried well” at hospitals, and a convergence of volunteers and concerned parties at the scene, which can overwhelm existing systems. Moreover, since early intervention can mitigate the psychological impact of trauma, both short-term and long-term, response planning should include assistance for victims who are dealing with psychological effects

of WMD terrorism, such as acute stress disorder, post-traumatic stress disorder, and depression.

Many emergency management plans currently lack well-developed mental health components. There is a lack of comprehensive response plans for fear management. This translates to a gap in preparedness on the part of federal, state, and local governments. The psychological impact of a WMD terrorist event need not cripple the community. The deleterious psychological effects of WMD terrorism can be ameliorated if a well-defined mental health plan is incorporated into emergency response plans. Such a plan should include all the tools of fear management.

### **Recommendations**

1. Address the Fear
2. Minimize Convergence at the Scene
3. Cross-Train
4. Strengthen State and Local Resources
5. Craft Roles for Victims and Bystanders
6. Intervene Early and Widely
7. Broaden the Definition of At-risk Individuals

### **1. Address the Fear.**

Despite some fears that the public might panic, if informed accurately of unprecedented threats, a well-informed public is in fact capable of acting in its best interest in the face of such threats. Since 1995, and particularly since the anthrax attacks in 2001, many U.S. government officials and mass media have been increasingly vocal regarding the terrorist threat. They have not, however, properly emphasized the low probability of attack, but instead, have emphasized the potential for catastrophic consequences, as well as America's lack of preparedness to meet this burgeoning threat. This type of communication between policymakers and the public can be counterproductive if it fails to explain how threat assessments are reached and what is being done to improve the

country's preparedness. Government officials must take this one step further by communicating both what the threat is, and how the assessment has been made. An educational campaign to inform citizens of the nature of potential weapons and appropriate responses is a necessary complement.

## **2. Minimize Convergence at the Scene.**

Experience suggests that people will tend to flock to the site of an attack, out of concern for others' safety, curiosity, or desire to volunteer. However, such convergence can be dangerous to the public and may hamper rescue and remediation efforts. One of the best ways to reduce convergence is by sharing information. A good public information campaign with regular updates on the situation removes the need for concerned family, the "worried well," and curious outsiders to enter the stricken area to seek information first-hand. A good way to communicate with the public, of course, is through the mass media, but this is not simple. Full disclosure to the media (within reasonable bounds) is critical, because withholding information may cause unnecessary and often detrimental alarms. Officials should be concerned with getting out accurate information, especially after misleading rumors begin to circulate.

Full disclosure can also alleviate "telecommunications convergence," which could overwhelm the communication infrastructure. Spokespersons for government and first-responder agencies can ask people to stay away from the scene and to refrain from calling emergency phone numbers unless they are facing a genuine emergency. They can also reduce the number of non-emergency calls by shifting to a "comprehensive news policy," giving out information that answers questions before people call to ask them, and reporting on areas not hit by disaster, as well as those that are, so people do not wonder if relatives or friends in those areas are affected.

## **3. Cross-Train.**

Cross-training is important: agencies should train first responders in mental health response, and mental health professionals in disaster response. Response personnel are often the first on the scene to interact with victims and their families; thus they need training on how best to handle fears. Just as response agencies prepare rescue workers for

the physical demands of their work, they should also prepare them for the psychological demands. They should emphasize two aspects of mental health training: preparing response personnel for their own psychological trauma, and training them to help with the trauma experienced by victims and witnesses. Mental health professionals, meanwhile, must be trained in the specifics of responding to a WMD terrorist attack, such as how to work in a contaminated environment, and wear a gas mask or other protective gear that may be needed.

#### **4. Strengthen State and Local Resources.**

The mental health needs of victims cannot be addressed by the federal government alone, yet current plans rely too heavily on federal resources rather than developing local assets. Federal law provides insufficient resources to meet the needs of victims, who will be spread throughout the nation and will require assistance over the long term. Executive orders such as Presidential Decision Directive 39 may place responsibility for domestic terrorism response in the federal arena, but responsibility for the mental health repercussions on rescue workers, for example, is not part of federal policy. This is justified on the basis that the federal government supports state and local governments in domestic disasters, but does not have a primary role in these matters. Therefore, the federal government has the responsibility for, but neither the institutional investment in nor the capability to pursue, a comprehensive disaster mental health response plan. Thus, state and local resources should be prepared to bear the brunt of these needs.

#### **5. Craft Roles for Victims and Bystanders.**

Psychological intervention may well begin in the immediate wake of the attack. In a mass casualty attack there may not be enough trained professionals to aid the victims. Hence, it may be necessary to craft roles for victims in the response effort, something as basic as serving beverages to aid workers. This may help fill the void, and there is also a secondary benefit: a terrorist attack is by its nature particularly stressful, but it may be more than the stress that is dangerous to individuals. The victim's inability to cope with stress, or sense of helplessness, may lead to greater psychological damage. Experts believe that an individual's ability to change a situation has a great impact on the onset

and severity of psychological distress. Thus, establishing useful roles for victims may be the first and most important step toward their psychological recovery.

## **6. Intervene Early and Widely.**

Professional mental health intervention may be required for victims after a WMD attack. Experts agree that early intervention is one key to preventing acute stress disorder and post-traumatic stress disorder, and mitigating the severity of these conditions. Intervention by trained professionals is only one aspect of a fear management program. There is also a significant role for community groups, trained lay people, and victims. Community groups (such as religious or civic organizations) can augment the cast of mental health professionals, bringing a greater sense of community support to the victims and providing useful roles for individuals who might otherwise join the ranks of the “worried well” or emotionally distressed. Working with community groups might also remove the stigma that can still surround psychiatric care.

## **7. Broaden the Definition of At-Risk Individuals.**

The population that is at risk of experiencing psychological disorders after a terrorist attack spreads far beyond the immediate perimeter of the attack scene. Friends, family, the “worried well,” colleagues, and concerned citizens may all suffer from emotional distress after an attack. A telephone study done to assess the immediate mental health effects of September 11 found that over 40 percent of the adults surveyed reported one or more substantial symptoms of stress, and 90 percent had one or more symptoms at least to some degree. The survey concluded that in general, after the September 11 attacks, adults and children across the country displayed substantial symptoms of stress. Because it is impossible to counsel every individual across the nation, multiple outreach tools must be available to explain the nature of the attack, possible outcomes, knowns and unknowns, the range of normal emotional reactions, and avenues for seeking mental health assistance for those who are affected.

## CHAPTER 3 — Local and State Public Health Planning

---

*Ralph Timperi*

Local and state public health agencies face major challenges to the development of a system for effective preparedness and efficient response to a terrorist attack using biological, chemical, or radiological weapons. For public health agencies, there are fundamental issues that make planning for unexpected acute illness affecting large numbers of people very difficult. These include the epidemiology of illness, the communication of risk, and the plurality of public and private systems.

First, the effects of an attack occur across political and institutional boundaries. The effects of an attack with an infectious agent, in particular, may be widespread, but the resources and institutions, including the political organizations that respond to these health events, are fixed. Second, the potential fear, terror, and anxiety evoked by fatalities, illnesses, and injuries due to such attacks know no geographic or political boundaries. The communication of the event and its associated stresses on people is global and rapid. Third, the response to a major event requires coordinated planning and access and integration of all available resources, but the multiplicity of systems makes this difficult.

Current initiatives that depend on new technology development and deployment, but that lack adequate problem definition or assessment of the value of intervention and of likely outcomes, are unlikely to be effective. The following recommendations therefore focus on harnessing existing but under-recognized or underutilized expertise and resources. They seek to quicken the pace of infrastructure improvements, especially at the local level. They focus on planning, problem-solving, and evaluation initiatives to achieve tangible improvements in preparedness.

### **Recommendations**

1. Plan First
2. Prioritize Second
3. Integrate Interagency Teams for Problem Solving
4. Strengthen the Foundation of Early Disease Surveillance
5. Target Resources

#### **1. Plan First.**

The harmonious orchestration of the components of the public and private sector may be even more critical to successful prevention of the effects of bioterrorism than the development of new technologies. Successful preparedness requires a strong and thoughtful effort to build infrastructure at the local level, public and private sector involvement in planning and practice, and functional network development that assures communication and coordination among the nation's heterogeneous political and private organizations. This cannot be done without some planning and foresight. Considerable resources are finally being provided to rebuild and modernize the public health infrastructure after decades of neglect. However, we risk wasting valuable resources and time on unnecessary efforts unless there is adequate strategic planning. The public health planning process to create the means for effective communication, coordination, and control of resources, is key.

#### **2. Prioritize Second.**

State health officers should convene a working retreat to facilitate, collectively and individually, a vision for public health preparedness in the states. They should aim to create a blueprint for full participation by local health representatives and the private sector in planning, infrastructure improvement, and definition of responsibilities. They should provide leadership to bring together public safety and private-sector partners to craft principles of collaboration, identify shared goals, and specify timelines for achieving critical milestones. The participants should evaluate the federal and other grant initiatives to identify best practices, eliminate weak ideas, and prioritize specific goals.



### **3. Integrate Interagency Teams for Problem Solving.**

Public health must have a strong, well-knit network at the local and state levels to participate effectively in planning and capacity building. This will require overcoming the effects of years of neglect in the public health infrastructure. Nevertheless, it is essential for the diverse players to work through processes of strategic planning and problem-solving toward a system that can prevent or minimize the deaths and harm that might be caused by bioterrorism. Within and between states, operational teams should be formed with the appropriate public health and safety, environment, fire, police, medical, National Guard, academia, and other representatives. These teams should work on developing solutions to problems that have been identified in preparedness planning and operations. These teams would be a resource for surge-capacity problem-solving during an actual event, by providing advice and consultation for the operational managers and decision-makers who are weighed down with situational issues. Effective communication — including secure electronic information communication of disease information among those many partners who need to know — must become integral to the system, not merely superficial add-ons mandated in pre-planned exercises and top-down requirements.

### **4. Strengthen the Foundation of Early Disease Surveillance.**

Improved reporting of disease can be achieved through increased training and basic resources for individuals within the disease surveillance system. A major investment is needed in education and training for health workers at the local level in both public and private sectors - health departments, hospitals, doctors' offices, schools, companies, and so forth - to eliminate chronic underreporting and delayed reporting of disease that occurs in non-outbreak periods. More powerful statistical techniques and more rapid testing is not useful without a specimen for testing or an illness report. Disease reporting must be sensitive and reliable enough to detect the early few cases that occur in natural or deliberate outbreaks. Timely recognition of the first cases is the key to effective response and prevention. Reliable disease reporting would provide information to enable linkage of even a few seemingly unrelated cases, through the use of analytical tools that should become available in the surveillance system.

## **5. Target Resources.**

This vision of a National Electronic Disease Surveillance System (NEDSS) must be translated quickly into practice for use at the local level. Development of model systems can be accelerated by targeting rewards to a few promising systems that are in development in state or local jurisdictions. Governors and mayors can aid the development of a vision for what is needed at the state and local level through promotion and support of collaboration between states and municipalities. There must be political commitment and cooperation to produce a working model that links more than one state and several municipalities for confidential electronic information sharing, which cannot afford to be done piecemeal. There must be a basic system in place for a national network of local and state health agencies that can deliver real-time confidential information and clear advisories to the public through multiple distribution channels, including the media. The private sector can be invited to aid this effort since they have the technology and actual systems that could supply many of the essential components of preparedness.

## CHAPTER 4 — The Policing Challenge

---

*Darrel W. Stephens and Francis X. Hartmann*

Many police executives have recognized, since the events of 9/11, that the threat of terrorism is real and that it must be given an important place in the myriad priorities that require their attention. To be sure, it had already been a part of the landscape, given the 1993 World Trade Center bombing, the 1995 Oklahoma City bombing, and other incidents throughout the world. But until now, terrorism has competed with more pressing demands such as street crime, or the shift from traditional policing approaches to building problem-solving relationships with members of the community. The complexity of the terrorist threat in our fast-paced world, where all of the other problems are still on our plate and new problems are constantly emerging (such as identity theft, cyber crime, and budget reductions), requires that the police develop new partnerships and strengthen old ones to prevent and respond to terrorist acts.

The police and the community in general must begin to see terrorism through different lenses than what we have historically used to view criminal acts, such as homicide. The motivation of those engaged in terrorist acts is not the same as a gang fighting over turf to sell drugs or striking out in revenge for some real or perceived slight. Nor are the threats the same: for example, the police and their communities must learn for the first time to deal with biological organisms intentionally released in order to take lives. In such cases, police departments will depend on other experts, such as public health officials who have not generally been pressed, to act on limited, incomplete information. Steps are now underway in many cities across America as police departments begin to rethink the threat of terrorism and what it means for law enforcement.

### **Recommendations**

1. Know Your Weakness
2. Integrate Terrorism into the “All Hazards Plan”
3. Emphasize Both Response and Prevention in the “All-Hazards Plan”
4. Develop Police Resource Utilization Plan
5. Exercise — Exercise — Exercise
6. Ensure Acquisitions are “Dual Use”
7. Isolate Fear Strategically
8. Utilize Community Policing Skills

#### **1. Know Your Weakness.**

A realistic assessment of what infrastructure is critical, and of other potential targets in the region, should be conducted. Problems must be corrected and steps taken to mitigate vulnerability when and where possible. Most communities have critical infrastructure that might be a target for terrorists. Mitigation efforts must therefore balance the potential threat with the cost to decrease or eliminate vulnerability. Without some sense of the local vulnerability, police will not know how to prioritize their efforts.

For example, control on parking around critical infrastructure is a reasonable and low-cost measure that could improve early identification of a potential problem and facilitate emergency response if a car or truck bomb were detonated. Training employees to be watchful for potential problems in critical infrastructure can make an important difference in the overall level of security. A well-thought-out and practiced evacuation plan is also helpful in saving lives and reducing fear in a variety of situations. These mitigation initiatives and other appropriate measures will contribute to deterring additional potential crime or security problems.

Other, more fundamental changes, may mitigate future terrorist harm. Strategic thinking about architecture, design, and the position of buildings, streets, and businesses should guide future development. Crime Prevention Through Environmental Design (CPTED)

has been applied in a wide range of settings in Charlotte, N.C., for several years as a crime prevention tool, and it has been particularly helpful since 9/11 when analyzing vulnerability in critical infrastructure and strengthening security against terrorist incidents.

## **2. Integrate Terrorism into the “All-Hazards Plan.”**

Cities, counties, and some regions have developed what is called an “All-Hazards Plan” to respond to events that require a large-scale coordinated multi-agency response. These events might include natural disasters such as hurricanes, floods, earthquakes, and tornados, civil disorder, or any other critical incident such as an airplane crash, train derailment, building collapse, bombing, or school shooting. The fundamental structure of the plan offers a solid foundation for developing a coordinated response to a terrorist incident. Specific annexes should be prepared to address the particular issues that terrorist incidents are likely to produce.

Where multiple agencies are involved, an Incident Command System (ICS) is useful. An ICS is a design for “ad hoc emergency management teams that coordinate the efforts of more than one agency under a unified command. It is a functionally based organizational template that facilitates information flow, decision-making, and operational coordination.”<sup>1</sup> ICS is a model for providing direction and oversight to the terrorist response effort. This is an approach that fire personnel use in their daily operations, but it is foreign to many police departments and other government agencies such as public works or public health. The “All-Hazards” plan should be structured around the ICS, and all agencies should understand this approach.

The police in particular need to work on improving their understanding of the ICS. There are numerous situations where incident command would be appropriate for day-to-day police operations. SWAT responses, major conventions, and large spectator events provide opportunities to develop and improve incident command skills. Communications interoperability is a particular challenge for emergency response throughout the nation; many local police departments cannot communicate with their local fire departments during a crisis. While there are significant technical challenges with bandwidth, which

should be a high priority for local government officials, a unified all hazards plan should address the difficulties with interoperable communications, assuring that they are disclosed and addressed.

### **3. Emphasize Both Response and Prevention in the “All-Hazards Plan.”**

Prevention must be an equally important emphasis in dealing with terrorism and, locally, police are in the best position to play a leadership role. Response to terrorist acts is, at least in the earliest stages, a local responsibility. Prevention of terrorism, on the other hand, is an amalgam of federal, state, regional, and local agency responsibilities. This set of relationships is being newly tested. These developing relationships — federal, state, regional, local — must be characterized by information sharing, joint problem solving, a fair sharing of resources, and the trust that is earned by working together to achieve a very important common goal.

Locally, a key aspect of prevention lies in addressing vulnerabilities in critical infrastructure (“threat assessment”). Equally important for local governments is the intelligence aspect of positioning the police so as to gain as much early warning as possible of any activities directed against the community. One way is to take part in the FBI Joint Terrorism Task Forces. Another is to develop information sources on a local level that might identify local residents who could likely engage in terrorist activities. A system should be established for evaluating those calls from suspicious citizens who tip the police when something unusual is taking place. Knowledge of local organizations that support or advocate terrorist acts is an important aspect of understanding the potential vulnerability of a community. The police are uniquely positioned to play a leading role in the local aspect of prevention of terrorism.

### **4. Develop Police Resource Utilization Plan.**

Serious thought must be given to the tasks that police will be expected to perform in response to a terrorist act. The “All-Hazards Plan” must provide clear direction on how police personnel will be deployed, the types of calls that will be handled, and the types of assignments that will or will not be permitted. Following 9/11 most police departments in America found themselves making assignments that were never before contemplated

in their emergency response plans. Community fear and unrealistic expectations quickly depleted police resources. Police departments that never had responsibility for airport security found themselves with a new role, sometimes with conflicting directions coming from the Federal Aviation Administration, airport authorities, and the airport police. In some cities, police officers were guarding military facilities for several days. Officers engaged in secondary employment provided a significant amount of the security for critical infrastructure and other locations. In a non-crisis situation, it is commonly understood that the first responsibility of a police officer is to the department and community. It is easy to say that secondary employment will be suspended during emergency situations. Yet, suspension of secondary employment is much more difficult in practice when the private sector owners of critical infrastructure are making legitimate calls for increased protection in the middle of managing the crisis.

Local government leadership must be engaged in thinking through the resource allocation policies under emergency circumstances (as Chapter 1 by Rebecca Denlinger with Kristin Gonzenbach details). The pool of police officers can be too quickly exhausted through filling assignments that were not contemplated in the development of the emergency response plan.

### **5. Exercise — Exercise — Exercise.**

The most effective responses by local governments to major incidents have come from those who have developed a good plan and who exercise it on a regular basis with a variety of scenarios. There are shelves full of plans waiting to be implemented but are never tested even in tabletop or mock exercises. In many cities, the police have become quite proficient at dealing with a wide range of issues. Police generally work well with other local government agencies if they are seeking help from them in dealing with a particular problem. Where more effort needs to be applied is the process of working as a team with other agencies or in a support role rather than being in charge. Exercises help strengthen such relationships and clarify roles.

If properly done, exercises may also identify deficiencies in plans, training, and preparation. At least two or three times a year, exercises should involve the actual deployment of personnel for a particular task.

#### **6. Ensure Acquisitions are “Dual Use.”**

The “all-hazards” concept should be applied to equipment purchases and any other measures implemented to deal with terrorism, making sure that they are useful not just for terrorism response but for other incidents as well (“dual use”). Although terrorism is clearly a significant area of concern, there are many other major incidents that are likely to require a full-scale emergency government response. For most jurisdictions, sustaining interest in terrorism and terrorism prevention, may wane over time. It is essential, then, to get the most “bang for the buck.” For example, personal protective equipment for police officers often has more than one use; gas masks that have traditionally been purchased for riot control situations might also be used to protect against a biological or chemical threat. Acquisition of bomb response and detection equipment is an example of an opportunity to enhance day-to-day response to these incidents as well as terrorist threats.

#### **7. Isolate Fear Strategically.**

Managing fear in the community has been an integral part of the strategy of community policing. The police already think in terms of addressing community fear, and utilizing their experience in this area makes sense because community fear is very much a part of the problem with terrorism (as Chapter 2 by Robyn Pangi details). Local government must have an approach for dealing with fear that results from warnings, threats, and attacks. A well-thought-out public information strategy is an important piece of managing fear. It should be designed in concert with news media and others to keep citizens informed of issues connected to terrorism while minimizing the sensationalism that increases fear. The plan must involve the local news media but should not rely exclusively on that outlet to reach people in the community. Connecting with community and neighborhood leaders through e-mail, fax, the Internet, local government cable television channels, and the telephone (such as calling trees and reverse 911) are effective methods of transmitting unfiltered information. Of primary import, responders need to



create links between schools, students, and parents. Planned responses to school closures are critical to moderating the panic that may arise between the time when parents become aware of a problem and the time when they are able to ensure that their children are safe.

Fear by first responders and other employees involved in the prevention and response to terrorist acts must be given serious consideration in the planning process as well. Most are unfamiliar with the biological and chemical aspects of this new enemy that they are asked to face. Training and proper equipment are important aspects to minimizing and overcoming this fear. Ensuring they have plans in place to take care of their families while they are at work protecting and caring for others is a critical step. First responders must also have the confidence that they will receive the appropriate medications to protect them, and must have some advance understanding of the potential consequences of taking that medicine.

### **8. Apply Community Policing Skills.**

Community policing has taught the police the value of developing relationships with community stakeholders, and this lesson applies to the threat of terrorism as well. It is particularly important in situations such as those that occurred in the aftermath of 9/11, where both Jews and Muslims have been threatened and victimized. It is local police, much more than federal law enforcement, who can develop and maintain relationships with all groups that might be targets of terrorist acts or the backlash that may follow.

Over the decade, the police have become better at connecting with the community and working in a partnership to solve problems; they have learned a great deal about how to engage people in activities that deter criminal acts and decrease fear. These skills should be put to use in helping mobilize the community to undertake projects and initiate programs that will have the dual purpose of preparing for acts of terror while strengthening overall neighborhood safety.

The “Citizen Corps” is a program initiated by the federal government that needs to be explored more thoroughly in the context of dual-use or all-hazards planning. There are a numerous opportunities for community volunteers to make a difference in the day-to-day life of a neighborhood while assisting with preventing crime and enhancing the response

to terrorist incidents. A neighborhood watch, for example, could help with planning for an unexpected school closure by setting up safe locations for children in a church, a home, or a business; such locations could offer a short-term shelter for children until their parents can arrive to care for them. The volunteer handicapped patrol unit could be a communication link to the businesses in the area they patrol, or could develop and maintain contact lists for police and local government use. Volunteers that have regular assignments could be trained in a secondary responsibility for emergency conditions.

## CHAPTER 5 — Engaging the Private Sector

---

*Juliette N. Kayyem and Patricia E. Chang*

The federal government has devoted much time and resources towards fighting the war against terrorism since September 11. In doing so, the government has concentrated primarily on coordinating ways in which federal, state, and local government agencies will respond to a catastrophic event, largely ignoring the role of the private sector. By neglecting the private sector in its emergency planning, however, the government limits the number of potential security needs that its homeland defense initiatives can address.

Likewise, many businesses, while concerned with revamping their disaster-preparedness plans, have spent most of their energies on the recovery and maintenance of operations and systems after the attacks and readdressing business continuity plans. While business continuity is essential, there is an even greater need for an integrated public and private domestic preparedness strategy, one that views the private sector not merely as a profit-making entity, but as an entity that is responsible, just as the government is, for protecting life and ensuring security.

Although protecting human life is the most compelling reason to establish a joint public-private domestic preparedness plan, there are many other reasons for the government to engage the private sector in homeland security, and for the private sector to collaborate with the public sector.

Arguments that promote private sector engagement in domestic preparedness are compelling, yet integration has not yet occurred, in part because the private sector has not historically been a part of disaster planning. The responsibility has been given primarily to first responders at the state and local level, or to the Federal Emergency Management and to the Department of Justice at the federal level.<sup>1</sup> The stronger and more problematic reason is that significant barriers discourage security investment. Security is often viewed as a disadvantageous cost, instead of an investment with a sizable return in the form of preventing losses. In other words, security is not viewed as adding to one's "bottom line"

but rather as a “necessary evil.”<sup>2</sup> Consequently, even if standards for preparedness are the responsibility of the government and are federally mandated and developed, the costs for implementing or evaluating these practices still fall mainly on the private sector. Finally, substantial legal concerns—that businesses could face antitrust violations for sharing information with industry partners, that information could be subjected to Freedom of Information Act (FOIA) disclosures, or that companies could face liability concerns—exacerbate the problem and limit private-sector involvement. Companies are generally hesitant to shoulder additional risks. Thus, whereas more rhetorical attention is being paid to the lack of private-sector engagement in preparedness, substantial initiatives to address this problem are lacking or are only in early developmental stages.

In the years ahead, while government will increasingly rely on the private sector for support in protecting critical infrastructure and the homeland, many in the private sector will rely on the government to encourage safer networking and information-sharing in nonlegislative and nonregulatory ways. Thus, local and state governments should take active steps to foster a private-public approach to homeland security, and to encourage private-sector participation in domestic preparedness.

### **Recommendations**

1. Designate a Public-Private Commission
2. Issue Risk and Threat Assessments
3. Inventory Private Sector Commodities and Services
4. Build Public-Private Partnerships
5. Implement Policy Instruments
6. Document Best Practices

### **1. Designate a Public-Private Commission.**

The first task of local and state governments is to understand the problem fully before making recommendations and taking action. A public-private commission comprised of people who have worked on critical infrastructure protection, health officials from the

private and public areas (as Chapter 3 by Ralph Timperi details), business leaders, and government officials in each jurisdiction should examine the lack of private-sector integration in homeland security. Any recommendations made by this public-private commission should be framed in terms of establishing and maintaining private-sector involvement in domestic preparedness programs. Once the commission's policy recommendations are implemented, the public-private commission may evaluate shortfalls, note successes, and recommend necessary changes. As private and public entities learn to work together, they will be better able to discover the gaps in domestic preparedness, identify and share some of their best security, safety, and recovery practices, and work to standardize their emergency planning with government guidance.

## **2. Issue Risk and Threat Assessments.**

Public officials must take the lead in gathering, interpreting, and disseminating intelligence, in order to provide actionable guidance, that is, information regarding actions that the private sector might take. This process entails government assistance to the private sector in the form of risk and threat assessments. Without the benefits of a threat and risk assessment, many companies depend on worst-case scenarios to generate countermeasures for prevention. This means that the company, steered by a worst-case scenario, focuses on vulnerabilities (which are unlimited) rather than credible threats (which are limited).<sup>3</sup> Compared to worst-case scenarios, targeted threat and risk assessments provide better guidance on how to address threats and allocate resources, based on a more realistic assessment of how much preparedness is necessary. Government sharing of pertinent information may help the private sector to build its own responses more effectively, taking into account the costs and benefits of alternative plans of action.

## **3. Inventory Private Sector Commodities and Services.**

Making a comprehensive inventory of the contributions that the private sector supplies during all stages of crisis is important. For example, many essential services used in an emergency—communications, power, water, food, and medical services—are owned or operated by private businesses.<sup>4</sup> Should a weapons of mass destruction (WMD) attack

occur, private doctors, hospitals, and emergency technicians would treat most of the victims; pharmaceutical companies would supply stockpiles of the critical medicines and vaccines; manufacturers would supply necessary protective equipment and gear; banks and financial institutions would provide monetary support to the disaster site; privately owned communications systems would provide equipment and repair services; and privately owned universities, schools, hospitals, or other buildings might contribute space for triage and other support activities. Identifying private sector commodities and services will raise awareness of resource capabilities and weaknesses within a jurisdiction. This awareness will also benefit regional coordination and mutual aid agreements, so that resources can be deployed more efficiently across a region during a crisis (as Chapter 6 by Arnold M. Howitt details).

#### **4. Build Public-Private Partnerships.**

Public-private partnerships cannot be built without first establishing trust through working relationships. Government can facilitate these relationships by approaching institutions such as the chamber of commerce in cities and localities, and identifying opportunities for collaboration with them. Low-key approaches from first responders, rather than public officials, are most likely to elicit cooperation from the business sector.<sup>5</sup> Building public-private partnerships also requires the involvement of local governments. Most of the operational issues of collaboration between the private and public sectors are best settled at the local level, especially when the private sector has a single government authority to deal with.

#### **5. Implement Policy Instruments.**

Local and state governments possess a variety of policy instruments such as regulations, tax incentives, regional coordination, and various partnerships that could be used to encourage or require private-sector entities to take actions when addressing security concerns. The methods for engaging the private sector may be regulatory (mandated security standards for the private sector), reward-based (providing incentives to the private sector for investing in security), or simply the removal of barriers to investment in security improvements. Because the regulatory approach may be too heavy-handed and

the reward approach too costly, removing barriers to security investment is the most appropriate action.<sup>6</sup> Removing barriers to security investment might include providing Freedom of Information Act exemptions to specific companies.<sup>7</sup> Narrow antitrust exemptions offer another technique; an example is the Information and Readiness Disclosure Act passed by the 105<sup>th</sup> Congress, which created an anti-trust exemption for information sharing for the purposes of Y2K preparedness.

## **6. Document Best Practices.**

Lead local agencies should develop a best-practices model for the private sector that enables more accurate assessments of risk, vulnerability, and survivability. Such a model would allow industry to address its security needs according to a set of performance standards, as opposed to government specifications. The Defense Department's internal assessment program may serve as a guide in developing best practices. In addition, the Department of Justice Office for Domestic Preparedness and the Federal Bureau of Investigation have worked together to provide state and local governments with a risk and threat assessment tool. Documenting which methodologies have been more or less successful in assessing threats, risks, and requirements and capturing "lessons learned" would aid companies that are just beginning to formulate security plans.

## CHAPTER 6 — Promoting Regional Collaboration

---

*Arnold M. Howitt*

Improving preparedness for terrorism is an expensive, time-consuming, and exacting task. Even large cities may lack sufficient resources to prepare for a huge surge of demand for emergency services. For many smaller localities and organizations, starting from a lower base of emergency management capability and often lacking adequate fiscal and management resources, effective preparedness is infeasible. It would be wasteful, moreover, to replicate capabilities in every community, especially highly specialized equipment and training, since many are likely never to use them. Thus there is a large potential for gains from regional partnerships to prepare for terrorism and other emergencies.

Although regional cooperation can sometimes be improvised in the moment of a disaster, it is more effective to place structures for collaboration in place in advance of dire need. But individual jurisdictions are often unable or unwilling to collaborate for several reasons. First, there is a geographic mismatch between the scale of the problem and the scope of the government institutions that must deal with it. The impact of a terrorist attack with weapons of mass destruction could well extend over a broad metropolitan or interstate area, potentially involving dozens or hundreds of local governments and several states. The American government, however, lacks strong decision-making structures that connect diverse localities or that reach across state borders.

Second, institutional complexity also makes cooperation difficult. Within each jurisdiction, there are numerous agencies and professional groups — for example, police, firefighters, emergency physicians, emergency medical technicians, epidemiologists, and emergency managers — who are potentially involved in response to disasters. Each has its own regular responsibilities and operating methods. They do not work day-to-day even with some agencies or professional groups in their own jurisdictions, let alone across borders. Some agencies jealously guard institutional turf.



Finally, collaboration generates costs that may be difficult for individual government units or firms to pay. They face competing priorities, and some worry that they may be criticized for not paying exclusive attention to their own jurisdiction's needs. Varied accountability relationships — to different stakeholders and officials — add layers of complication. Some small entities may be unwilling to pay, creating a free-rider problem.

State or federal regulatory requirements or mandates are not likely to be as effective in spurring collaboration as will be voluntary commitments. Generating regional cooperation is difficult, but strategies to provide leadership, create benefits and lower costs, and find workable governance methods hold promise for increasing levels of effective collaboration.

### **Recommendations**

1. Policy Entrepreneurs Step Forward
2. Seize the Moment
3. Create Benefits to Cooperation
4. Reduce the Risks of Partnering
5. Begin Small, Work Big Later
6. Carry the Weight

### **1. Policy Entrepreneurs Step Forward.**

One or more “policy entrepreneurs” are needed to promote collaboration, just as new business formation requires entrepreneurial energy. A policy entrepreneur needs a sharp vision of the potential gain from cooperation — in this case, not to profit, but to promote more effective government and private-sector preparedness for emergency response. He or she must be willing to commit scarce resources (time, funds, influence) and be able to use them skillfully to achieve that gain. Significantly, policy entrepreneurs do not have to be senior government leaders. Although they may come from high levels of government, they may also come from middle management or staff positions or from outside of government altogether. In Los Angeles, for example, a key leadership role in securing

greater cooperation among police organizations was played by a police sergeant. In the greater Washington area, business leaders, working with the regional Council of Governments, took the initiative in improving regional plans.

## **2. Seize the Moment.**

Opportunities for overcoming the barriers to cooperation are greatest when public and government attention is focused on the need for more effective emergency prevention and response, as occurred in the aftermath of the September 11 attacks. These moments make decision makers and their organizations acutely aware of the risks from terrorism or other disasters and make clear the shortcomings of existing levels of government and private company preparedness. They increase the perceived value of cooperation by highlighting the importance of operational continuity and the responsibility to protect people, property, and — for businesses — other assets and reputation (as Chapter 5 by Juliette Kayyem and Patricia Chang details). The chance to capitalize on such opportunities dissipates relatively quickly, however, as other pressing issues inevitably claim the attention and priority of senior public and business officials.

## **3. Create Benefits to Cooperation.**

Successful efforts to foster cooperation should not only achieve common goals but also create specific benefits for individual “partners.” Benefits for individual jurisdictions, such as equipment or training grants, can motivate potential partners in return for their commitment to cooperative relationships. Timely, focused information sharing, for example, can be a major incentive for cooperation. If it is specific by sector or industry and geographically focused, it is more valuable to those who receive it, and increases the incentive for cooperation. Furthermore, opportunities to lower the costs of providing security or emergency response capability are attractive incentives for collaboration. Equipment sharing and mutual aid arrangements among jurisdictions, for example, reduce the need for each partner to procure specialized gear or to provide for peak needs. Providing even modest financial subsidies for cooperation in the form of grants from federal or state governments can make it easier to achieve collaboration.

#### **4. Reduce the Risks of Partnering.**

Reducing the costs and risks of cooperation increases the willingness of potential partners to collaborate. For example, transaction costs — the hassle of repeatedly making agreements — can impede cooperation. Developing standard mutual aid agreements and communication systems that make it easier to work together and reach decisions can reduce transaction costs. Jurisdictions may also be reluctant to cooperate because of perceived risks from collaboration, such as damage to equipment, injuries to personnel, or liability for actions taken while aiding a partner. These can be reduced by state legislation to provide insurance against loss or to protect jurisdictions from liability claims.

#### **5. Begin Small, Work Big Later.**

Developing regional collaboration structures requires thoughtfully addressing governance issues, but this may require prior development of trust among the potential partners. Ad hoc accomplishments may be necessary first steps to more extensive cooperation. As initial interactions produce results, the development of trust among collaborating jurisdictions can allay mutual suspicions that partnership is a means of exploitation.

#### **6. Carry the Weight.**

To make cooperation feasible, large communities or counties must be prepared to make some accommodations to small communities. Large jurisdictions may have to accept governance arrangements that give reassurance to jurisdictions concerned that their independence is at stake. Small jurisdictions, moreover, may lack sufficient means to contribute their share of financial resources. The benefits of effective collaboration among the larger jurisdictions may make these accommodations to smaller entities acceptable.

## CHAPTER 7 — The “Local” Military

---

*Major General Philip Oates*

The attacks on our homeland that occurred on September 11, 2001, have generated many initiatives to improve domestic preparedness for homeland security against major acts of terrorism. The first ever National Strategy for Homeland Security was approved and released by the president in July 2002. Congress is currently deliberating legislation that is likely to generate the most significant reorganization of the federal government of the last fifty years. A new emergency management paradigm is evolving because the threat of terrorism is now seen by many as a major hazard and a reason to revise planning.

A tremendous change is also occurring within the military. Indeed, because of September 11, many argue for a greater use of military capabilities and procedures to improve domestic preparedness. Although the Department of Defense will not be designated the lead federal agency in most homeland security contingencies and scenarios, it has many processes and procedures that could be helpful to the federal efforts to identify, generate, and develop the overarching requirements and programs for homeland security. In homeland security scenarios, however, the military will normally perform a supporting role, providing assistance to civil authorities and lead federal agencies.

While there may be a tendency to view the military as simply a federal role, it is important not to overlook the significant contributions of the National Guard to other agencies during this period of transformation. Indeed, instead of simply looking to Washington for the kinds of military support imagined for domestic preparedness, state capabilities and capacities might prove sufficient.

### **Recommendations**

1. Focus on the National Guard
2. Enhance Civil Support Teams
3. Learn from the “War on Drugs”

#### **1. Focus on the National Guard.**

Predominant use of the National Guard for homeland security against major acts of terrorism is appropriate for three key reasons. First, the National Guard already has a significant emergency response capability that would provide a firm foundation for a larger role in homeland security. Local units, familiar with geography and locale, will best serve a community’s needs. Second, while there has been much discussion about the legal impediments to utilizing the military in the domestic arena, the National Guard can provide significant assistance and authority during a crisis. Statutes and case law establish the authority to employ the National Guard in significant and leading domestic roles against terrorism. Third, because active-duty forces provide our nation’s leading military resources for rapid deployment and expeditionary warfare, these forces are less available as a contingency force for domestic missions and might be completely unavailable in the event of a major overseas deployment. We risk overextending ourselves if we overlook the tremendous benefits of the National Guard.

#### **2. Enhance Civil Support Teams.**

A new capability that has already come to the National Guard in many states is called the Civil Support Team. It offers significant and deployable capabilities to assess, identify, and detect chemical, biological, radiological, nuclear, and high explosive agents rapidly. The team includes individuals capable of providing expert advice to government and military officials and first responders about the response to and management of a weapons of mass destruction event. The team also has robust capabilities to provide voice and digital communications. Although these teams are relatively new, they are already

providing significant capabilities that are improving domestic preparedness. Their capabilities and funding should be increased.

### **3. Learn from the “War on Drugs.”**

Further improvement of homeland security capabilities in the National Guard could be achieved by establishing a homeland security support program similar to that found in the National Guard Counter-Drug Support Program (CDSP). That program provides an apt model for a small full-time organization that could significantly improve interagency capabilities for homeland security. As seen in the CDSP, such organizations could do this by providing National Guard resources and manpower to other “homeland security” agencies on a continuous basis. (For further reference see Jonathan P. Caulkins et al, “Lessons of the ‘War’ on Drugs for the ‘War’ on Terrorism,” [www.esdp.org](http://www.esdp.org))

The CDSP, established by Congress in 1989, has had continuous funding since then through annual appropriations to the National Guard Bureau. This budget provides pay and allowances for full-time personnel and for the operations and maintenance costs of the military equipment and other resources used to support drug law enforcement agencies in drug demand reduction and counter-drug support operations. National Guard resources are made available to states to be used by agencies at all levels of government to achieve those missions (within the constraints of the annual budget and under a federally approved governor’s plan).

A similar approach might produce improvements to agency cooperation, interoperability, and communications in the areas of preventing and responding to major acts of terrorism. A “National Guard Homeland Security Support Program” could provide daily coordination, integration, and assistance between agencies such as the Federal Bureau of Investigation (FBI) and the Federal Emergency Management Agency (FEMA). National Guard resources could be made available to manage flows of information and intelligence, while improving all players’ abilities to plan, train, exercise, and operate together. Law enforcement roles would be possible for these forces within the constraints of a federally approved governor’s plan.

## CHAPTER 8 — Utilizing the Mass Media

---

*Peter Van D. Emerson*

Like it or not, media outlets are the most reliable and productive way for first responders to communicate to a public that may be traumatized and scared in the midst of a terrorist attack. While the First Amendment and the sanctity of an independent press generally protect the media from regulation, many voluntary efforts between first responders and the media have gone underutilized. After all, the media is just as likely to become victims as anyone else in the community (maybe more so, as was seen in the anthrax attacks). In a highly competitive and global world with 24/7 news cycles and myriad sources of information available, including the Internet, it is imperative that local and state governments and local, state, and national media organizations begin intensive discussions about their particular needs and expectations of one another, about how to educate the public and themselves about potential threats and possible future attacks, and about negotiating mutual assistance agreements. All of this will ultimately save lives. The media need not become a tool of terrorism, by inadvertently spreading misinformation and escalating panic. Instead, state and local governments should learn to look at the mass media as partners in responding effectively to an attack.

### **Recommendations**

1. Utilize the Press as a Dual Use Resource
2. Prioritize First-Responder Media Training
3. Feed the Media What They Need
4. Protect Journalists
5. Ensure Viable Communications

### **1. Utilize the Press as a Dual Use Resource.**

As domestic preparedness planners begin to integrate the private sector in planning and preparation exercises, these efforts should include representatives of the senior management of media companies, many of which are businesses with considerable technical and logistical resources. From helicopters to sophisticated mobile telecommunications systems to Internet interconnectivity, as well as real estate that could be used for many purposes, including shelters, staging areas, and vantage points, media organizations have an inventory of resources that should be added to a community's pre-incident planning strategies. They also have technical expertise that could prove invaluable.

### **2. Prioritize First-Responder Media Training.**

An education program should be initiated for all senior local and state officials, including senior first responders, to teach them about the needs and constraints of the media. Too often, the "sound bites" come from political appointees who may know little about the substance of an issue. There were mis-steps, for example, when a series of Cabinet officials began to discuss the intricacies of anthrax, but the information they provided to the media was faulty. Existing relationships should be expanded and strengthened, and, more specifically, first responders must understand how the situation changes once national and international media arrive. Planning for reporters who are strangers to the community must occur. For example, too often the location of the press briefing center is distant from the actual incident site, thus requiring a reporter to decide whether to stay at the site or go to the briefing. In the first few hours of an event, most media outlets will not have two satellite trucks to cover both. If there are no serious threats to the welfare of participants or the rescue efforts, moving the press briefing closer to the incident site might facilitate both reporting and control over the story.

### **3. Feed the Media What They Need.**

Local governments should prepare comprehensive press briefing kits in anticipation of the next terrorist attack. The information must be consistent and simple, with names and contact information of local and national experts from whom the media can seek advice.



Most news agencies have in-house experts on a variety of topics, and similar steps should be taken to designate someone within the media organization to become familiar with nuclear, biological, and chemical agents as well as other potential threats. A media outlet would then have an in-house source to turn to for basic guidance and information.

#### **4. Protect Journalists.**

The sense of security felt by members of the mass media themselves will have a tremendous impact on the public's sense of safety. The anthrax attacks were so successful, in part, because the targeting of media outlets had an amplifying effect, as the news tended to magnify the risk. There is an immediate need for media companies to provide their reporters, producers, and field staff with training in hostile and hazardous environments, as is often done when reporters are sent to cover armed hostilities. For example, when a helicopter from a television station flies through a chlorine gas cloud, even as the station is broadcasting warnings to clear the area because of the chlorine, this provides a message to the public that is confusing, at best, and threatens the safety of the reporters. There must be a better understanding by the media of what is and is not harmful.

#### **5. Ensure Viable Communications.**

Most cities lack the extraordinary communications and broadcast capabilities of New York City, and in an attack situation could find themselves without adequate means to get information to the public. In order to ensure that reporters can get through, there has to be an investment in communications systems that can handle the massive load that a crisis would impose. Local officials and local media technical personnel should review existing telephone and broadcast systems and make recommendations about what new equipment is required to keep both the media and government officials connected in a crisis, and to stream accurate and timely information to the public.

## CHAPTER 9 — Sustaining Preparedness

---

David Grannis

Domestic preparedness—the subset of homeland security activities focused on preparing and responding to terrorist attack—encompasses efforts from numerous federal government departments and agencies, state and local government and responder group efforts, and relationships with the general public and private sector. Prior to 9/11, piecemeal domestic preparedness initiatives at the federal, state, and local levels were frequently threatened by budget cuts and competing priorities. The aircraft and anthrax attacks last fall drastically focused massive attention on all aspects of homeland security. The programs remain, however, vulnerable to an array of sustainment challenges that can be grouped into two broad categories.

The first issue is one of *operational readiness*: the ability of the responders to react to a given threat quickly and efficiently, in a manner that has been planned and rehearsed. Operational readiness requires that new personnel be trained and that all personnel keep up with best practices and new policies. It also requires conducting exercises to test and practice domestic preparedness skills, and procuring, distributing, and maintaining equipment in good working order. Sustainment is likely to be a more pressing concern when practitioners are not dedicated specifically to weapons of mass destruction (WMD) response, which makes operational sustainment a bigger issue for local responders than federal.

The second consideration is *program sustainment*: maintaining adequate funding and effective management of preparedness programs and keeping domestic preparedness as a policy priority. While local funding for domestic preparedness is crucial, because it is local communities that provide the response capabilities, program sustainment generally requires federal support. State and local governments and agencies look to the federal government for funding and development of specialized equipment. Like operational sustainment, program sustainment is subject to changing forces such as the availability

and willingness to spend government funds, and the introduction of other issues that divert the attention of policymakers.

There are several challenges that apply to both operational and programmatic sustainment. The first challenge is that programs will succumb to the tension between federal and local responsibilities. The local personnel who respond daily to injury, illness, and everyday hazards—who are not devoted exclusively to domestic preparedness—are also the first responders in a WMD event. The federal government faces the greatest likelihood of dealing with a WMD attack, simply because it confronts the risk across the entire country, but it relies on local responders to take the responsibility for initial handling of an event. Benefits from investing both funds and time in domestic preparedness accrue at the local level, such as improved public health monitoring and joint training of law enforcement and emergency response personnel. The federal government may perceive that local agencies that are benefiting from the training should also bear responsibility for funding the training. Local governments, however, have competing priorities and often severely limited budgets. As a result, federal and local governments each view the other as having primary responsibility for domestic preparedness, and the total support needed from each level is threatened.

The second potential pitfall is referred to as “boom or bust prioritization” – the windfall of funding and programmatic initiatives dedicated to domestic preparedness in the wake of an attack that may fall by the wayside if there are not additional terrorist attacks or significant homeland security threats in the next couple of years. Lawmakers and first responders may turn away from domestic preparedness and focus on other needs. The huge increases in expected funding at the federal, state, and local levels make domestic preparedness a target for future budget cuts. Critics of past domestic preparedness efforts have pointed to the unwillingness to sustain attention to terrorism, even after the 1993 World Trade Center bombing, the 1995 Oklahoma City attack, and the 1998 embassy bombings. Funding at the state level is especially precarious, as many states are undergoing budget shortfalls and are prevented by law from running operating deficits. This scenario is less probable, however, both because budgetary inertia tends to favor existing spending levels, and because further attacks are, unfortunately, very likely.

The third potential pitfall is setting the wrong priorities: focusing on visible security issues at the expense of more complex but less visible organizational and strategic issues. The sudden attention to homeland security has created a need to take steps to reduce the vulnerability to terrorist attack and improve response capabilities. This is true for elected officials wishing to appear strong on security, for businesses seeking to minimize losses from a threatened consumer base, and for those that provide security — first responders and others — to show that they are able to defeat terrorist plots. With so much focus on domestic preparedness and terrorism prevention, there is a push to devote resources exclusively to security. This push is largely based not on expertise, as the experience with domestic preparedness before 9/11 proved insufficient to guide policymakers and security providers, but rather is driven by the perceived need. Domestic preparedness may take the wrong direction, in effect preparing to counter the last attack rather than future threats. Planning and guidance are therefore necessary for program and operational sustainment for domestic preparedness.

#### **Recommendations**

1. Designate a Lead Government Entity
2. Monitor for Readiness
3. Minimize Terrorism Specialties
4. Institutionalize Domestic Preparedness

#### **1. Designate a Lead Government Entity.**

Designating an organizational home for domestic preparedness issues and an entrenched organizational bureaucracy to fight for those interests is a first step to ensuring sustainability. Establishing a Department of Homeland Security would be a positive step towards a federal nexus for domestic preparedness, but it will not entirely solve many of the local and state needs on the operational level. A Department would be an institutional force for the continued funding and priority of domestic preparedness, overcoming sustainability problems inherent in keeping domestic preparedness control in other departments with conflicting funding needs. The same will likely be true on the state and

local level as well. Many states have adopted “czars” to address homeland security, but without authority over personnel and budgets, they will continue to lack true power.

## **2. Monitor for Readiness.**

It is difficult to monitor and measure operational readiness to respond to emergencies. The federal government should work with states, cities, and first-responder groups to develop metrics for measuring operational readiness, as has occurred to some extent for the Institutes of Health with medical readiness. This will require identifying desired response capabilities and making a judgment of who should be capable of performing what tasks. Federal, state, and local response units should be judged against the developed metrics, as should federal offices providing training or equipment.<sup>1</sup> Once objective measurements are implemented, more attention can be devoted to setting standards for how skills and equipment are improved or maintained and what changes to current procedures are necessary to sustain the desired level of preparedness.

Simulation exercises are critical for training and for measuring readiness. While large-scale federal exercises should be continued annually, smaller exercises at the state, county, or city level should be run periodically to test readiness and identify shortcomings in preparation. Provisions should be made to disseminate lessons learned from all exercises to responders and planners in other geographic areas.

## **3. Minimize Terrorism Specialties.**

The structure and goals of the domestic preparedness have great importance for the effort’s sustainability. The goal of the programs should be to maximize the ability to prepare for and respond to a range of attacks or emergencies on U.S. territory to minimize detrimental impacts. For this goal to be realized in a sustained manner, local responders must be prepared to follow exacting procedures for extremely unlikely eventualities without degrading their daily operations. This implies a tradeoff between attention to specialization and maximum readiness with attention to more commonplace needs. Domestic preparedness should thus be thought of as part of the existing “all-hazards” approach to disaster management rather than a separate entity; to the maximum

extent possible, domestic preparedness capabilities should be developed in ways that benefit other responsibilities.

#### **4. Institutionalize Domestic Preparedness.**

To the extent possible, domestic preparedness should become institutionalized or automated within the participating communities. Creating protocols or automated tasks that increase response effectiveness will decrease the chance that sustainment will fail. Some of these protocols will require the responder community to change standard procedures, such as requiring that extra protective clothing be worn or WMD detectors be brought to deployment sites. Other protocols, such as notifying specific officials if there is a high level of hospital admits or unusual veterinary activity, may be automated through computer protocols triggered by data entry. To the extent that technologies can be used independent of human activity (for example, detectors placed in strategic sites to monitor WMD and relay results to a central facility), automation can replace training or attention without risking sustainability.

Additionally, WMD response should be made part of the training that firefighters, police, HazMat (hazardous materials) workers, public health personnel, doctors, and nurses are required to complete before employment. While this instruction is conducted locally and is sometimes private, federal legislation should mandate that standards for training be set by the relevant federal agencies, and that training academies be trained directly by the federal experts.<sup>2</sup>

## Conclusion

---

Although any future federal Department of Homeland Security (DHS) will have overarching responsibility for homeland security, successful domestic preparedness against terrorism with weapons of mass destruction will require integration and coordination of efforts across a complex interagency environment that includes all levels of government, public agencies, private organizations, educational institutions, and businesses. As this major change in government evolves, it will become increasingly important, yet increasingly difficult, to integrate and coordinate training, assessments, experimentation, analyses, demonstrations, modeling, and simulations to develop the best possible technology, techniques, procedures, and requirements for homeland security.

What we do know, however, is that a new Department is not the end of the discussion. DHS is merely one patch on a very complicated quilt that, in some places, is quite complete, but in others still has many voids to fill. A concerted and sustained effort that continues to focus on local responders, and on how they can best protect Americans, is an essential part of this difficult process.

## Endnotes

---

### CHAPTER 1: The “Two-Hat Syndrome:” Determining Response Capabilities and Mutual Aid Limitations (*Rebecca F. Denlinger with Kristin Gonzenbach*)

1. Two-Hat Project Survey, Cobb County (Georgia) Fire and Emergency Services, June 2002.
2. Ed Plaughter, Fire Chief, Arlington County, Virginia, telephone interview, May 13, 2002.

### CHAPTER 2: After the Attack: The Psychological Consequences of Terrorism (*Robyn Pangi*)

1. Mark J. Morgan and Paul M. Camper, “Fear Management,” April 1, 1998, unpublished manuscript, p. 1. (Manuscript available from the authors.)

### CHAPTER 4: The Policing Challenge (*Darrel W. Stephens and Francis X. Hartmann*)

1. Hank Christen, Paul Maniscalco, Alan Vickery, and Frances Winslow. “An Overview of Incident Management Systems,” *Perspectives on Preparedness*, No. 4 (September 2001) at <ksgnotes1.harvard.edu/BCSIA/Library.nsf/pubs/POP4>.

### CHAPTER 5: Engaging the Private Sector (*Juliette N. Kayyem and Patricia E. Chang*)

1. Crisis management involves activities that preclude a terrorist attack: efforts to prevent and deter a terrorist attack, protect public health and safety, arrest terrorists, and gather evidence for criminal prosecution. Consequence management takes place after a terrorist incident, and includes efforts to provide medical treatment and emergency services, to evacuate people from dangerous areas, and to restore government services. GAO Report to Congressional Committees, “Combating Terrorism: Selected Challenges and Related Recommendations,” GAO-01-822 (September 2001), p. 5.
2. Maureen Tkacik, “Workplace Security (A Special Report): Ready Response: Plenty of companies are aiming to cash in on the security business, but so far it’s no bonanza,” *The Wall Street Journal* (March 11, 2002), p. R12.
3. GAO Report to Congressional Committees, “Combating Terrorism: Selected Challenges and Related Recommendations,” p. 45.
4. The private sector also is a producer of innovative technology, medicines, services, and products that help combat terrorism. Many private companies, for instance, work as subcontractors to government agencies or as outsources of critical functions in an emergency.



5. This idea was offered by Marshall Carter, John F. Kennedy School of Government, during the Executive Session on Domestic Preparedness session of June 2002.
6. The regulatory approach, for instance, largely places the burden of paying for security on private entities, whereas the “reward” approach may require the federal government to utilize tax incentives to private entities, which may be costly and thus difficult to implement in a period of economic decline.
7. FOIA makes the following records exempt from disclosure: 1. information vital to national defense; 2. information related to solely internal personnel rules and practices; 3. information specifically exempted from disclosure by statute; 4. information that is a trade secret; 5. information contained in inter-or intra-agency memorandums or letters that would not be available by law; 6. information that violates confidentiality of personnel and medical files; 7. information compiled for law enforcement purposes. See [www.federalreserve.gov/generalinfo/foia/exemptions.cfm](http://www.federalreserve.gov/generalinfo/foia/exemptions.cfm).

## CHAPTER 9: Sustaining Preparedness (*David Grannis*)

1. Measuring requires some entity to judge. Assessments might be made by private or non-profit institutions, state governors offices, or federal organizations such as the Government Accounting Office or the Office of Management and Budget.
2. Amy Smithson and Leslie-Anne Levy, *The Chemical and Biological Threat and the U.S. Response* (Washington, D.C.: Henry L. Stimson Center, October 2000), pp. 298–303.