Winning Plays:
Essential Guidance from the Terrorism Line of Scrimmage

Peter S. Beering, Paul M. Maniscalco, Hank Christen,
Steven B. Storment, and A.D. Vickery

ESDP-2002-02
BCSIA-2002-6 **February 2002**

Citation and Reproduction

This document appears as Discussion Paper 2002-6 of the Belfer Center for Science and International Affairs and as contribution ESDP-2002-02 of the Executive Session on Domestic Preparedness, a joint project of the Belfer Center and the Taubman Center for State and Local Government. Comments are welcome and may be directed to the authors in care of the Executive Session on Domestic Session.

This paper may be cited as Peter S. Beering, et al. "Winning Plays: Essential Guidance from the Terrorism Line of Scrimmage." BCSIA Discussion Paper 2002-6, ESDP Discussion Paper ESDP-2002-02, John F. Kennedy School of Government, Harvard University, February 2002.

About the Authors

Peter S. Beering, J.D., CFI, EMT/D, is Indianapolis Terrorism Preparedness Coordinator. Paul M. Maniscalco, MPA, Ph.D. (c), EMT/P, is Adjunct Assistant Professor, The George Washington University School of Medicine and Health Sciences and Deputy Chief, Emergency Medical Services Command, New York City. Hank Christen, MPA, EMT/D, is Emergency Response Consultant, Unconventional Concepts, Inc. Steven B. Storment, EMT/P, is Assistant Fire Chief, Phoenix Fire Department. A. D. Vickery, EMT/D, is Deputy Chief, Special Operations, Seattle Fire Department. All are members of the Executive Session on Domestic Preparedness.

Contributions to this paper were also made by Steven G. Vogt and Executive Session members Leslee Stein-Spencer, RN, MS, Darrel Stephens, MPA, and Frances Winslow, Ph.D.

Dedication

We dedicate this to our friend and colleague, Jack Fanning, who died as he lived, in the service of others, on September 11, 2001.

The views expressed in this paper are those of the authors and do not necessarily reflect those of the Belfer Center for Science and International Affairs, Taubman Center for State and Local Government, Executive Session on Domestic Preparedness, or Harvard University. Reproduction of this paper is not permitted without permission of the Executive Session on Domestic Preparedness. To order copies of the paper or to request permission for reproduction, please contact Rebecca Storo, John F. Kennedy School of Government, Harvard University, 79 John F. Kennedy Street, Cambridge, MA 02138, phone (617) 495-1410, fax (617) 496-7024, or email esdp@ksg.harvard.edu.

The Executive Session on Domestic Preparedness is supported by Grant No. 1999-MU-CX-0008 awarded by the Office for State and Local Domestic Preparedness Support, 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 and 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 author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

INTRODUCTION

This paper provides recommendations for the "play book" used by policy makers and emergency preparedness practitioners in assembling the elements necessary to effectively plan for and respond to terrorist actions by developing critical relationships, building systems, and setting training and funding priorities. It is not intended to be a model plan but to offer practical guidance, based on our expertise, for planning effectively, spending wisely, and making our nation safer. This document is divided into sections by subject matter, with a brief overview for that particular section followed by a series of recommendations.

The athletic field provides many useful analogies for emergency planning and response. Winning teams practice various "plays," develop and rehearse "game plans" before game day, and do extensive research about their opponents. Legendary Coach John Wooden's somber reminder that, "failure to prepare is preparing to fail" applies to the daunting challenge of preparing for terrorist attacks. Terrorist opponents have an almost limitless arsenal of plays, techniques, and players to use in the contest, some even willing to sacrifice themselves in the process. Because terrorists strike without particular warning, and because our nation is so geographically large, with a myriad of appealing targets, we remain vulnerable to attack. When we are attacked, our "game day," the response must be immediate, competent, coordinated, sustainable, and effective if we are to prevent or minimize the loss of life and property that can result.

Unlike more conventional emergencies where there is often opportunity to consider options, terrorism response decisions must be executed very quickly to prevent additional harm. We must develop, practice, and refine our "plays" before they are needed. We must know our own strengths and weaknesses, and appreciate those of our opponents. We must develop core capabilities, skills, and knowledge. We must learn from past contests, but must remain mindful that the opponent in the next contest will probably execute different plays, using different techniques.

ABOUT THE AUTHORS

We may be people you have never seen, have never met, and of whom you have never heard. We are a few of the people who toil silently on the "sidelines" of emergency preparedness. We are not academics viewing the contest from the grandstands (although we have contributed to academic works on the subject); we are the coaches and players on the fields of emergency response. We have assessed the risks, written the plans, and managed the responses to catastrophes large and small. We have planned for and responded to contingencies that the participants and fans never knew were taking place at major special and sporting events. We have worked with airport directors and pilots, farmers and food processors, veterinarians and cattlemen, hospital directors and doctors, judges and lawyers, businessmen and their mail room employees, the managers of sports venues and the players who compete there. We have trained the heads of nations, states, cities, and corporations, as well as the new found heroes on the front lines, about risks and potential responses to those risks. We have responded to airline crashes, explosions, terrorist attacks, fires, floods, hazardous materials incidents, tornados, and criminal acts. When the emergencies were over, we investigated them, prosecuted the perpetrators, and derived lessons to help others. We have traveled the nation and the world for many years to spread the message of preparedness.

ABOUT THIS PROJECT

When September 11 came, the United States realized it was vulnerable to covert attacks. We already knew that. We warned national, state, and local officials about the risks, but were often ignored. We began our study of terrorism many years ago. To many observers, our work was anomalous, unlikely, and

irrelevant. As we studied the subject, we realized that there were simple, inexpensive steps that organizations could take to be better prepared for *all* emergencies. We have dealt with victims of tragedies and comforted those they left behind. Many of the victims of the attacks September 11 were our colleagues and friends. Our recommendations about public policy are based on our experience, expertise, and analysis. We offer these recommendations in the hope that they will prevent those catastrophes that can be prevented and minimize the impact of those that cannot.

PLANNING IS CRITICAL

A review of prior terrorist acts, major special events, and major antiterrorism exercises reveals the importance of planning. Emergency plans exist in a number of different forms, some very formal, some very informal. Emergency plans have the following critical components:

1. An identification of the threats.
2. An assessment of the vulnerability to those threats.
3. A determination of what resources are available to address the threats (before and after an incident).
4. Response plans for actual incidents.
5. Recovery and restoration of normalcy after an incident.
6. Investigation of the incident.
7. Establishment of an evaluation process to determine the effectiveness of emergency plans through a structured post-incident analysis.

Experience has shown that emergency plans need not be particularly formal to be effective. The effectiveness of such plans is related to familiarity with them possessed by those who must carry them out, relationships among plan participants, and the amount of practice officials have had with the plans. Planning is therefore more a process than a product. An effective planning process identifies potential targets and risks--vulnerabilities to various forms of attack--and allows these targets to be hardened and risks to be mitigated. It also allows for modifications and amendments to protocol and operational doctrine based upon performance evaluation findings. This cycle must be encouraged and preserved to provide the most contemporary and safe operating procedures.

We recommend that:

- Each jurisdiction review, rehearse, and revise its emergency plans.
- Representatives of the response agencies, human service providers, hospitals, and key private-sector community organizations meet to share ideas and coordinate resource acquisition and emergency communication.

PREPAREDNESS "EVANGELISM"

The most successful jurisdictions have a "preparedness evangelist" who typically takes responsibility for emergency planning and then spreads enthusiasm for contingency planning throughout the jurisdiction. Such evangelists occasionally are appointed, but more commonly they develop informally. The most successful of these evangelists have direct access and support to senior policy and decision makers and have budget authority over planning and response matters.

We recommend that:

- Each jurisdiction appoint and support a "preparedness evangelist" with full public and financial resources.
- This "evangelist" be vested with necessary authority via executive order or legislation to be effective.

INCIDENT MANAGEMENT/COMMAND

The greatest success in addressing terrorist (and other) emergency incidents has been achieved through the employment of some incident management system. Incident management systems facilitate the orderly application of resources to various problems and challenges. These systems also facilitate necessary documentation that is important for investigation and recovery after the incident is stabilized.

There are a wide variety of incident management systems in use throughout the United States. Some operate by statute, others by custom, still others by industry. A variety of systems exist , tailored for different industries and organizations. Their component parts are similar, although there are some differences in nomenclature. As with planning, regular use of the system is critical to its success during an emergency.[1]

We recommend that:

- Each jurisdiction adopt a systemic incident management system.
- The incident management system be fully implemented across disciplines, including hospitals and health care, and that it be employed routinely to address daily incidents and events so that it will be familiar to system participants for effective utility at a major incident.

RELATIONSHIPS

Among the key factors that yield success in managing emergencies are the relationships developed *before* the emergency among those who will respond. Informal relationships have repeatedly bridged operational, technical, legal, and other impediments to successful response to various incidents.

We recommend that:

- Each jurisdiction develop and maintain relationships with and among those persons, agencies, and organizations that may be called upon to respond to a major emergency. This recommendation extends past intrajurisdictional boundaries and embraces local, state, federal, and non governmental organizations that may be called upon to respond in times of high-impact/high-yield events.
- These relationships be formalized where appropriate.

[1] For more information see Hank Christen, Paul Maniscalco, Alan Vickery, and Frances Winslow, "An Overview of Incident Management Systems." BCSIA Discussion Paper, ESDP Discussion Paper no. ESDP-2001-04, John F. Kennedy School of Government, Harvard University, September 2001.

EDUCATION

Critical to effective response capacity are the knowledge and skill sets required to implement emergency operations expeditiously and safely. This is particularly true when confronting weapons of mass injury. Education of emergency responders (across various discipline lines), political leaders, lawmakers, the media, and the public is a multidimensional task requiring coordination to ensure favorable outcomes. The greater the knowledge base, the greater the sophistication of the systemic response, and the greater the likelihood of favorable outcomes will be.

We recommend that:

- Each jurisdiction incorporate emergency planning and response training into new-hire and incumbent training programs for all disciplines, including responders, hospitals, health care, political leadership, business, the media, and the general public.
- Jurisdictions give serious consideration to pooling training resources and expertise to share these assets, promulgating a more coordinated educational effort that will yield greater operational response efficiency because of responders' familiarity with the threat and the requisite response.
- Training be conducted using train-the-trainer, Internet, Intranet, and other systems that permit distance and home learning.

EMERGENCY MANAGEMENT SKILL SETS

Managing catastrophic events requires a unique skill set that may be uncommon among elected and appointed officials. Terrorist attacks will require organizations that typically do not engage in an emergency response to participate actively in emergency management activities. Senior managers and officials may also be targeted by the attacks, as was the case on September 11, making prior emergency management training more critical because decision-making abilities are compromised.

We recommend that:

- Emergency management training be developed and delivered to federal, state, and local agency executives and key staff members.
- Such training be mandatory and be tied to federal funding.

FEDERAL COORDINATION

The agencies of the federal government involved in preparing for terrorism incidents have historically been poorly coordinated, poorly organized, and generally unable to look beyond their individual missions. Programmatic and fiscal competition among the agencies have also contributed to confusion among many elected and appointed officials about how much is being done by the federal government to improve domestic preparedness for terrorist attacks. Regulations promulgated by individual agencies have often been in direct conflict with the missions of other federal agencies, occasionally compromising national security. Efforts by various federal agencies to coordinate the diverse array of activities associated with domestic preparedness have fallen far short of what is needed.[2] Compounding this situation is general lack of agreement as to whether terrorism is a national security problem or a law enforcement matter. The

[2] See Richard A. Falkenrath, Robert D. Newman, and Bradley A. Thayer *America's Achilles Heel*, BCSIA Studies in International Security (Cambridge: MIT Press, 1998), for a full discussion of these issues.

Office of Homeland Security is an excellent step toward coordinating the efforts of the various federal agencies, but today it has little more authority than the threat of voicing displeasure to the president about the actions or nonactions of federal agencies. Many academics and government experts have argued that the office should have direct budget authority and line control, and that the organization's head should be a cabinet post.[3] It is imperative that the Office of Homeland Security succeed in its mission to improve our domestic preparedness.

We recommend that:

- The Office of Homeland Security become a cabinet-level agency with full budget and administrative control to act as the "architect"[4]of domestic preparedness.
- Each federal agency perform a security impact analysis on their regulations, including public disclosure requirements.
- The United States establish and fund a non conventional think tank to explore unconventional threats and develop creative, active, responses to those threats.[5]

INTELLIGENCE, DATA, AND INFORMATION

Central to limiting the country's vulnerability to covert attack is the gathering, analysis, and dissemination of intelligence information. Recent events have demonstrated the consequences associated with the deterioration of the nation's intelligence-gathering capabilities. Intelligence for military purposes has increasingly been gathered through the use of sophisticated technologies with less involvement of human analysts. This has created an abundance of data, but has not necessarily yielded more or better information. An associated difficulty is the training of persons who can speak various languages and interact in various cultures, particularly non-European languages and cultures. The creation of this capacity is likely to take a number of years.

We recommend that:

- Efforts be initiated immediately to increase human intelligence capacity of the nation's intelligence-gathering system.
- We recommend that intensive recruiting and training be commenced to increase the number of analysts and operatives fluent in Arabic, Slavic, and Asian languages, as well as other languages spoken in cultures now thought to be potential adversaries to the United States, and able to function effectively in the cultures in which those languages are spoken.

Law enforcement intelligence gathering similarly needs to be reinvigorated. The FBI and other federal law enforcement agencies have large amounts of intelligence information available to them. These agencies, particularly the FBI, are notorious for their reluctance to share information with local law enforcement officials, while nonetheless demanding that local officials share everything with them. . Local police chiefs have complained about the timeliness and quality of the information obtained from federal sources. Many departments rely on CNN, MSNBC, and the Internet for intelligence information, because these sources often provide more complete, detailed, and timely information to local authorities than the FBI provides. This one-way information flow creates several challenges, the first being a strain on relationships with local officials, who generally will be the first to have to address a problem. The

[3] See Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction: *Third Annual Report to the President and the Congress*, (The Gilmore Report), December 15, 2001.
[4] Ashton B. Carter, "The Architecture of Government In the Face of Terrorism," *International Security*, Vol. 26, No. 3 (Winter 2001/02) p. 14.
[5] Ibid.

second challenge this creates is one of logistics. There are only 14,000 FBI agents, whereas there are more than 400,000 local law enforcement officers. Many federal law enforcement agencies bring significant technical expertise yet often lack tactical capacity, forcing them to rely heavily on local law enforcement.

Timeliness and specificity of warnings about potential or predicted terrorist activity is also problematic. Warnings must be sufficiently early to allow a response and must contain sufficient information to allow law enforcement and other local officials to assess the information and respond. Repeated warnings urging law enforcement to be "on the highest alert" against vague or unspecified threats do little good. Such warnings also create anxiety among the public that often manifests itself as increased calls for service from already taxed agencies. Although it is a difficult task to balance the need for specificity in warnings against the risks of compromising confidential information, it is important to recognize that information is a commodity available to many. Many items treated as confidential by some in law enforcement are already being reported by various media networks that have substantial information gathering capabilities. Information that can be used to prevent an attack should not be protected to preserve a possible prosecution after an incident.

Equally problematic is the law enforcement response to closely held information once it becomes public. Officials must manage the situation to prevent practical and political harm. An inadequate or inexperienced public information response by law enforcement to the release of such information is particularly troublesome.

We recommend that:

- Federal intelligence agencies and federal law enforcement agencies increase the use of analytical capabilities and technologies that enable them to analyze the data available to them more quickly.
- Federal law enforcement intelligence gathering and dissemination be revamped to include timely and accurate information sharing with local law enforcement agencies and "trusted agents" outside of the local law enforcement universe, including health departments, hospitals, and others that may participate in response to a terrorist incident.
- A nationwide intelligence list-server be created using secure web sites and trusted e-mail accounts.
- A tiered warning and alerting system be developed, similar to that employed by the National Weather Service or the military,[6] to provide warnings concerning suspected terrorist threats or attacks to affected agencies and the public. These warnings must be specific and timely.

EMERGENCY COMMUNICATIONS

The ability to communicate with various response organizations and their capacity to communicate among themselves are pivotal to the success of any emergency response operation, particularly a sizable one. System capacity and interoperability are critical components of response planning and response. Many jurisdictions have not migrated their communications systems to newer, higher capacity

[6] The National Weather Service's warning model uses watches to describe conditions favorable for severe weather conditions and warnings to denote specific hazards and response instructions. The military's tiered warning model uses threat conditions A through D, with Threatcon A being "normal" and Threatcon D being "imminent attack." These models could easily be adapted to provide information concerning increased terrorist activity, or non-specific threats reserving warnings for specific threats or attacks.

architectures and platforms. Many more have no interoperability within their own agencies and departments or with mutual-aid jurisdictions[7].

Upgrades, or more commonly wholesale replacement, of public-sector communications systems, telephone hardware and switches, and dispatch software are likely to be multi million-dollar expenditures. Many large municipalities have shouldered this burden through tax levies, bond issues, and other municipal financing. Many more medium-sized and small communities have insufficient financial bases for such expenditures. There are additional obstacles to such upgrading and replacement in the form of political parochialism, system control, and turfism. Although this situation seems ideal for regional solutions, these obstacles are often difficult to overcome.

Capacity and redundancy of private communications networks is similarly important. Wireline providers have for many years built several layers of redundancy into their networks. The telephone switches for lower Manhattan, located in the subbasement of the World Trade Center, continued to operate until the backup batteries ran out 36 hours after the towers collapsed. Cellular telephone systems and networks have become increasingly popular and have become an important communications tool for both public officials and the general public. Although most systems have significant capacity, their designs dictate certain limits on how many users can be supported by a single site. Difficult questions concerning the balance of use, particularly during emergencies, surround cellular capacity. Plans to limit cellular infrastructure access and use to public officials during emergencies ignore the central role cellular technology played in warning the public about the September 11 attacks, when passengers on the hijacked airliners were able to call family members and 911 centers to report the terrorist plot. Equally important is the role cellular systems play in notifying public officials about various emergencies, since most officials use cellular technology heavily. These systems must have backup capabilities, including satellite and portable cellular site capacities to replace or augment stricken sites, switches, or other key infrastructures.

We recommend that:

- The Federal Communications Commission (FCC) establish regulations governing the upgrade of public safety voice and data communication networks to ensure regional compatibility and interoperability.
- Congress fund a nationwide system of regional voice and data communication systems for state and local government use.
- The FCC disseminate information concerning recent orders which set aside portions of the electromagnetic spectrum for public-safety use[8].
- The FCC Homeland Security Policy Council develop a system to prioritize cellular traffic.
- FEMA establish a rapidly deployable cache of communications equipment similar to that used by the United States Forest Service.

---

[7] **For a thorough examination of interoperability issues see Viktor Mayer-Schönberger "Emergency Communication - The Quest for Interoperability in the United States and Europe" BCSIA Discussion Paper 2002-__, ESDP Discussion Paper no. ESDP-2002-__, John F. Kennedy School of Government, Harvard University, Publication forthcoming 2002**

[8] See http://www.fcc.gov/Bureaus/Wireless/News_Releases/2002/nrwl0202.html

CRITICAL INFRASTRUCTURE

By virtue of their size, geographic distribution, and nature, critical energy, water, wastewater, telecommunications, and technological infrastructures are vulnerable to a wide variety of potential attacks. The threats to energy and telecommunications utilities are relatively well understood, and particularly in the nuclear power industry, some security measures have already been deployed. Significantly less attention has been paid however, to the security of telecommunications, water, and wastewater utilities. Many of these utilities are operated on a municipal level, and responsibility for their security falls to an already burdened local police force. Water utility operators find themselves confused by conflicting information as to contamination threats, sampling protocols, and treatment methodologies. Media reports of reservoir contamination have exacerbated public concerns in this area.

Cyberterrorism has been identified at least since the millennium rollover (Y2K) as a potential threat. Recent reports of system control intrusions, denial-of-service attacks, electronic fraud, and even securities violations, perhaps perpetrated by terrorist supporters, have stimulated a renewed interest in protection against cyberterror. The FBI-sponsored Infraguard initiative has made substantial progress in establishing public and private relationships, encouraging reporting of computer intrusions, and reducing vulnerability of Infraguard member systems, but participation in the Infraguard program among both public agencies and private-sector companies and organizations is minimal.

We recommend that:

- The National Infrastructure Protection Commission (NIPC) be expanded and that it be given the authority to coordinate and responsibility for coordinating the production of planning and response guidance documents for each of the utility disciplines.
- The Environmental Protection Agency (EPA) immediately coordinate water treatment methodology and guidance with the Department of Defense and promulgate potable water treatment standards for known or suspected chemical and biological contaminants.
- The EPA fund research to develop additional treatment, sampling, and laboratory identification techniques for potable water contaminants.
- The FBI Infraguard program be marketed to business and government to increase participation.
- The FBI enhance the electronic surveillance and warning system for alerting participants in the Infraguard program of electronic attacks.
- Regulations requiring publication of hazardous materials “worst-case-scenarios” be modified to prevent the discovery of this information by potential adversaries.

AGRICULTURE AND LIVESTOCK

The outbreak of hoof-and-mouth disease in Europe and England during 2001 devastated economies, produced drastic changes to entry requirements worldwide, and provided insight into the potential impact of an attack launched against this nation’s food supply. Only U.S. Department of Agriculture (USDA) and a few states have adequate resources to address the prospect of agricultural terrorism.[9] The production of foodstuffs and livestock typically takes place in rural environments with limited response capacities.

[9] Gavin Cameron and Jason Pate. "Covert Biological Weapons Attacks Against Agricultural Targets: Assessing the Impact Against U.S. Agriculture," BCSIA Discussion Paper 2001-9, ESDP Discussion Paper no. ESDP-2001-05, John F. Kennedy School of Government, Harvard University, August 2001.

Internet based information systems must be employed to alert farmers and food producers to possible threats. Surveillance systems for livestock and crop diseases can provide advance warning that will allow outbreaks to be contained. Similar to other forms of biological terrorism, agricultural terrorism may be difficult to distinguish from natural occurrences of disease, making rapid identification and response to outbreaks as important as is it within human populations, particularly since outbreaks in these environments often provide warning to potential human exposure.

We recommend that:

- The USDA establish a veterinary "push-pack" where key pharmaceuticals necessary to treat to a variety of livestock and plant diseases are pre-positioned in strategic locations, similar to that established by the CDC for human diseases.
- The USDA set up a biosecurity training program to counter the threat of diseases and pests at the farm level.[10]
- The USDA devote more resources to disease detection, surveillance, and diagnostic technologies, including creating linked animal-human disease databases, developing more rapid diagnostic tests, increasing capacities at the Plum Island laboratory (where key agricultural testing is performed), and establishing a contingency network of veterinarians that could respond to veterinary emergencies.[11]
- The USDA be ready to deal with the public reaction to a serious food scare from disease in the event of an agro terrorist attack, and be given the budgetary means to proceed with fast and efficient recovery.[12]
- The USDA establish a program of security assessment and detection for food-processing facilities.
- The USDA, Food and Drug Administration (FDA), and CDC link their disease monitoring databases and jointly develop surveillance systems that use this combined data to improve early warning systems.

TRANSPORTATION

The size, diversity, and volume of transportation activities in the United States present one of the largest series of potential terrorist targets, vulnerabilities, and challenges to response and preparedness. The agencies charged with managing this diverse set of activities face substantial challenges in terms of logistics and technology development and deployment, as well as those associated with implementation. We have subdivided the subject matter in this area according to various types of transportation to facilitate presentation.

Vehicular Traffic

Vehicular and particularly truck traffic is critical to the nation's economy as it is the primary means of delivering goods. There are an estimated 500,000 trucks on the nation's highways every day, and each of

[10] Anne Kohnen, "Responding to the Threat of Agroterrorism: Specific Recommendations for the United States Department of Agriculture." BCSIA Discussion Paper no. 2000-29, ESDP Discussion Paper no. ESDP-2000-04, John F. Kennedy School of Government, Harvard University, October 2000. P 39.
[11] Ibid.
[12] Ibid.

these vehicles is both an important part of the economy and also a potential terrorist weapon. Monitoring the transport of hazardous materials, chemicals, and precursor materials (those chemicals or materials which can be easily made into a weapon) by truck is a daunting task made more difficult by the immediacy of the impact chemicals can have if they are released. The nation has engaged in significant training and equipping of hazardous materials response teams in many fire departments and has built a regulatory framework designed to mitigate environmental damage from the release of hazardous materials. The regulations are not, however, optimized for monitoring of the content or the location of many types of hazardous materials during shipment. There is also no standard mechanism for monitoring the safety of the driver of a vehicle transporting hazardous materials, or to ensure that the assigned driver remains with the vehicle. There are also no systems currently in use to monitor the movement of rental vehicles and trucks that may be used to transport hazardous materials or that may be used as truck-bombs.

Bridges, tunnels, and other key transit infrastructures are also vulnerable to attack, either from vehicle bombs or from other types of covert attacks. Physical barriers protecting structural components have been erected in some locations, restrictions have been imposed on certain types of traffic, and guards or police officers have been deployed at other locations to prevent physical destruction of key transportation infrastructures. Many of these measures must be considered temporary, as their long-term deployment is not financially possible.

We recommend that:

- The regulatory framework focus on building a system that can reliably identify legitimate transportation activity to allow closer inspection and regulation of actvity deemed otherwise by exception.[13]
- The Transportation Secretary immediately require the satellite tracking of hazardous materials shipments by carriers.
- This requirement include route plans, driver links with personal identification numbers (PINs), and cargo identification and that these systems be configured to report by exception those loads that deviate significantly from their route plan. Deviations should be immediately reported to the appropriate law enforcement agency.
- These systems should first be deployed on shipments of hazardous materials, second on shipments of non-hazardous materials, and third on commercial rental fleets.
- Key bridges, tunnels, and transit infrastructures be identified and monitored in terms of hazardous materials traffic on them or through them. Hazardous materials should not be allowed in, on, or near these structures. The monitoring of these structures should be performed by local law and transportation enforcement officials.

Trains

Much of the heavy freight in the United States and large quantities of its hazardous materials, are transported by rail. In addition to being critical components of the nation's transportation system, trains can become targets of opportunity for terrorists. Rails often pass close to metropolitan centers and assembly occupancies and also traverse rural areas. This can present problems in terms of massive releases of chemicals being transported as cargo, which can burn or explode, or may themselves be toxic. Urban releases have the potential to affect significant numbers of people whereas releases in rural areas are problematic because of the limited resources for response available in most rural areas.

[13] Stephen E. Flynn, "The Unguarded Homeland—A Study In Malign Neglect," in James F. Hodge and Gideon Rose (eds.), *How Did This Happen? Public Affairs Reports*, (Cambridge, Mass.: Council on Foreign Relations, 2001) pp. 183-197 at p. 195.

Trains and subways also represent significant passenger transportation resources in many parts of the country. Passenger traffic on trains has dramatically increased since the September attacks with comparatively little increase in security.

We recommend that:

- Tracking of hazardous materials be implemented, similar to that described for trucking shipments above.
- Additional training be provided to rural first responders to increase their recognition of potential terrorist incidents involving rail freight.
- Passenger rail security be completely reevaluated taking into account current and future threats.

Maritime Vessels and Seaports

The United States operates a large number of seaports both domestically and in its territories. These ports are vital links to shipping, international commerce, and domestic product export. For a number of locations, the ports are the primary connection to the rest of the country or the world. Significant amounts of hazardous materials and cargoes pass through these ports, and these materials, as well as the infrastructures that house and transport them are potentially appealing terrorist targets. These ports and the vessels that use them are protected by an aging fleet of vessels, which are often borrowed from volunteers. Only a small number of ports have their own law enforcement agencies; few have adequate staffing to patrol, police, and interdict potential attackers.

We recommend that:

- The Coast Guard and the Department of Transportation immediately assess the equipment and staffing needed to protect the nation's harbors and the shipping vessels using them.
- Activities in the major seaports, particularly those handling hazardous cargoes and military vessels, be monitored in a manner similar to that described above for the trucking industry.
- Screening and prescreening of high-risk cargo containers bound for the United States be expanded.

Aviation

The use of aircraft as weapons is not new, yet the use for which they were deployed September 11, was in many respects different from those in previously encountered hijacking scenarios. Securing the nation's airspace since the attacks has involved a complicated dynamic seeking to balance passenger flow, symbolic security, and actual security against a diverse collection of threats.

The United States has struggled with aviation security for a number of years. Driven by a series of hijackings in the 1970s, airport security was modified at that time to include x-raying of carry-on bags and inspection of passengers with magnetometers, credentialing of ramp personnel, and increased inspection of airline freight, cargo, and baggage. These security measures have improved the security of the nation's airports but are far from a perfect solution to an evolving threat.

The Federal Aviation Administration (FAA) has delegated the responsibility for airport security to the airlines, a move criticized by many because of the inherent conflict between cost savings and security. The FAA has historically operated as a reactive agency, addressing threats as or after they occur rather

than planning for them before they occur. It has created a cumbersome bureaucracy that is frustrating to airlines, to airport operators, to aircraft manufacturers, and to travelers. Aviation threats have been evolving for the past decade or more, yet the regulatory framework has not evolved to meet the challenges these new threats pose. After the bombing of Pan Am Flight 103, the world's aviation community made significant changes in security. Bag matching, passenger profiling, screening of both checked and hand luggage, watch lists, and credentialing changes, including background and criminal history checks for ramp personnel and caterers, became the norm.

The nonoccurrence of hijacking events in the United States during the past two decades has lulled the airline industry into a false sense of security. Unfortunately the government propensity to react rather than plan has now created a situation foisting dramatic hardships on entire sections of the economy. In its efforts to increase airport security in the wake of the September 11 attacks, the FAA, and to an extent well-intentioned lawmakers, have focused on highly symbolic measures that have staggering economic and liberty costs and limited security impact. Many of these measures are completely ineffective against suicide bombers. Many others have created new security threats, including the risks associated with bombing now overloaded ticketing halls, passenger drop-off areas, and food courts, "piggy backing" to gain access to restricted areas, and kidnapping or killing of credentialed employees to gain ramp or aircraft access. The creation of the Transportation Security Administration (TSA) provides an opportunity to address many of these issues.

We recommend that:

- The TSA take a fresh approach to aviation security, including making changes in contractors, personnel, programs, and methodology as appropriate.
- Airline ticketing systems and databases be linked to law enforcement information systems to prevent wanted and suspect individuals from obtaining tickets for airline flights
- Federal watch lists be similarly linked to airline ticketing systems and that these systems be updated to flag any record containing obvious warning signs, including cash transactions, absence of luggage, unusual passports or visas, recorded reports of odd behavior, and past histories of security issues.
- The FAA eliminate ineffective passenger questioning concerning packing and custody of bags now being conducted by airline personnel, replacing it with a series of interview questions concerning the passenger's occupation, destination, and details about these which are available from the airline database.
- The FAA revisit its proposed deployment of computerized tomography x-ray (CTX) screening devices in airports, because of their throughput limitations and instead install combinations of CTX, baggage x-ray and explosive trace detection (ETD) machines to achieve 100 percent screening of checked baggage with acceptable throughput to meet airline scheduling needs. To minimize the potential for casualties from an explosive device hidden in checked luggage, measures involving these devices should be conducted away from ticket halls and out of passenger sight.
- The FAA require bag matching on all legs of all flights.
- The TSA, the FAA and DOT immediately evaluate the physical facilities of all major U.S. airports, starting with the major airline hubs, and assist with funding redesign and reconstruction to adequately support contemporary security needs, including passenger drop-off, bag checking, freight screening, catering, and airport administrative activities.

- The TSA and the FAA eliminate restrictions at terminal parking facilities added after September 11 that have created significant traffic problems and created new ticket hall vulnerability and have significantly affected airport revenues, while offering little if any protection from explosives.
- The TSA, the FBI, and other agencies immediately improve background checks and credentialing for airline, airport, and ramp workers, including automated fingerprint information system (AFIS) fingerprinting, biometric identification, and criminal history checks.
- The TSA, the FAA, and the airlines develop and implement a "trusted flyer" program for frequent flyers that incorporates background checks, fingerprinting, and biometric identification to allow more limited screening of these persons at airport check-in and check points.
- The TSA develop consistent guidance and sensible operational procedures for checkpoint operation and eliminate reactive restrictions on sharp objects such as pocket knives, sewing and medical needles, and nail files.
- Flight crews receive additional training on in-flight emergencies involving passengers.
- The FAA amend preflight passenger briefings to include a statement that the protection of the cockpit is the responsibility of both the flight crew and the passengers.[14]
- Airlines eliminate or modify meal service for the flight crew to limit opening of the cockpit door while in flight.
- Airlines bullet-proof the cockpit enclosure.
- Computerized passenger profiling systems (CAPPS) be revised to include ethnic and national-origin factors with respect to passengers from countries known to support terrorism.[15]
- The TSA and the FAA continue to evaluate new technologies, deploying them where appropriate, to further protect the cockpit, baggage holds, flight crews, and passengers.
- Further development of whole-body, noninvasive scanning.
- The National Guard be removed from airport security posts.[16]

PUBLIC HEALTH

A robust public health system provides significant benefits to the country. Systems used to protect the nation from covert biological attack also provide early-warning and epidemiological information concerning flu viruses, colds, bacterial outbreaks, and other naturally occurring illnesses. These systems can make the nation healthier, spot disease trends before they become significant problems, and allow the rapid deployment of drugs and other medical resources to address problems.

Unfortunately the public health infrastructure in the United States has deteriorated dramatically during the past several decades. Contemporary health care successes and the tendency for public funding to follow crises and individual disease priorities have resulted in understaffed and poorly equipped public health departments that in some cases lack even basic office technology. The national network of

[14] Gavin De Becker, *Fear Less* (Boston: 2002), Little Brown, p. 185.

[15] Gregg Easterbrook, "The All-Too-Friendly Skies," in James F. Hodge and Gideon Rose (eds.), *How Did This Happen? Public Affairs Reports*, (Cambridge, Mass.: Council on Foreign Relations, 2001) pp. 163-181.

[16] National Guard troops are inappropriate for airport security duty. Many guard units are not equipped, nor can they easily be equipped, with the appropriate weapons for this assignment. They also have not been properly trained for this mission. Airport security corridors are not designed for the additional personnel, and state budgets are not well positioned to absorb this cost.

epidemiological investigation capacity, the foundation of infectious disease surveillance, response, and prevention, is threadbare in some areas of the country and in nearly all areas lacks sufficient depth to sustain operations effectively against the challenge of a extraordinary outbreak. Resources are not sufficient to develop regular and wide-ranging interactions among public health and safety professionals at the local level. The resulting lack of familiarity with one another and the lack of relationships among these personnel created difficulties in recent anthrax investigations.

Stockpiles of pharmaceuticals and vaccines have dwindled until recently. Although there are currently several caches of crucial disease-fighting drugs in the country, additional caches need to be established to add response capacity in the event of multiple attacks or outbreaks. A system has been established to identify sources for drugs and vaccines for use during an emergency, but the system currently requires individual jurisdictions to make the necessary purchases, which present legal and logistical problems for those jurisdictions. Rotating stockpiles of essential drugs also proves problematic for local jurisdictions. Furthermore, the prophylactic administration of certain drugs has raised a number of clinical questions, including those involving the efficacy of and justification for such administration.

Laboratory identification of the organisms suspected to be involved in a biological attack is critical mounting an effective response to such an attack. Currently even the largest jurisdictions have only moderate capacity to test for biological agents, often less than 100 specimens per day. Recent testing of environmental specimens for anthrax quickly exceeded laboratory capacities. There is no uniform guidance on packaging environmental specimens for lab submittal, and there are numerous anecdotal reports of confusion among users of lab services as to which labs, public and private, are capable of performing preliminary and confirmatory tests for the presence of biological agents.

We recommend that:

- The public health infrastructure be enhanced to include improved access to information technologies and the Internet and additional staffing.
- The Department of Health and Human Services (HHS), in conjunction with the CDC and the state departments of health, establish and maintain a national epidemiological tracking system that employs both nontraditional and syndromatic surveillance methodology.[17] The system should be populated with data from emergency department visits, 911 centers, and health clinics and should track the sale of antibiotics and cough and cold medications.
- Epidemiological training programs be strengthened and made more widely available, with curricula appropriate for public health and law enforcement professionals.
- HHS purchase, deploy, and maintain baseline stocks of pharmaceuticals, vaccines, and antidotes in the thirty largest cities in the United States, and in strategic locations in all fifty states.
- HHS and CDC fund and perform studies to determine best practices for mass prophylaxis.
- CDC and USAMRIID more widely promulgate sampling, packaging, submittal, and testing guidelines for identification of suspected biological agents.
- CDC and USAMRIID develop and promulgate triage guidelines for environmental samples testing.
- All health departments develop staff epidemiologist capacity through direct hiring of personnel or via contract with suitable physicians.

[17] Nontraditional surveillance includes tracking emergency department visits, health clinic visits, 911 calls, just-in-time deliveries of cough and cold remedies from retailers, school attendance, police, fire, and emergency medical sick leave, etc. Syndromatic surveillance tracks symptom sets rather than diagnoses.

- That additional grant programs be established to increase laboratory capacity nationwide so that each of the thirty largest cities in the U.S. and each of the fifty states have their own Level B (or greater) laboratories to perform definitive identification analyses.

MEDICAL CAPACITY

The health care system in the United States has undergone massive changes in the past decade. Many of these changes have been driven by cost controls and have incorporated just-in-time delivery systems, managed care, and other measures that have severely limited the surge capacity of the nation's health care delivery system. The health care delivery system has also decentralized, which has created new challenges for epidemiologic data gathering and dissemination of information to health practitioners. There is also a significant misunderstanding within the prehospital emergency medical community about the impact of bioterrorism on the healthcare system.[18] The notional conclusions are that prehospital providers (ambulance services and fire departments) will bring patients to hospitals for treatment as they do during "normal" circumstances. The recent covert anthrax attacks suggest however, that people will present themselves to hospitals outside of the traditional 911 environment. If an incident occurs on any significant scale, hospital resources are likely to be overwhelmed quickly.

We recommend that:

- Cost recovery mechanisms be developed to allow the creation of additional surge capacities within hospital systems.
- The Department of Defense acute care center (ACC) and neighborhood emergency health center (NEHC) models be further studied and refined for deployment.
- Medical centers, hospitals, health care centers, community health clinics, and other distributed medical care facilities be required by the Centers for Medicare and Medicaid Services and JCAHO, to engage in emergency planning for various catastrophic events, including various forms of terrorism. This planning should be funded by the federal government.
- Existing educational programs for medical and allied health professionals incorporate and institutionalize training for terrorism response into curricula to preserve the "corporate knowledge" required for readiness.

IMMIGRATION AND BOARDER CONTROL

The threat posed by unmonitored foreign nationals in the United States became dramatically real September 11. Immigration and border officials have been unable to stem the flow of illegal immigrants and have insufficient staff to monitor those in the country legally. The vast borders of the United States present numerous opportunities for adversaries to enter the country illegally. It is critically important that border checkpoints have detection capacities to interdict the illegal import of dangerous substances, including explosives and chemical, biological, and improvised nuclear weapons. . Student visas are freely

[18] For more information see Joseph A. Barbera, Anthony G. Macintyre, and Craig A. DeAtley,. "Ambulances to Nowhere: America's Critical Shortfall in Medical Preparedness for Catastrophic Terrorism." BCSIA Discussion Paper no. 2001-15, ESDP Discussion paper no. ESDP-2001-07, John F. Kennedy School of Government, Harvard University, October 2001 and Juliette Kayyem, "U.S. Preparations for Biological Terrorism: Legal Limitations and the Need for Planning." BCSIA Discussion Paper no. 2001-4, ESDP Discussion Paper no. ESDP-2001-02, John F. Kennedy School of Government, Harvard University, March 2001.

issued, are poorly monitored and have been used by terrorists to gain inappropriate access to the United States.

A large number of agencies and organizations are involved in protecting the borders of and controlling the access of people and commodities to the United States. The U.S. Border Patrol, Immigration and Naturalization Service (INS), Customs Service, and Coast Guard all play a role in defending the nation in these areas.

We recommend that:

- The activities of the various agencies associated with border control, coastal protection, and immigration control be coordinated by the Office of Homeland Security.
- A treaty be developed with those nations that share borders with the United States to allow enforcement activities across international borders.
- Applications for student visas and green cards be tied to Interpol and other law enforcement databases.
- Students attending U.S. colleges and universities on student visas be expelled from the United States within 180 days if they are not actively enrolled in courses.
- Immigration databases be automated to include biometric identification and maintain information as to the whereabouts and activities of foreign nationals in the United States.
- U.S. Border Patrol capacities be increased to stem the flow of illegal immigrants into the United States.
- Border entry points be equipped with additional detection and inspection technologies to aid in the interdiction of illegal or dangerous materials.
- Federal and state statutes be amended to allow state and local law enforcement to detain foreign nationals for INS violations.

TERROR IN "REAL TIME": CHALLENGES FOR AND FROM THE MEDIA

Coverage of terrorism creates substantial problems for the news media. Contemporary technologies allow the broadcast of images virtually in real time, effectively allowing viewers to "live the events". Tremendous challenges exist in determining how to cover these types of events. Producers face challenges concerning how much, how long, and even how to cover terrorist activities. In many cases, "the story" became "the story". Media outlets had to identify new experts to assist them with information analysis and editorial decision-making. The attacks of September 11, and to a lesser extent the subsequent anthrax incidents, was the first real major news events many involved in the media had covered. The definition, perspective, and challenge of media coverage changed as a result of these events and the coverage of them. Producers and editors discovered that their staffs were themselves traumatized by the events.

We recommend that:

- A training program be developed for news producers and editors, covering editorial decision making, sources of information, particular risks to national security, and tactical law enforcement operations.

- A training program for field reporters be developed, including the above material and additional information on personal protection.
- The Office of Homeland Security and FEMA coordinate the creation of media information kits including fact sheets about the known chemical, biological, and nuclear agents and various explosive devices common to terrorist use.
- The Office of Homeland Security and FEMA coordinate the creation of training materials for senior federal, state, and municipal officials in dealing with the particular challenges of media coverage of major emergencies.

COLLEGES AND UNIVERSITIES

There are many colleges and universities in the United States. Many of these institutions conduct research using materials that can be, or have already been, made into chemical, biological, or even nuclear weapons. Some of these institutions also have significant populations of foreign students who may have direct or indirect ties to known adversaries of the U.S. Some types of research facilities on college and university campuses and a number of types of sporting or other events commonly held under college and university auspices may also constitute appealing targets for an adversary. Many of these institutions are situated outside municipalities and thus have limited public safety response resources.

We recommend that:

- A field training program be developed and deployed for colleges and university administrators and law enforcement officials including, information on weapons of mass destruction, civil disorder, incident management, and target identification and hardening.
- University labs and research facilities working with known or suspected chemical or biological agents be registered with the FBI.
- Colleges and Universities be required to monitor the enrollment status of all foreign students attending their facilities who are in the U.S. on student visas and immediately report those students who are not enrolled in active coursework for more than 180 days.

SUSTAINMENT FUNDING

Preparedness to meet the threat of terrorism is expensive. Training, equipment, technology, pharmaceuticals, security measures, and personnel all clamor for funding. In crafting response plans for various events, policymakers have long recognized that response forces are a critical, albeit expensive, necessity. Terrorism preparedness requires additional resources and capacities beyond those normally present in conventional public and private response systems. The question of whether terrorism is a national security matter or merely another emergency for which states and local officials must be prepared is coupled with competing interests and viewpoints.

There are essentially two types of funding available for emergency response preparedness: government and private. Government funding comes from national, state, and local sources. Private funding comes from insurance, private owners, and charitable donations. Sole reliance on any single funding source is foolish, and trying to shift the risk through insurance is likely to be prohibitively expensive because of the inherent difficulty of rating and assessing the actuarial probabilities associated with terrorist attacks.

We recommend that:

- The federal government fund the gap between normal preparedness and the extraordinary measures and equipment associated with terrorism preparedness, using a system of categorical and block grants to be administered through the existing grant administration mechanisms.
- Federal training support for the seventy-five largest jurisdictions in the United States be configured such that there is direct fiscal disbursement to these jurisdictions with no intermediary agency involved.

PRELIMINARY LESSIONS FROM THE WORLD TRADE CENTER AND PENTAGON ATTACKS

The attacks on the Pentagon and World Trade Center were unprecedented yet both of the attacked buildings had been attacked previously.[19] Assumptions about human behavior, structural stability, and confusion about what had occurred added to the additional loss of life sustained in both attacks. Private communications networks were overwhelmed immediately after the attacks. Confusing instructions given to occupants also contributed to delay in evacuating the buildings. More formal analyses are forthcoming; we believe however that there are critical lessons to be derived immediately from these incidents:

- Interagency communication capability and capacity are critical at major incidents.
- Staging of resources at the incident scene is critical to the success of incident management. Incident commanders *must* stage resources far enough away from the incident that they will not be lost if secondary events including collapse and explosions occur.
- Situational size-up by both initial responders and command officers is critically important. Senior commanders must anticipate and prepare for various contingencies.
- Response organizations should train and equip sufficient specialized response resources so that there is a redundancy of critical resources in an emergency response situation. These resources must be deployed in such a way as to minimize or prevent their complete destruction in the event various follow-on risks, including secondary attack, and structural collapse, after a primary terrorist attack.
- Emergency response personnel have an inclination to enter unsafe environments. Senior commanders must evaluate the risks of entry, including the location of forward command areas, and prevent personnel from engaging in extremely high-risk behavior.
- Employment of incident command is critical to the success of large operations. Incident command should be coordinated, and command posts should be established in safe areas with necessary support resources.
- Mutual-aid agreements are critical in all jurisdictions and for all states.
- State and federal response resources must be immediately deployed and utilized upon their arrival at incident scenes.[20]

[19] For more information see Jonathan B. Tucker, *Toxic Terror—Assessing the Use of Chemical and Biological Weapons*, (Cambridge: MIT Press, 2000), pp. 185-207.

[20] A review of the World Trade Center and Pentagon incidents, studies of the response to the bombing of the Murrah Federal Building in Oklahoma City, and the response to the most recent California earthquakes, all indicate that elements of local pride interfered with the rapid deployment of assisting response resources.

- Incident commanders must develop mechanisms to manage volunteers and donated goods, and the media should encourage cash donations rather than goods.

PRELIMINARY LESSONS FROM THE ANTRHAX ATTACKS

During October 2001, various media and political figures received a series of envelopes with crude handwriting containing finely milled anthracis bacillus powder. These letters became the first biological attack in the United States since the 1984 contamination of salad bars by the Bagwan Shree Rajineeshes in Oregon.

The anthrax letters were handled by postal workers and postal machinery and provided authorities with their first opportunity to determine the impact of mail-handling equipment and mail processes on tainted mail. They also presented the first opportunity to gauge the vulnerability of mail recipients and served to underscore the importance of immediate medical recognition and treatment of anthrax symptoms.

Of those victims anthracis bacillus infections who were seen by medical personnel, those who received immediate treatment with contemporary quinolone drugs recovered from the infections. Additionally, emergency and infectious-disease physicians determined that modern medical imaging, including MRI and CAT scans, can provide diagnostic information about anthrax exposure significantly earlier than conventional x-ray techniques.

It seems axiomatic in hindsight that a weaponized powder milled to a diameter of 3 microns would escape a conventional envelope with 100-micron holes in the seams. Mail-handling machinery is designed to handle large volumes of mail quickly. Such devices exert considerable force on the envelopes as they are sorted and processed. We now know that this force is sufficient to squeeze substances out of the envelopes and can cross-contaminate postal workers, other mail, and mail machinery.

The October 2001 anthrax attacks have demonstrated unequivocally that sophisticated delivery mechanisms are not necessary for suspected biological agents to cause significant disruption. Public safety and public health officials have been inundated with responses to examine powders on mail and in a variety of places. Public fear of powders created an environmental testing crisis. It remains unclear whether nonmilitary delivery means can effectively deliver a large scale attack. Although the total number of casualties from these attacks was fewer than 10, the disruptive effect and costs of cleanup are measured in billions of dollars.

These attacks have also underscored the lack of emergency management skills present in many leaders in a number of government agencies. The hazardous materials response, which was employed in the recent anthrax incidents, is ill-suited to medical incidents because it protects against different types of risks and raises inapposite concerns. Lack of familiarity with emergency response practices and decision paralysis produced great psychological trauma for affected postal, clerical, and mail-handling employees. Powder scares in unaffected facilities produced scores of needless responses. The collection of samples by workers clad in encapsulated protective suits, often from machines being operated by employees with no protection whatsoever, created significant labor issues with employees who were convinced by these actions they had been placed at substantial health risk. Disparate prophylaxis and exposure testing methodologies between political and postal staffs also created significant issues.

The October 2001 anthrax attacks have underscored many of the vulnerabilities highlighted elsewhere in this report, but have also yielded a number of specific lessons:

- Inhalational anthrax is not universally fatal if treated immediately.
- There is generally insufficient laboratory capacity in the United States to perform definitive identification testing. The CDC and USAMRIID labs need additional capacity, as do state and municipal health department labs.
- The CDC and USAMRIID need to immediately develop standardized lab protocols for preliminary and definitive identification testing of suspect substances. Once these protocols are developed, training programs to implement them need to be developed and deployed nationwide.
- The CDC and USAMRIID also need to immediately develop sampling and packaging protocols for laboratory submittal of suspect substances. Once these protocols are developed, training programs to implement them need to be developed and deployed nationwide.
- Environmental sampling protocols and building occupant reentry criteria need to be established by the EPA in conjunction with the CDC, USAMRIID, and the U.S. Public Health Service. These protocols must be based on medical risk assessment, not on hazardous materials methodology.
- The U.S. Postal Service, major freight companies, the CDC, USAMRIID, EPA, and U.S. Public Health Service should immediately develop and promulgate a single set of suspect mail and package-handling procedures. These procedures should include decision algorithms for suspicious envelopes, packages, and facilities and should include specific response checklists.
- The CDC, USAMRIID, and the U.S. Public Health Service should immediately develop and promulgate specific prophylaxis guidelines based on the efficacy of treatments used during anthrax attacks.
- The EPA, the CDC, and USAMRIID should develop specific guidance for immediate and thorough decontamination of facilities based on the efficacy of methods used to decontaminate facilities contaminated during these attacks.
- The U.S. Public Health Service should promulgate 911 call center triage algorithms that were developed by several major municipalities to address “suspicious powder” queries.
- The CDC and the U.S. Public Health Service should reevaluate the location and contents of the national stockpile of pharmaceuticals.
- The federal health community should streamline procedural guidance vetting processes to allow more timely issue of guidance.
- Great care must be taken to avoid disparity in prophylaxis to patients.
- FEMA should establish a general disaster declaration that is not tied to a specific geographic location.

THE CHALLENGE AHEAD

Terrorism readiness, planning, and response must balance opportunity costs against risk management.[21] As the nation reevaluates its readiness, it must overcome the human tendency to react to terrorist stimuli and must instead carefully consider its plans and responses. Difficult issues surround intrusions on liberty in the name of security. Terrorism is not new. It has been a staple of life in Northern Ireland for almost a century.[22] When terror first struck there, temporary laws were enacted that greatly restricted the liberty of Irish citizens. Almost a century later, many of these intrusions remain. The United States is a country built upon principles of restrained government, reasoned laws, due process, and fundamental fairness for all of its citizens. In addressing the terrorist threat, the nation must not sacrifice fundamental freedoms in reaction (or over-reaction) to threats and perceived risks. It must resist the temptation to react to the threat of yesterday and concentrate proactive efforts on preparing for the threat of today and tomorrow.

Successful responses to terrorist events, much like responses to more mundane emergencies and athletic competition, hinge on relationships, knowledge, and proactive responses based on thoughtful, comprehensive, and well-rehearsed plans. As Senator Richard G. Lugar, coauthor of the landmark Nunn, Lugar, Domenici anti-terror legislation, warned: “We will lose persons in the initial attack, but failure to prepare for these attacks, and failure of people in responsible positions to know what to do, will be indefensible.” Our experience tells us that the recommendations we have offered in this paper will allow the teams on the fields of emergency response to play well at the terrorism line of scrimmage. Vince Lombardi’s guidance is especially appropriate for this contest: “Winning isn’t everything; it’s the only thing.”

We encourage the immediate adoption of the recommendations presented in this paper to make our nation a safer place.

[21] The discussion in this section draws significantly on Richard A. Falkenrath, "The Problems of Preparedness: Challenges Facing the U.S. Domestic Preparedness Program." BCSIA Discussion Paper no. 2000-28, ESDP Discussion Paper no. ESDP-2000-05, John F. Kennedy School of Government, Harvard University, December 2000.

[22] Laura K. Donohue, "In the Name of National Security: U.S. Counterterrorist Measures, 1960-2000." BCSIA Discussion Paper no. 2001-6, ESDP Discussion Paper no. ESDP-2001-04, John F. Kennedy School of Government, Harvard University, August 2001.

EXECUTIVE SESSION ON DOMESTIC PREPAREDNESS

JOHN F. KENNEDY SCHOOL OF GOVERNMENT
HARVARD UNIVERSITY

The John F. Kennedy School of Government and the U.S. Department of Justice have created the Executive Session on Domestic Preparedness to focus on understanding and improving U.S. preparedness for domestic terrorism. The Executive Session is a joint project of the Kennedy School's Belfer Center for Science and International Affairs and Taubman Center for State and Local Government.

The Executive Session convenes a multi-disciplinary task force of leading practitioners from state and local agencies, senior officials from federal agencies, and academic specialists from Harvard University. The members bring to the Executive Session extensive policy expertise and operational experience in a wide range of fields - emergency management, law enforcement, national security, law, fire protection, the National Guard, public health, emergency medicine, and elected office - that play important roles in an effective domestic preparedness program. The project combines faculty research, analysis of current policy issues, field investigations, and case studies of past terrorist incidents and analogous emergency situations. The Executive Session is expected to meet six times over its three-year term.

Through its research, publications, and the professional activities of its members, the Executive Session intends to become a major resource for federal, state, and local government officials, congressional committees, and others interested in preparation for a coordinated response to acts of domestic terrorism.

***For more information on the Executive Session on Domestic Preparedness, please contact*:**

Rebecca Storo, Project Coordinator, Executive Session on Domestic Preparedness
John F. Kennedy School of Government, Harvard University
79 John F. Kennedy Street, Cambridge, MA 02138
Phone: (617) 495-1410, Fax: (617) 496-7024
Email: esdp@ksg.harvard.edu
http://www.esdp.org

BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS

JOHN F. KENNEDY SCHOOL OF GOVERNMENT
HARVARD UNIVERSITY

BCSIA is a vibrant and productive research community at Harvard's John F. Kennedy School of Government. Emphasizing the role of science and technology in the analysis of international affairs and in the shaping of foreign policy, it is the axis of work on international relations at Harvard University's John F. Kennedy School of Government. BCSIA has three fundamental issues: to anticipate emerging international problems, to identify practical solutions, and to galvanize policy-makers into action. These goals animate the work of all the Center's major programs.

The Center's Director is Graham Allison, former Dean of the Kennedy School. Stephen Nicoloro is Director of Finance and Operations.

BCSIA's *International Security Program (ISP)* is the home of the Center's core concern with security issues. It is directed by Steven E. Miller, who is also Editor-in-Chief of the journal, *International Security*.

The *Strengthening Democratic Institutions (SDI)* project works to catalyze international support for political and economic transformation in the former Soviet Union. SDI's Director is Graham Allison.

The *Science, Technology, and Public Policy (STPP)* program emphasizes public policy issues in which understanding of science, technology and systems of innovation is crucial. John Holdren, the STPP Director, is an expert in plasma physics, fusion energy technology, energy and resource options, global environmental problems, impacts of population growth, and international security and arms control.

The *Environment and Natural Resources Program (ENRP)* is the locus of interdisciplinary research on environmental policy issues. It is directed by Henry Lee, expert in energy and environment. Robert Stavins, expert in economics and environmental and resource policy issues, serves as ENRP's faculty chair.

The heart of the Center is its resident research staff: scholars and public policy practitioners, Kennedy School faculty members, and a multi-national and inter-disciplinary group of some two dozen pre-doctoral and post-doctoral research fellows. Their work is enriched by frequent seminars, workshops, conferences, speeches by international leaders and experts, and discussions with their colleagues from other Boston-area universities and research institutions and the Center's Harvard faculty affiliates. Alumni include many past and current government policy-makers.

The Center has an active publication program including the quarterly journal *International Security*, book and monograph series, and Discussion Papers. Members of the research staff also contribute frequently to other leading publications, advise the government, participate in special commissions, brief journalists, and share research results with both specialists and the public in a wide variety of ways.

BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS

RECENT DISCUSSION PAPERS

For a complete listing of BCSIA Publications, please visit www.ksg.harvard.edu/bcsia

---

2001-09 Pate, Jason and Gavin Cameron, "Covert Biological Weapons Attacks Against Agricultural Targets: Assessing the Impact Against U.S. Agruculture."

2001-08 Carment, David. "The Role of Bias in Third Party Intervention: Theory and Evidence."

2001-07 Foster, Charles, H.W. Foster and James N. Levitt. "Reawakening the Beginner's Mind: Innovation in Environmental Practice."

2001-06 Donohue, Laura. "In the Name of National Security: U.S. Counterterrorism Measures, 1960-2000."

2001-05 Koblentz, Gregory. "Overview of Federal Programs to Enhance State and Local Preparedness for Terrorism with Weapons of Mass Destruction."

2001-04 Kayyem, Juliette. "U.S. Preparations for Biological Terrorism: Legal Limitations and the Need for Planning."

2001-03 Foster, Charles H.W. and James S. Hoyte. "Preserving the Trust: The Founding of the Massachusetts Environmental Trust."

2001-02 Coglianese, Cary. "Is Consensus and Appropriate Basis for Regulatory Policy?"

2001-01 Donohue, Laura K. and Juliette N. Kayyem. "The Rise of the Counterterrorist States,"

2000-33 Kates, Robert, William Clark, Robert Corell, J. Michael Hall, Carlo Jaeger, Ian Lowe, James McCarthy, Hans Joachim Schellnhuber, et al. "Sustainability Science."

2000-32 Guston, David H., William Clark, Terry Keating, David Cash, Susanne Moser, Clark Miller, and Charles Powers. "Report of the Workshop on Boundary Organizations in Environmental Policy and Science."

2000-31 Falkenrath, Richard. "Analytic Models and Policy Prescription: Understanding Recent Innovation in U.S. Counterterrorism."

2000-30 Merari, Ariel. "Israel's Preparedness for High Consequence Terrorism."

2000-29 Kohnen, Anne. "Responding to the Threat of Agroterrorism: Specific Recommendations for The United States Department of Agriculture."

2000-28 Falkenrath, Richard. "The Problems of Preparedness: Challenges Facing the U.S. Domestic Preparedness Program."

2000-27 Clark, William. "America's National Interests in Promoting a Transition Toward Sustainability."

TAUBMAN CENTER FOR STATE AND LOCAL GOVERNMENT

JOHN F. KENNEDY SCHOOL OF GOVERNMENT
HARVARD UNIVERSITY

The Taubman Center for State and Local Government focuses on public policy and management in the U.S. federal system. Through research, participation in the Kennedy School's graduate training and executive education programs, sponsorship of conferences and workshops, and interaction with policy makers and public managers, the Center's affiliated faculty and researchers contribute to public deliberations about key domestic policy issues and the process of governance. While the Center has a particular concern with state and local institutions, it is broadly interested in domestic policy and intergovernmental relations, including the role of the federal government.

The Center's research program deals with a range of specific policy areas, including urban development and land use, transportation, environmental protection, education, labor- management relations and public finance. The Center is also concerned with issues of governance, political and institutional leadership, innovation, and applications of information and telecommunications technology to public management problems. The Center has also established an initiative to assist all levels of government in preparing for the threat of domestic terrorism.

The Center makes its research and curriculum materials widely available through various publications, including books, research monographs, working papers, and case studies. In addition, the Taubman Center sponsors several special programs:

The Program on Innovations in American Government, a joint undertaking by the Ford Foundation and Harvard University, seeks to identify creative approaches to difficult public problems. In an annual national competition, the Innovations program awards grants of $100,000 to 15 innovative federal, state, and local government programs selected from among more than 1,500 applicants. The program also conducts research and develops teaching case studies on the process of innovation.

The Program on Education Policy and Governance, a joint initiative of the Taubman Center and Harvard's Center for American Political Studies, brings together experts on elementary and secondary education with specialists in governance and public management to examine strategies of educational reform and evaluate important educational experiments.

The Saguaro Seminar for Civic Engagement in America is dedicated to building new civil institutions and restoring our stock of civic capital.

The Program on Strategic Computing and Telecommunications in the Public Sector carries out research and organizes conferences on how information technology can be applied to government problems -- not merely to enhance efficiency in routine tasks but to produce more basic organizational changes and improve the nature and quality of services to citizens.

The Executive Session on Domestic Preparedness brings together senior government officials and academic experts to examine how federal, state, and local agencies can best prepare for terrorist attacks within U.S. borders.

The Program on Labor-Management Relations links union leaders, senior managers and faculty specialists in identifying promising new approaches to labor management.

The Internet and Conservation Project, an initiative of the Taubman Center with additional support from the Kennedy School's Environment and Natural Resources Program, is a research and education initiative. The Project focuses on the constructive and disruptive impacts of new networks on the landscape and biodiversity, as well as on the conservation community.

TAUBMAN CENTER FOR STATE AND LOCAL GOVERNMENT

RECENT DISCUSSION PAPERS

A Complete Publications List Is Available at www.ksg.harvard.edu/taubmancenter

---

2001 Donohue, Laura K. "In the Name of National Security: U.S. Counterterrorist Measures, 1960-2000

2001 Donohue, Laura K. and Juliette N. Kayyem. "The Rise of the Counterterrorist States."

2001 Executive Session on Domestic Preparedness. "A New National Priority: Enhancing Public Safety and Health Though Domestic Preparedness."

2001 Gómez-Ibáñez, José A. "Deregulating Infrastructure: Breaking Up Is Hard To Do," $6.

2001 Greene, Jay P. "An Evaluation of the Florida A-Plus Accountability and School Choice Program," $6.

2001 Harvard Policy Group on Network-Enabled Services and Government. "Use for IT Strategic Innovation, Not Simply Tactical Automation," $7.

2001 Harvard Policy Group on Network-Enabled Services and Government. "Utilize Best Practices in Implementing IT Initiatives," $7.

2001 Kayyem, Juliette N. "U.S. Preparations for Biological Terrorism: Legal Limitations and the Need for Planning."

2001 Koblentz, Gregory D. "Overview of Federal Programs to Enhance State and Local Preparedness for Terrorism with Weapons of Mass Destruction."

2001 Pate, Jason and Gavin Cameron, "Covert Biological Weapons Attacks Against Agricultural Targets: Assessing the Impact Against U.S. Agriculture."

2001 Peterson, Paul, David Campbell and Martin West. "An Evaluation of the Basic Fund Scholarship Program in the San Francisco Bay Area, California," $6.

2000 Donohue, Laura. "Civil Liberties, Terrorism, and Liberal Democracy: Lessons from the United Kingdom."

2000 Falkenrath, Richard A. "Analytic Models and Policy Prescription: Understanding Recent Innovation in U.S. Counterterrorism."

2000 Falkenrath, Richard A. "The Problems of Preparedness: Challenges Facing the U.S. Domestic Preparedness Program."

2000 Fung, Archon, Charles Sabel and Dara O'Rourke. "Ratcheting Labour Standards: How Open Competition Can Save Ethical Sourcing," $6.

2000 Harvard Policy Group on Network-Enabled Services and Government. "Eight Imperatives for Leaders in a Networked World: Guidelines for the 2000 Election and Beyond," $7.

2000 Harvard Policy Group on Network-Enabled Services and Government. "Focus on How IT Can Reshape Work and Public Sector Strategies," $7.

2000 Harvard Policy Group on Network-Enabled Services and Government. "Guidelines for the 2000 Election and Beyond," $7.

2000 Hassel, Bryan and Lucy Steiner. "Strategies for Scale: Learning from Two Educational Innovations," $6.

2000 Howell, William G., and Paul E. Peterson. "School Choice in Dayton, Ohio: An Evaluation After One Year," $5.

2000 Kohnen, Anne. "Responding to the Threat of Agroterrorism: Specific Recommendations for the United States Department of Agriculture."

2000 Leonard, Herman (Dutch) and Jay Walder. "The Federal Budget and the States: Fiscal Year 1999."

2000 Merari, Ariel. "Israel's Preparedness for High Consequence Terrorism."

2000 Peterson, Paul et al. "School Choice in New York City After Two Years: An Evaluation of the School Choice Scholarships Program," $6.

2000 Peterson, Paul Patrick Wolf and William Howell. "School Choice in Washington, DC: An Evaluation After One Year," $6.

2000 Peterson, Paul and William Howell. "The Effect of School Vouchers on Student Achievement: A Response to Critics," $6.

2000 Peterson, Paul Patrick Wolf William Howell and David Campbell. "Test Score Effect of School Vouchers in Dayton, Ohio, New York City and Washington, DC: Evidence on Randomized Field Trials," $6.

2000 Richmond, Jonathan. "The Private Provision of Public Transport," $25.

2000 Saguaro Seminar: Civic Engagement in America. "Better Together," $10.

2000 Stuart, Guy. "Segregation in the Boston Metropolitan Area at the end of the 20th Century," $5.

2000 Weil, David. "Everything Old Is New Again: Regulating Labor Standards in the U.S. Apparel Industry," $5.

2000 Wolf, Patrick J., Paul E. Peterson and William G. Howell. "School Choice in Washington D.C.: An Evaluation After One Year," $5.