

IV. CONCLUSIONS AND RECOMMENDATIONS

On the publication date of this report, the Panel will have been formally conducting business for about six months, and will have had three official meetings—the most recent on December 13, 1999. During that time, substantial information and authoritative analyses have been presented to or have come to the attention of the Panel and its members. Moreover, the Panel is composed of members who have significant expertise and broad experience in this field.

Based on the information provided, the thorough analysis of the potential threats contained in this report, and the collective knowledge and experience of its members, the Panel has drawn some initial conclusions and is making several broad recommendations. In its two subsequent annual reports, the Panel will make more comprehensive and definitive recommendations on a variety of topics.

These initial conclusions and recommendations should not be construed to suggest that the Federal government—either in its executive or legislative branch—currently undertake a major restructuring for this (or any other) potential crisis. The recommendations are intended to propose solutions to this critical national problem to assist in making Federal programs and activities more effective and efficient.

It is axiomatic that, the better we prepare, through a broad spectrum of antiterrorism and counterterrorism activities, the more likely we are to reach the ideal situation—the deterrence, prevention, or interdiction of any terrorist event before it occurs. Given the nature of the potential threats, it is likely that no amount of preparation will cover all possible threat scenarios, and that adequate measures must be undertaken to respond, if an event should occur, in a way that will—first and foremost—minimize human casualties, and that will also mitigate damage to property and to the environment.

In order to achieve these inter-related goals—effective deterrence, prevention, interdiction, and response—efforts at all levels of government must be concerted, concentrated, and collective.¹⁸¹

Threat Assessments and Analyses

This report observes that there has not been universal agreement on several aspects of the potential threat or threats from terrorists who may use or attempt to

¹⁸¹The Panel notes with much interest the recent announcement by the Federal Bureau of Investigation of its plan to reorganize the bureau, creating a separate Counterterrorism Division, which will focus on terrorist threats, domestic preparedness, and critical infrastructure protection. See “FBI to Restructure, Adding Emphasis on Crime Prevention,” *The Washington Post*, November 11, 1999, p. A2.

use CBRN devices or other “weapons of mass destruction.” Early in its deliberations, the Panel determined that, for it to make well-reasoned and informed assessments and to offer substantive, comprehensive, and articulate policy recommendations to the nation’s executive and its legislature, a complete, current, and realistic analysis of the potential domestic threats from terrorists was an essential condition precedent to fulfilling the Panel’s legislative mandate. With some condensation, this report sets forth the analysis commissioned by the Panel.

That fundamental philosophy—the need for comprehensive, definitive, authoritative, articulate assessments and analyses of the potential domestic threats from terrorists on a continuing basis—has application to policymakers at all levels of government who may have any responsibility for addressing this issue.

Because the United States is very much an open society, it always will be vulnerable to terrorism. Nevertheless, it does not necessarily follow that, just because a particular locality or facility is vulnerable to terrorist attack at any point in time, a credible threat exists that can exploit that vulnerability. On the other hand, because of the potential catastrophic consequences of a successful incident perpetrated by a terrorist using a CBRN or other device that has the capability to cause “mass destruction” or “mass casualties,” agencies at all levels must be diligent in developing and assessing information on credible terrorists threats. Only through thorough, comprehensive, articulate, and continuing threat assessments and analyses will appropriate entities at the various levels of government be able to conduct the ensuing risk and vulnerability assessments, to develop and conduct activities to counter any credible threat, or to respond if an event occurs. A recent report of the United States General Accounting Office (GAO) entitled “Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks,”¹⁸² succinctly states:

A formal assessment of the domestic-origin threat, combined with existing assessments of the foreign-origin threat, would provide an authoritative, written, comprehensive, intelligence community view on specific chemical and biological terrorist threats. . . . Soundly performed risk assessments could help ensure that specific programs and related expenditures are justified and targeted according to the threat and risk of validated terrorist attack scenarios generated and assessed by a multidisciplinary team of experts.¹⁸³

The Panel has indicated its concern about a preoccupation with the “worst-case scenario,” and the attendant assumption that any lesser incident can be addressed

¹⁸²GAO/NSIAD-99-163, September 1999. The report is the fourteenth comprehensive analysis in an impressive list of reports on combating terrorism. The report and its related predecessors may be ordered from the GAO or accessed at its Website at: <http://www.gao.gov>

¹⁸³Ibid., at p. 3.

equally well by planning for the most catastrophic threat—ignoring the fact that higher-probability/lower-consequence attacks might present unique challenges of their own. As noted, this approach may not be the best means of setting budgetary priorities and allocating resources. The Panel is convinced, therefore, that more attention should be directed to assessments of the higher-probability, lower-consequence end of the potential terrorist threat spectrum—not at the expense of, but in addition to, assessments and analyses of the higher-consequence threat scenarios.

The Panel has been provided with the recent FBI report on “Project Megiddo,” and considers that effort to be clearly within the ambit of the foregoing assessment and recommendations. With respect to this topic, and other recommendations and initiatives addressed elsewhere in this report (notably on the subject of information sharing, which follows), the Panel is sensitive to the civil liberties implications and issues that may arise in the course of such activities. In the interest of sustaining the broadest-possible public support, the Panel urges officials at all levels of government to ensure that the civil liberties of our citizens are protected.

A National Strategy

Based on the Panel’s threat analysis, other relevant information that has come to its attention, and the knowledge and experience of its own members, the Panel is convinced that a national strategy to address the issues of domestic preparedness and response to terrorist incidents involving CBRN and other types of weapons is urgently needed.

Combating terrorism is clearly a national issue, but the responsibility for the domestic response to a terrorist CBRN incident is not necessarily—and will almost never be exclusively—a Federal one. For a response to those incidents described as “higher probability, lower consequence,” the Federal role is essentially one of providing support to state and local responders, fundamentally in reaction to a request for assistance. It is at the local and state level where the task of the initial response and, in almost every case, the primary responsibilities lie. It is only in the case of a catastrophic event—certainly possible, but of the “lower probability, higher consequence” type—that major responsibilities will reside at the Federal level. Federal involvement in an incident, which could include numerous civilian departments and agencies as well as military entities, will be defined by the nature and severity of the incident. As an example, in any case where an incident may be a terrorist act, the FBI will have an initial involvement in an investigation; if the incident is determined to be terrorism, the FBI will assume a leading role. Nevertheless, the Federal role will, in most cases, be supportive of state and local authorities, who traditionally have the fundamental responsibility for responding.

At the same time, the Federal government can and must provide significant support and assistance, both in preparation and in the event that such an incident actually occurs. There are considerable Federal resources that can be brought to bear in the areas of planning, training, standards, research and development, and equipment. Consequently, there needs to be a “Federal Government Strategy” component of the national strategy—one which clearly articulates Federal responsibilities, roles, and missions, and distinguishes those from state and local ones. Federal funding, and the activities and programs of a number of Federal agencies, to address domestic preparedness and response to such incidents, have increased dramatically in recent years, especially in the wake of the New York World Trade Center and Oklahoma City bombings, and the Aum Shinrikyo attack in the Tokyo subway system. Despite good intentions, and recent improvements in coordination and implementation, Federal programs addressing the issue appear, in many cases, to be fragmented, overlapping, lacking focus, and uncoordinated. The Federal component of a national strategy can help to reduce the redundancy, confusion, and fragmentation of current Federal efforts.

Representatives of the National Domestic Preparedness Office (NDPO)(which will be discussed in more detail below) have stated that the NDPO will develop a “national strategy” to address domestic preparedness issues. Given the fact that the responsibility for the initial and, in large measure, continuing response to *any* such incident will likely fall most heavily on the backs of state and local responders, the Panel suggests that a true national strategy must have a “bottom-up” approach—that it be developed in close consultation and collaboration with state and local officials, and the law enforcement and emergency response communities from across the country. This Panel can help to forge that collaboration. Moreover, any such national strategy—despite its “bottom-up” structure—must have the direct leadership, guidance, and imprimatur of the President. Only that way can a strategy have a truly national tenor; but more importantly, it will contain a comprehensive, articulate expression by the nation’s chief executive of the appropriateness of and distinctions between the Federal role and missions and those at state and local levels.

By focusing on higher-probability/lower-consequence threats, while recognizing and addressing concerns about lower-probability/higher-consequence events, a national strategy can lay the groundwork for assessing and monitoring the threat, and for making adjustments to response strategies as required. As has been argued elsewhere, too much of the Federal effort to date—even those programs that ostensibly are designed to enhance state and local response capabilities—has been predicated on the tacit assumption that preparing for the “worst case” will automatically encompass lesser threats. The foregoing analysis suggests otherwise, because the nature and scale of the consequences can vary so widely. This needs to be recognized and articulated at the national level.

The Panel is aware of the “Five-Year Interagency Counterterrorism and Technology Crime Plan”—recently released (September 1999) by the Attorney General of the United States, under the auspices of Department of Justice “lead agency” responsibility—as well as the interagency working group process dedicated to “WMD preparedness” within the National Security Council structure. Although significant steps in the right direction, the five-year plan does not equate to a comprehensive, fully coordinated national strategy—nor for that matter even the Federal government component of such a strategy—one with clear, concise, and unambiguous leadership and direction from the President in consultation with all who share responsibility for related Federal efforts.

The Panel also recommends that any such strategy include, within its purview, incidents involving more conventional weapons—such as conventional high-explosive or fabricated weapons (e.g., the type used in the Oklahoma City bombing)—that have the potential to cause significant casualties or physical damage; as well as incidents involving CBRN devices that may not be capable of producing “mass casualties” but that can, nevertheless, produce considerable fear, panic, or other major disruptions to the infrastructure or economy of the potential domestic target.

Considering the serious nature and potential consequences of any terrorist incident, the Panel is convinced that comprehensive public education and information programs must be developed, programs that will provide straight-forward, timely information and advice both prior to any terrorist incident and in the immediate aftermath of any attack. The national strategy should lay the groundwork for those programs.

Complexity of the Federal Structure

As indicated by the charts at Appendix A, which depict departments and agencies that have various programs addressing antiterrorism or counterterrorism, or both, the Federal bureaucratic structure is massive and complex. In various forums, state and local officials consistently express frustration in understanding where or how to enter this bureaucratic maze to obtain information, assistance, funding and support. In addition, Federal programs, especially those involving grants for funding or other resources, may be overly complicated, time consuming, and repetitive.

In recent months, the Federal Bureau of Investigation, pursuant to its “lead-agency” role (specified in the related Presidential Decision Directives) for crisis management for terrorism involving weapons of mass destruction, was directed by the Attorney General of the United States to organize, within its own resources, a National Domestic Preparedness Office (NDPO). The ostensible purpose of the NDPO is to serve as a focal point and “clearinghouse” for related preparedness information and for directing state and local entities to the appropriate agency of the Federal government

for obtaining additional information, assistance, and support. There has been discussion about the issue of whether the FBI is the appropriate location or whether the NDPO structure and approach is the most effective way to address the complexities of the Federal organization and programs designed to enhance domestic response capabilities. The Panel is convinced that the *concept* behind the NDPO is sound, and notes with interest that the Congress has recently authorized and appropriated funds (\$6 million) for the operation of the NDPO. While that authority will give the NDPO some wherewithal to operate and to hire persons from outside the FBI, the Panel has seen no specific direction to other Federal agencies to provide personnel or other resources to the NDPO, to assist in a concerted, well-coordinated effort.¹⁸⁴

Congressional Responsibilities

In much the same way that the complexity of the Federal bureaucratic structure is an obstacle—from a state and local perspective—to the provision of effective and efficient Federal assistance, it appears that the Congress has made most of its decisions for authority and funding to address domestic preparedness and response issues with little or no coordination. The various committees of the Congress continue to provide authority and money within the confines of each committee's jurisdiction over one or a limited number of Federal agencies and programs.¹⁸⁵ The Panel recommends, therefore, that the Congress consider forming an *ad hoc* Joint Special or Select Committee, composed of representatives of the various committees with oversight and funding responsibilities for these issues, and give such an entity the authority to make determinations that will result in more coherent efforts at the Federal level.

Information Sharing

State and local officials express the need for more “intelligence”, and for better information sharing among entities at all levels on potential terrorist threats. While the Panel is acutely aware of the need to protect classified national security information, and the sources and methods by which it may have been obtained, the Panel believes that more can and must be done to provide timely information—up, down, and laterally, at all levels of government—to those who need the information to provide effective deterrence, interdiction, protection, or response to potential

¹⁸⁴Some Federal agencies have, however, agreed to “detail” personnel to the NDPO.

¹⁸⁵With coordination from the Office of Management and Budget, and the National Security Council staff, the budget submission from the Executive “rolls up”—for display purposes—all related programs to combat terrorism, including those designed to strengthen domestic preparedness. Nevertheless, representatives of the Executive Branch must “market” those programs to the individual oversight and appropriating committees.

threats.¹⁸⁶ This may entail granting security clearances to additional officials at the state and local level. And as noted, the FBI report on Project Megiddo, and the briefings of its findings to state and local officials, is salutary.

The Panel is also aware of efforts in the Los Angeles area, in connection with the operational area terrorism working group (TWG) composed of LA county and municipal agencies, and the area's terrorism early warning (TEW) group; and of the multi-jurisdictional effort in New England aimed at collective information sharing of terrorist and other criminal threats. Those initiatives, as well as others that have been formed under the auspices of the FBI program to establish joint terrorism task forces, could be models for other regional programs, and for Federal interface with state and local jurisdictions, to improve and facilitate information sharing.

The Panel is convinced that efforts in this area must be based on the use of the most modern information technology available.

Definitions and Terms of Reference

Many of the terms and definitions that are essential to the instant discussion are ambiguous and confusing. The definition contained in the Nunn-Lugar-Domenici (NLD) Act—which directed specific actions in this arena, and which has been used as the basis for the development of others—defines “weapons of mass destruction” as

-any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release, dissemination, or impact of—
- (A) toxic or poisonous chemicals or their precursors;
 - (B) a disease organism; or
 - (C) radiation or radioactivity.

Nevertheless, 18 U.S.C, Section 2332a, which makes it a Federal crime—carrying a maximum penalty of death or life imprisonment—to use “certain weapons of mass destruction,” includes in its definition of such weapons not only definitional elements substantially similar to those contained in NLD, but also “any destructive device as defined in section 921” of that title, which includes

- (A) any explosive, incendiary, or poison gas
 - (i) bomb,
 - (ii) grenade,

¹⁸⁶From discussions at Panel meetings, and from comments that have been made by officials in other forums, information-sharing apparently has been improving in recent months.

- (iii) rocket having a propellant charge of more than four ounces,
- (iv) missile having an explosive or incendiary charge of more than one-quarter ounce,
- (v) mine, or
- (vi) device similar to any of the devices described in the preceding clauses;

(B) any type of weapon (other than a shotgun or a shotgun shell which . . . is generally recognized as particularly suitable for sporting purposes) by whatever name known which will, or which may be readily converted to, expel a projectile by the action of an explosive or other propellant, and which has any barrel with a bore of more than one-half inch in diameter; and

(C) any combination of parts either designed or intended for use in converting any device into any destructive device described in subparagraph (A) or (B) and from any combination of parts either designed or intended for use in converting any which a destructive device may be readily assembled.

While the Title 18 definition is more inclusive in terms of certain conventional explosive devices that do not fit within the traditional categories of chemical, biological, radiological or other nuclear devices, both definitions beg the question of what constitutes a “significant number of people.” A single CBRN or conventional weapon that is neither intended nor has the capability “to cause death or serious bodily injury to a significant number of people” is not included within the actions proscribed; but could, either alone or in a series of actual or threatened events create panic or other significant disruptions.

A recent GAO report on Combating Terrorism flatly states, “no federal agency has defined what constitutes ‘mass casualties’.”¹⁸⁷

And several Federal agencies (e.g., the FBI and the Department of Defense) have their own definition of terrorism.

The Panel recommends that there be a revision and codification of universal, unambiguous, and easily understandable definitions of the various terms used in this context.

¹⁸⁷GAO/NSIAD-99-163, at p. 6. The Department of Health and Human Services has arbitrarily determined that it will use the figure of 1,000 casualties for planning purposes in establishing its Metropolitan Medical Response System.

Standards, and Research, Development, Test and Evaluation

The Panel will devote significant attention during its current fiscal year activities to standards, especially for training and equipment. Given the likelihood that multiple jurisdictions in one or more states, as well as agencies of the Federal government, will be involved in any serious terrorist incident, it will be critical that every responder in a particular emergency function be trained to the same standard. The types of equipment used by response entities—detection devices, personal protective equipment, and communications equipment—must be compatible and inter-operable. The Panel commends the efforts being undertaken by the Interagency Board (IAB) for Equipment Standardization and InterOperability—composed of representatives of various Federal, state, and local entities, as well as some nongovernmental professional organizations—in its attempt to develop a national “standardized equipment list,” to provide responders at all levels with a resource with which to make better-informed decisions about the selection and acquisition of equipment. Such efforts are a positive step toward ensuring better compatibility and inter-operability of equipment among potential responders.

Local responders continue to express frustration at the vast array of devices and equipment available from industry that may have application for domestic preparedness for terrorist attacks. At the same time, some have expressed displeasure at the fact that certain items, previously purchased by local responders, do not measure up to the claims of manufacturers.

In order to develop and maintain operationally effective standards for equipment compatibility and inter-operability, the Panel has determined that more research and development is required to meet local responder needs. Given the significant costs associated with sophisticated equipment, such as certain chemical and biological detection devices, emphasis should be placed on the development of multi-purpose pieces of equipment, which can be used not only in the terrorism context, but which will also have application in other fields, such as the detection of naturally transmitted infectious diseases.

To help to reassure responders that the equipment that is being used is in fact capable of doing what it is designed to do, it is likely that an ambitious program of independent testing and evaluation will have to be undertaken. The Panel recognizes that any such program will likely have to be conducted—because of its national implications—under Federal sponsorship; and will require the addition or reallocation

of significant resources.¹⁸⁸ For reasons that are self-evident, local responders are insisting that testing be done with “live” agents.

The Panel is aware of a project being undertaken by the National Institute of Justice (NIJ), an agency the U.S. Department of Justice’s Office of Justice Programs, which is ultimately designed to be a “consumer report” catalogue of available equipment that meets certain listed standards.

The Issue of “Who’s in Charge”

Increasingly, the Panel and its supporting staff have heard the question raised, “When an incident occurs, who’s in charge?” The Panel has initially concluded that there is no single answer to the question—a determination will likely have to be made on a case-by-case basis, taking into consideration, among other factors, the nature of the incident; the perpetrator source; the actual or potential consequences immediately and over time; and the then-current capabilities for effective response at various levels. In every actual terrorist incident, non-Federal local responders will always be in charge initially, unless of course the incident occurs on a military or other Federal reservation which has its own response capability. Even in the latter case, an incident may be of such proportions that non-Federal responders may be just as engaged, if not more so, as the Federal responders on the government enclave may be.

The issue may be compounded by the fact that certain responsibilities at the Federal level have been bifurcated. Under the related Presidential Decision Directives, the Federal Bureau of Investigation has the “lead agency” responsibility for “crisis management,” while the Federal Emergency Management Agency is “lead” for “consequence management.” The “five-year plan,” recently released by the Department of Justice, acknowledges that

there is often no clear point in time when resolution of a terrorist incident moves from the crisis to the consequence management stage. Indeed, these phases may occur simultaneously or, in some cases, the consequence management phase may actually precede the identification of a terrorist event.¹⁸⁹

At this point, the Panel reserves judgment on the issue of whether changes should be made in Federal “lead agency” responsibilities, but will include the issue as a “thread”

¹⁸⁸At a recent conference of the IAB, it was noted by an official from the National Institute of Occupational Safety and Health that there are some 7,000 respiratory devices—mostly protective masks—that have potential application to a response to a chemical or biological incident, and that to test a device properly will take form four to six weeks—per device.

¹⁸⁹ “Five-Year Interagency Counterterrorism and Technology Crime Plan,” p. 21.

which runs throughout its consideration of many aspects of preparations for response at all levels.

Many local responders are also justifiably concerned that Federal agents will assume command following almost any terrorist attack. In more discrete terms, local responders express concern that, having established an excellent relationship with Federal agencies at the local or regional level, when the “planes from Washington” start to arrive, local agencies will be faced with an entirely new team—one which may set different ground rules than those to which local responders and their local or regional Federal counterparts have previously agreed. Nevertheless, in various forums, local responders have noted improvement in this area during the past year, especially in the out-reach and bridge-building initiatives of the Federal Bureau of Investigation.

When an actual incident is or becomes one that requires a major Federal response, to the point that a Federal entity may have to “take command” of an operation, the issue of when and how an appropriate “hand-off” from local to Federal authorities takes place continues to be a significant one for resolution—sooner rather than later. While the Panel is aware that the issue is being addressed in inter-agency and inter-governmental agreements, and is being included in a number of exercises, efforts by entities at all levels must, in the opinion of the Panel, be accelerated to provide the necessary agreed-on templates for such hand-offs to take place. This issue, especially any specific agreements that may be reached between Federal and local officials, should always be included in related training, exercises, and other appropriate forums, to ensure that any such transition will be as smooth as possible in an actual operation.

Summary

Regardless of the level of consequences from a terrorist event, we must as a nation ensure that we have programs that will provide the capabilities for local, state, and Federal authorities to respond effectively. Existing local, state and national response systems, used for a variety of emergency situations, may provide a solid foundation for preparedness for a terrorist incident. Managing the consequences of any type or size terrorist event may require, however, a somewhat different approach on the part of state and local officials and their Federal partners. Thus, we must ensure a basic ability for the three levels of government to integrate activities laterally and vertically in the development of policy and operational guidelines.