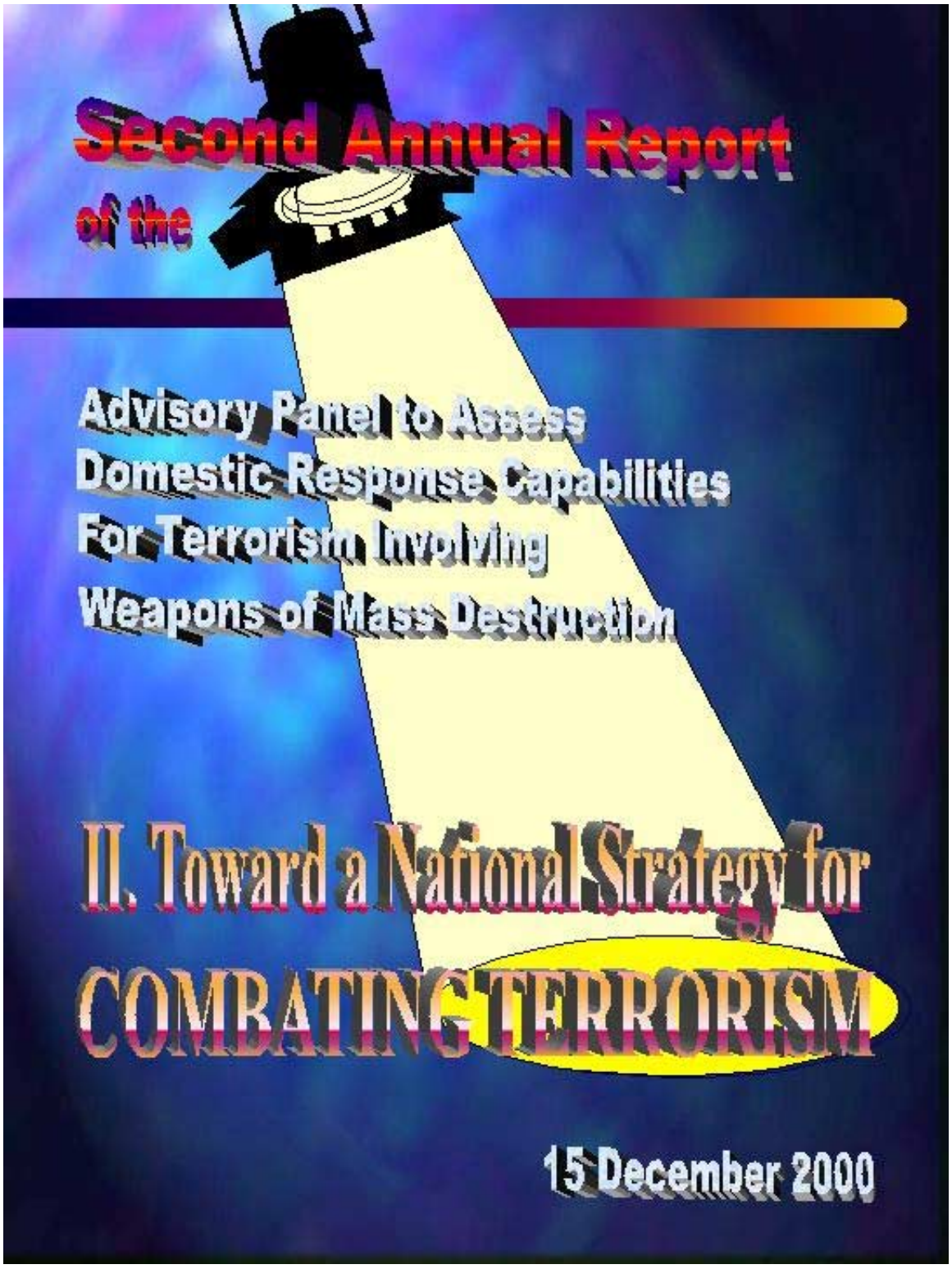

Second Annual Report
of the
Advisory Panel to Assess
Domestic Response Capabilities
For Terrorism Involving
Weapons of Mass Destruction
II. Toward a National Strategy for
COMBATING TERRORISM
15 December 2000

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

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

Second Annual Report to

The President and The Congress

Of the

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

II. TOWARD A NATIONAL STRATEGY FOR COMBATING TERRORISM

15 December 2000

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

December 15, 2000

To Our Readers:

I am pleased to provide the Second Annual Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, as our Congressional mandate requires.

Contemplating the specter of terrorism in this country is a sobering—but critically necessary—responsibility of government officials at all levels. It is a truly "national" issue that requires synchronization of our efforts—"vertically" among the federal, state, and local levels, and "horizontally" among the functional constituent stakeholders. The individual capabilities of all critical elements must be brought to bear in a much more coherent way than is now the case. That fundamental tenet underlies our work over the last two years.

We are impelled by the stark realization that a terrorist attack on some level inside our borders is inevitable and the United States must be ready. We are similarly convinced, however, that much of the legitimate fear associated with the prospect of a terrorist attack can be substantially reduced.

Improving our ability to address the threat and reducing the fear of citizens and government leaders is possible if—and only if—we are willing to take bold action as a nation. Specifically, we must:

- craft a truly "national" strategy to address the threat of domestic terrorism—conventional, cyber, chemical, biological, radiological and nuclear—from the perspectives of deterrence, prevention, preparedness and response;

- empower a senior authority to be in charge of our overall planning and preparation in the Federal Executive Branch, with special emphasis on preserving our civil liberties in a time of emergency;

- consolidate the Congressional approach to legislation governing domestic preparedness for such attacks;

- concentrate much more serious attention on state and local concerns and capabilities; and

- strengthen functional capabilities across all levels of government for intelligence collection and information sharing; planning; training, equipping and exercising; research and development; health and medical; and across all first responder stakeholders—fire, law enforcement, emergency medical services and emergency management.

These five imperatives represent the major themes in this report. We stress in the strongest terms that their implementation must *always* hold in strict regard the preservation of our Constitution and the complete protection of our civil liberties. We steadfastly adhere to the bedrock principle that these considerations must always transcend what might be more efficient or expedient.

It is clear to us that our nation collectively will have to make some significant resource commitments and overcome daunting technological challenges if we are successfully to confront this threat in all dimensions. I submit, however, that our most imposing challenge centers on policy and whether we have the collective fortitude to forge change, both in organization as well as process. We are convinced the changes we recommend are essential to ensure the safety and security of our nation.

Respectfully,

James S. Gilmore, III
Governor of Virginia
Chairman

Please address comments or questions to:

RAND

1200 South Hayes Street, Arlington, Virginia 22202-5050 Telephone 703-413-1100 FAX 703-413-8111

The Federally-Funded Research and Development Center providing support to the Advisory Panel

CONTENTS

Executive Summary

We have been fortunate as a nation. The terrorist incidents in this country—however tragic—have occurred so rarely that the foundations of our society or our form of government have not been threatened. Nevertheless, the potential for terrorist attacks inside the borders of the United States is a serious emerging threat. There is no guarantee that our comparatively secure domestic sanctuary will always remain so. Because the stakes are so high, our nation's leaders must take seriously the possibility of an escalation of terrorist violence against the homeland.

The continuing challenge for the United States is first to deter and, failing that, to detect and interdict terrorists before they strike. Should an attack occur, local, State, and Federal authorities must be prepared to respond and mitigate the consequences of the attack.

To prepare to manage the consequences of such attacks effectively, the United States needs changes in the relationships among all levels of government. Our ability to respond cannot depend on a single level or agency of government. Rather we need a *national* approach, one that recognizes the unique individual skills that communities, States, and the Federal government possess and that, collectively, will give us the "total package" needed to address all aspects of terrorism.

The Advisory Panel produced a comprehensive assessment, in its first report, of the terrorist threat. The Panel stands by its conclusions from one year ago.

In its second year, the Advisory Panel shifted its emphasis from threat assessment to broad program assessment. The Advisory Panel addressed specific programs for combating terrorism and larger questions of national strategy and Federal organization. While the Advisory Panel found much to commend, it also found problems at all levels of government and in virtually every functional discipline relevant to combating terrorism. The Panel believes these problems are particularly acute at high levels of the Federal Executive

Branch. Hence, the present report highlights the related issues of national strategy and Federal organization, and recommends solutions for these and other problems.

Finding 1: The United States has no coherent, functional national strategy for combating terrorism.

The United States needs a functional, coherent national strategy for domestic preparedness against terrorism. The nation has a loosely coupled set of plans and specific programs that aim, individually, to achieve certain specific preparedness objectives. The Executive Branch portrays as its strategy a compilation of broad policy statements, and various plans and programs already under way. Many programs have resulted from specific Congressional earmarks in various appropriations bills and did not originate in Executive Branch budget requests; they are the initiatives of activist legislators. Although Federal agencies are administering programs assigned to them, the Executive Branch has not articulated a broad functional national strategy that would synchronize the existing programs and identify future program priorities needed to achieve national objectives for domestic preparedness for terrorism. Given the structure of our national government, only the Executive Branch can produce such a national strategy.

Recommendation 1: The next President should develop and present to the Congress a national strategy for combating terrorism within one year of assuming office.

A national strategy is a high-level statement of national objectives coupled logically to a statement of the means that will be used to achieve these objectives. In a coherent strategy, program details are analytically derived from the statement of goals. The next Administration should begin a process of developing a national strategy by a thoughtful articulation of national goals, encompassing deterrence, prevention, preparedness, and response.

Ends. The first step in developing a coherent national strategy is for the Executive Branch to define a meaningful, measurable expression of what it is trying to achieve in combating terrorism. To date, the Federal government's goals have been expressed primarily in terms of program execution. Rather, the national strategy must express goals in terms of the "end state" toward which the program strives. Since there exists no ready-made measure of a country's preparedness for terrorism (especially domestically), the Executive Branch must

develop objective measurements for its program to combat terrorism, to track its progress, to determine priorities and appropriate funding levels, and to know when the desired "end state" has been achieved.

Means. With meaningful objectives, logical priorities and appropriate policy prescriptions can be developed. That is the essence of any coherent strategy. Setting priorities is essential and can only be done after specific objectives have been clearly defined. For instance, should the nation seek a higher level of preparedness for its large urban centers than for its rural areas and, if so, how much higher? In the broad area of terrorism preparedness, what should be the relative importance of preparing for conventional terrorism, radiological incidents, chemical weapons, or biological weapons? With respect to biological weapons, which pathogens deserve priority? What priority and commensurate resources need to be devoted to defending against cyber attacks? A proper national strategy will provide a clear answer to these and many other questions. With these answers in hand it will be possible to design and manage an appropriate set of programs. The country is at a disadvantage, of course, in that a large number of programs have already been established and may have to be reconfigured—an inevitable consequence of their ad hoc origins.

Essential Characteristics of a Comprehensive Functional Strategy for Combating Terrorism

NATIONAL IN SCOPE, NOT JUST FEDERAL

APPROPRIATELY RESOURCED AND BASED ON MEASURABLE PERFORMANCE OBJECTIVES

FOCUSED ON THE FULL RANGE OF DETERRENCE, PREVENTION, PREPAREDNESS, AND RESPONSE ACROSS THE SPECTRUM OF THREATS—DOMESTIC AND INTERNATIONAL

FOR DOMESTIC PROGRAMS, BUILT ON REQUIREMENTS FROM AND FULLY COORDINATED WITH RELEVANT LOCAL, STATE, AND FEDERAL AUTHORITIES

Finding 2: The organization of the Federal government's programs for combating terrorism is fragmented, uncoordinated, and politically unaccountable.

The lack of a national strategy results in part from the fragmentation of Executive Branch programs for combating terrorism. These programs cross an extraordinary number of jurisdictions and substantive domains: national security, law enforcement, intelligence, emergency management, fire protection, public health, medical care, as well as parts of the private sector.

No one, at any level, is "in charge" of all relevant capabilities, most of which are not dedicated exclusively to combating terrorism. The lack of a national strategy is inextricably linked to the fact that no entity has the authority to direct all of the entities that may be engaged. At the Federal level, no entity has the authority even to direct the coordination of relevant Federal efforts.

Recommendation 2: The next President should establish a National Office for Combating Terrorism in the Executive Office of the President, and should seek a statutory basis for this office.

The office should have a broad and comprehensive scope, with responsibility for the full range of deterring, preventing, preparing for, and responding to international as well as domestic terrorism. The director of this office should be the principal spokesman of the Executive Branch on all matters related to Federal programs for combating terrorism and should be appointed by the President and confirmed by the Senate. The office should have a substantial and professional staff, drawn from existing National Security Council offices and other relevant agencies. It should have at least five major sections, each headed by an Assistant Director:

1. Domestic Preparedness Programs
2. Intelligence
3. Health and Medical Programs
4. Research, Development, Test, and Evaluation (RDT&E), and National Standards
5. Management and Budget

The National Office for Combating Terrorism should exercise program and budget authority over Federal efforts to combat terrorism. It should have the authority to conduct a review of Federal agency programs and budgets to ensure compliance with the priorities established in the national strategy, as well as the elimination of conflicts and unnecessary duplication among agencies. The National Office should administer a budget certification/decertification process with the authority to determine whether an agency's budget complies with the national strategy and to appeal ultimately to the President to resolve disputes.

In addition to developing and overseeing the national strategy, the National Office for Combating Terrorism should oversee terrorism-related intelligence activities. The office should coordinate Federal programs designed to assist response entities at the local and State levels, especially for planning, training, exercises, and equipment. The office should provide direction and priorities for research and development, and related test and evaluation (RDT&E) for combating terrorism, as well as for developing nationally recognized standards for equipment and laboratory protocols and techniques. It should coordinate programs designed to enhance the capabilities of and coordination among the various health and medical entities at all levels.

The National Office for Combating Terrorism should not be an operational entity in the sense of exerting direct control over Federal assets in operations to combat terrorism.

Finally, the director of the National Office should establish an Advisory Board for Domestic Programs to assist in providing broad strategic guidance and to serve as part of the approval process for the domestic portion of strategy, plans, and programs of the National Office for Combating Terrorism. This board should be composed of one or more sitting State governors, mayors of several U.S. cities, the heads of several major professional organizations, and nationally recognized subject matter experts in combating terrorism, in addition to senior representatives of the major Federal entities that have responsibility for combating terrorism. The President and the Congress should each appoint members to this board.

Finding 3: The Congress shares responsibility for the inadequate coordination of programs to combat terrorism.

The Congress's strong interest in, and commitment to, U.S. efforts to combat terrorism is readily apparent. The Congress took the initiative in 1995 to improve

the nation's domestic preparedness against terrorism. But the Congress has also contributed to the Executive Branch's problems. Over the past five years, there have been a half-dozen Congressional attempts to reorganize the Executive Branch's efforts to combat terrorism, all of which failed. None enjoyed the support of the Executive Branch. At least 11 full committees in the Senate and 14 full committees in the House—as well as their numerous subcommittees—claim oversight or some responsibility for various U.S. programs for combating terrorism. Earmarks in appropriations bills created many of the Federal government's specific domestic preparedness programs without authorizing legislation or oversight. The rapidly growing U.S. budget for combating terrorism is now laced with such earmarks, which have proliferated in the absence of an Executive Branch strategy. The Executive Branch cannot successfully coordinate its programs for combating terrorism alone. Congress must better organize itself and exercise much greater discipline.

Recommendation 3: The Congress should consolidate its authority over programs for combating terrorism into a Special Committee for Combating Terrorism—either a joint committee between the Houses or separate committees in each House—and Congressional leadership should instruct all other committees to respect the authority of this new committee and to conform strictly to authorizing legislation.

The creation of a new joint committee or separate committees in each House is necessary to improve the nation's efforts to fight terrorism. The committee should have a substantial standing staff. The new National Office for Combating Terrorism must establish a close working relationship with the committee, and propose comprehensive and coherent programs and budget requests in support of the new national strategy. The new joint or separate committee should have the authority to dispose of the Executive Branch request and to oversee the execution of programs that it authorizes. For this to work, other Congressional authorizing committees with an interest in programs for combating terrorism must recognize the concurrent, consolidated authority of the joint or separate committee; and relevant appropriations committees must exercise restraint and respect the authorizing legislation of the new structure. We recognize that this task is no less daunting than the Executive Branch reorganization that we propose above, but it is no less needed.

Finding 4: The Executive Branch and the Congress have not paid sufficient attention to State and local capabilities for combating terrorism and have not devoted sufficient resources to augment these capabilities to enhance the preparedness of the nation as a whole.

The foundation of the nation's domestic preparedness for terrorism is the network of emergency response capabilities and disaster management systems provided by State and local governments. "Local" response personnel—community and State law enforcement officers, firefighters, emergency medical technicians, hospital emergency personnel, public health officials, and emergency managers—will be the "first responders" to virtually any terrorist attack anywhere in the nation. Federal resources may not arrive for many hours—if not days—after the attack. A disproportionately small amount of the total funds appropriated for combating terrorism is being allocated to provide direct or indirect assistance to State and local response efforts. This level of Federal funding for non-Federal capabilities is not commensurate with the importance that State and local capabilities will have in any operational response to a major terrorist attack inside our borders.

Any coherent national strategy for combating terrorism domestically must recognize the critical need to build on the nation's existing emergency response and management systems for the pragmatic reasons of viability and cost-effectiveness.

Recommendation 4: The Executive Branch should establish a strong institutional mechanism for ensuring the participation of high-level State and local officials in the development and implementation of a national strategy for terrorism preparedness.

To be consistent with the Federal structure of our government, the President should work in closer partnership with State and local governments as they collectively strive to achieve higher levels of domestic preparedness for terrorism. The domestic portion of a national strategy for combating terrorism should emphasize programs and initiatives that build appropriately on existing State and local capabilities for other emergencies and disasters. The Executive Branch, therefore, should develop the national strategy in close partnership with high-level State and local officials drawn from key professional communities: elected officials, law enforcement, fire protection, emergency medical technicians, public

health officials, hospital medical care providers, and emergency managers. State and local officials should, in particular, have substantial responsibility for the detailed design and oversight of the Federal training, equipment, and exercise programs. The Advisory Board for Domestic Programs, proposed earlier, should provide advice for these functions, augmented as necessary by State and local representatives assigned to the National Office for Combating Terrorism.

Finding 5: Federal programs for domestic preparedness to combat terrorism lack clear priorities and are deficient in numerous specific areas.

We have a number of recommendations about selected aspects of current U.S. programs for domestic preparedness to combat terrorism. The lack of clear priorities is an obvious byproduct of the lack of a strategy. Thus, many of our specific recommendations reflect criticisms that are subordinate to our macro-critique that the United States lacks a coherent national strategy. We recognize the problem of offering detailed programmatic recommendations in advance of a national strategy. Through its deliberations, the Advisory Panel has, nevertheless, reached consensus on a number of specific findings and recommendations, summarized below and detailed in the full report.

Specific Functional Recommendations.

Our focus continues to be on the needs of local and State response entities. "Local" response entities—law enforcement, fire service, emergency medical technicians, hospital emergency personnel, public health officials, and emergency managers—will *always* be the "first response," and conceivably the only response. When entities at various levels of government are engaged, the responsibilities of all entities and lines of authority must be clear.

1. *Collecting Intelligence, Assessing Threats, and Sharing Information*. The National Office for Combating Terrorism should foster the development of a consolidated all-source analysis and assessment capability that would provide various response entities as well as policymakers with continuing analysis of potential threats and broad threat assessment input into the development of the annual national strategy. That capability should be augmented by improved human intelligence collection abroad, more effective domestic activities with a

thorough review of various Federal guidelines, and reasonable restrictions on acquisition of CBRN precursors or equipment. The National Office should also foster enhancements in measurement and signature intelligence, forensics, and indications and warning capabilities. To promote the broadest possible dissemination of useful, timely (and if necessary, classified) information, the National Office should also oversee the development and implementation of a protected, Internet-based single-source web page system, linking appropriate sources of information and databases on combating terrorism across all relevant functional disciplines.

2. *Operational Coordination*. The National Office for Combating Terrorism should encourage Governors to designate State emergency management entities as domestic preparedness focal points for coordination with the Federal government. The National Office should identify and promote the establishment of single-source, "all hazards" planning documents, standardized Incident Command and Unified Command Systems, and other model programs for use in the full range of emergency contingencies, including terrorism. Adherence to these systems should become a requirement of Federal preparedness assistance.

3. *Training, Equipping, and Exercising*. The National Office for Combating Terrorism should develop and manage a comprehensive national plan for Federal assistance to State and local agencies for training and equipment and the conduct of exercises, including the promulgation of standards in each area. The National Office should consult closely with State and local stakeholders in the development of this national plan. Federal resources to support the plan should be allocated according to the goals and objectives specified in the national strategy, with State and local entities also providing resources to support its implementation.

4. *Health and Medical Considerations*. The National Office for Combating Terrorism should reevaluate the current U.S. approach to providing public health and medical care in response to acts of terrorism, especially possible mass casualty incidents and most particularly bioterrorism. The key issues are insufficient education and training in terrorism-related subjects, minimum capabilities in surge capacity and in treatment facilities, and clear standards and protocols for laboratories and other activities, and vaccine programs. A robust public health infrastructure is necessary to ensure an effective response to terrorist attacks, especially those involving biologic agents. After consultation with public health and medical care entities, the National Office should oversee

the establishment of financial incentives coupled with standards and certification requirements that will, over time, encourage the health and medical sector to build and maintain required capabilities. In addition, Federal, State, and local governments should clarify legal and regulatory authorities for quarantine, vaccinations, and other prescriptive measures.

5. *Research and Development, and National Standards*. The National Office for Combating Terrorism should establish a clear set of priorities for research and development for combating terrorism, including long-range programs. Priorities for targeted research should be responder personnel protective equipment; medical surveillance, identification, and forensics; improved sensor and rapid readout capability; vaccines and antidotes; and communications interoperability. The National Office must also coordinate the development of nationally recognized standards for equipment, training, and laboratory protocols and techniques, with the ultimate objective being official certification.

6. Providing Cyber Security Against Terrorism. Cyber attacks inside the United States could have "mass disruptive," even if not "mass destructive" or "mass casualty" consequences. During the coming year, the Advisory Panel will focus on specific aspects of critical infrastructure protection (CIP), as they relate to the potential for terrorist attacks. In our discussions thus far, we have identified several areas for further deliberation, including CIP policy oversight; standards; alert, warning, and response; liability and other legal issues, and CIP research. We will make specific policy recommendations in our next report.

Chapter One

Forging a National Strategy

We have been fortunate as a nation. The terrorist incidents in this country—however tragic—have occurred so rarely that the foundations of our society or our form of government have not been threatened. Nevertheless, the potential for terrorist attacks inside the borders of the United States is a serious emerging threat. There is no guarantee that our comparatively secure domestic sanctuary will always remain so. Because the stakes are so high, our nation's leaders must take seriously the possibility of an escalation of terrorist violence against the homeland.

The continuing challenge for the United States is first to deter and, failing that, to detect and interdict terrorists before they strike. Should an attack occur, local, State, and Federal authorities must be prepared to respond and mitigate the consequences of the attack.

To prepare to manage the consequences of such attacks effectively, the United States needs changes in the relationships among all levels of government. Our ability to respond cannot depend on a single level or agency of government. Rather we need a *national* approach, one that recognizes the unique individual skills that communities, States, and the Federal government possess and that, collectively, will give us the "total package" needed to address all aspects of terrorism.

The Advisory Panel produced a comprehensive assessment, in its first report, of the terrorist threat, with a focus on chemical, biological, radiological, and nuclear (CBRN) weapons. There we said:

> The Panel concludes that the Nation must be prepared for the entire spectrum of potential terrorist threats – both the unprecedented higher-consequence attack, as well as the historically more frequent, lesser-consequence terrorist attack, which the Panel believes is more likely in the near term. Conventional explosives, traditionally a favorite tool of the terrorist, will likely remain the terrorist weapon of choice in the near term as well. Whether smaller-scale CBRN or conventional, any such lower-consequence event—at least in terms of casualties or destruction—could, nevertheless, accomplish one or more terrorist objectives: exhausting response capabilities, instilling fear, undermining government credibility, or provoking an overreaction by the

> government. With that in mind, the Panel's report urges a more balanced approach, so that not only higher-consequence scenarios will be considered, but that increasing attention must now also be paid to the historically more frequent, more probable, lesser-consequence attack, especially in terms of policy implications for budget priorities or the allocation of other resources, to optimize local response capabilities. A singular focus on preparing for an event potentially affecting thousands or tens of thousands may result in a smaller, but nevertheless lethal attack involving dozens failing to receive an appropriate response in the first critical minutes and hours.
>
> While noting that the technology currently exists that would allow terrorists to produce one of several lethal CBRN weapons, the report also describes the current difficulties in acquiring or developing and in maintaining, handling, testing, transporting, and delivering a device that truly has the capability to cause "mass casualties."[1]

The Panel stands by its conclusions from one year ago.

In its second year, the Advisory Panel shifted its emphasis from threat assessment to broad program assessment. While the Advisory Panel found much to commend, it also found problems at all levels of government and in virtually every functional discipline relevant to combating terrorism. The Panel believes these problems are particularly acute at high levels of the Federal Executive Branch. Hence, the present report highlights the related issues of national strategy and Federal organization, and recommends solutions for these and other problems.

The United States needs a functional, coherent national strategy for domestic preparedness against terrorism. A national strategy is a high-level statement of national objectives coupled logically to a statement of the means to be used to achieve these objectives. In a coherent strategy, programmatic details are analytically derived from the statement of goals. Currently, there is no overarching statement of what the United States is trying to achieve with its program to combat terrorism . Goals must be expressed in terms of results, not process. Government officials currently speak of terrorism preparedness goals in terms of program execution. Administrative measurements of program implementation are not meaningful for the purposes of strategic management and obscure the more fundamental and important question: To what end are these programs being implemented?

Instead of a national strategy, the nation has a loosely coupled set of plans and specific programs that aim, individually, to achieve certain particular preparedness objectives. Senior U.S. officials state that several official broad policy and planning documents that have been published in recent years—Presidential Decision Directives 39 and 62, the

[1] *The First Annual Report to the President and the Congress: I. Assessing the Threat* (the "First Report"), p. viii. The First Report was delivered on December 15, 1999. For a complete copy of the report, see http://www.rand.org/organization/nsrd/terrpanel/

Attorney General's 1999 Five-Year Interagency Counterterrorism and Technology Crime Plan, and the most recent Annual Report to Congress on Combating Terrorism[2]—taken as a whole, constitute a national strategy. These documents describe plans, the compilation of various programs already under way, and some objectives; but they do not either individually or collectively constitute a national strategy.

Many of the current programs have resulted from specific Congressional earmarks in various appropriations bills and did not originate in Executive Branch budget requests. They are the initiatives of concerned and proactive Senators and Representatives.

Although Executive Branch agencies are administering programs assigned to them in the appropriations legislation, the Executive Branch has not articulated a broad national strategy that would synchronize the existing programs or identify future program priorities needed to achieve national objectives for domestic preparedness for terrorism. Given the structure of our national government, only the Executive Branch can produce such a national strategy.

The Advisory Panel therefore recommends that the next President develop and present to the Congress a national strategy for combating terrorism within one year of assuming office.[3] The next Administration should begin this process of developing a national strategy by a thoughtful articulation of national goals (ends) of the program, focusing on results rather than process. The structure and specifics of the national program should derive logically and transparently from the goals, not the other way around.

Basic Assumptions

The Advisory Panel agreed on several basic assumptions to guide its approach to strategy development.

First, "local" response entities—law enforcement, fire service, emergency medical technicians, hospital emergency personnel, public health officials, and emergency managers, in any of several combinations depending on the nature of the attack—will *always* be the "first "—and conceivably only—response. "Local" entities in this context can include elements of incorporated and unincorporated municipalities, counties, and State organizations. In every case, some combination of those entities will inevitably be involved.

Second, in the event of a *major* terrorist attack, however defined—number of fatalities or total casualties, the point at which local and State capabilities are overwhelmed, or some

[2]The Office of Management and Budget, *Annual Report to Congress on Combating Terrorism, Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection*, May 18, 2000.

[3] The Advisory Panel made essentially the same recommendation in its first annual report: "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." First Report, p. 54.

other measure—no single jurisdiction is likely to be capable of responding to such an attack without outside assistance. This assumption is critical to understanding the need for mutual aid agreements and coordinated operations.

Third—and perhaps most important—there are existing emergency response and management capabilities, developed over many years, for responses to natural disasters, disease outbreaks, and accidents. Those capabilities can and should be used as a base for enhancing our domestic capability for response to a terrorist attack. We are not, as some have asserted, "totally unprepared" for a major terrorist attack, even with a biological weapon. We can strengthen existing capabilities, without buying duplicative, cost-prohibitive capabilities exclusively dedicated to terrorism. Similarly, our capabilities to deter, prevent, or respond to a terrorist attack correspondingly enhance capabilities against attacks from nation-states.

Essential Characteristics of a Comprehensive Functional Strategy for Combating Terrorism

NATIONAL IN SCOPE, NOT JUST FEDERAL

APPROPRIATELY RESOURCED AND BASED ON MEASURABLE PERFORMANCE OBJECTIVES

FOCUSED ON THE FULL RANGE OF DETERRENCE, PREVENTION, PREPAREDNESS, AND RESPONSE ACROSS THE SPECTRUM OF THREATS—DOMESTIC AND INTERNATIONAL

FOR DOMESTIC PROGRAMS, BUILT UPON REQUIREMENTS FROM AND FULLY COORDINATED WITH RELEVANT LOCAL, STATE, AND FEDERAL AUTHORITIES

The national strategy should be geographically and functionally comprehensive. It should address both international and domestic terrorism. The distinction between terrorism outside the borders of the United States and domestic terrorist threats is eroding. International terrorism crosses borders easily and may directly affect the American homeland. This was evident in the New York World Trade Center bombing in 1993, and more recently in the activities around the turn of the century, especially with the arrests of Ahmed Ressam in Washington State, and Lucia Garofalo and Bouabide Chamchi in Vermont. The terrorist bombings of the U.S. garrison at Khobar Towers, Saudi Arabia, the two U.S. embassies in East Africa, and the recent USS *Cole* incident, also illustrate the reach of terrorists against U.S. interests and the profound domestic implications they pose.

To be functionally comprehensive, the national strategy should address the full spectrum of the nation's efforts against terrorism: intelligence, deterrence, prevention, investigation, prosecution, preemption, crisis management, and consequence management. As the Advisory Panel recognized in its first report, our nation's highest goal must be the deterrence and prevention of terrorism. The United States cannot, however, prevent all terrorist attacks. When deterrence and prevention fail, the nation must respond effectively to terrorism, whether to resolve an ongoing incident, mitigate its consequences, identify the perpetrators, and prosecute or retaliate as appropriate. The

national strategy should deal with all aspects of combating terrorism and must carefully weigh their relative importance for the purpose of allocating resources among them.

The national strategy should apply to the nation as a whole, not just the Federal Executive Branch. The Federal government should lead a strategic planning process that involves States and communities as essential and equal partners.[4]

The national strategy must be appropriately resourced, by all levels of government, to provide a reasonable opportunity to achieve its successful implementation. At the Federal level, that will require a closer relationship between the Executive and Legislative Branches. Nationally, that will require better coordination with State and local governments.

Identifying the Ends of Strategy: National Goals

The first step in developing a coherent national strategy is for the Executive Branch to define some meaningful, measurable expression of what it is trying to achieve in combating terrorism. The Federal government's goals are currently expressed primarily in terms of program execution. Administrative measurements alone do not foster effective management of a national program.

The national strategy must express preparedness goals in terms of an "end state" toward which the program strives. Since there exists no ready-made measurement of a country's preparedness for terrorism, especially domestically, the Executive Branch must develop objective measurements for its program to combat terrorism, to track its progress, to determine priorities and appropriate funding levels, and to know when the desired "end state" has been achieved.

The nation's strategy for combating terrorism requires results-based goals for three reasons. First, the programs need an end-state goal. Elected and appointed officials from Federal, State, and local governments must be able to allocate resources to specific geographic regions according to requirements of that region. Resources should be allocated to achieve that broadest application for all emergency and disaster needs, consistent with preparedness goals. That approach is fundamental to the principles of building on existing systems and to achieving the maximum possible multipurpose capability.

Second, programs for combating terrorism need accountability. Legislators and public officials, especially elected ones, must have some reliable, systematic way of assessing the extent to which their efforts and taxpayers' money are producing effective results.

[4] One of the most effective processes for identifying the issues most important to State and local entities has been the joint effort of the National Governors Association (NGA) Center for Best Practices and the National Emergency Management Association (NEMA) in conducting "States' Regional Terrorism Policy Forums." The entire compilation of "States' Recommendations" from the NGA/NEMA Policy Forums is contained in Appendix J. Future references in this report will be to "States' Recommendations" by recommendation number.

The performance and results of programs for combating terrorism are currently assessed almost solely according to anecdote. The only concrete measure available at the moment is the dispersal of Federal funds—a process measurement that does not achieve effective strategic management.

Third, programs for combating terrorism need clear priorities. It is impossible to set priorities without first defining results-based objectives. The essence of any coherent strategy is a clear statement of priorities that can be translated into specific policy and programmatic initiatives. Priorities are the transmission mechanism that connects ends to means.

Developing the Means of Strategy: Program Structure and Priorities

Setting priorities is essential in any strategy, but priorities require clear, results-based objectives. With some meaningful sense of objectives, it will be possible to develop coherent priorities and an appropriate set of policy prescriptions. For instance, should the nation seek a different level of preparedness for large urban centers than for rural areas? What should be the relative importance of preparing for conventional terrorism, radiological incidents, chemical weapons, biological weapons, or cyber attacks? Should the nation seek to improve its preparedness more against the types of attacks that are most likely to occur, such as conventional terrorist bombings or the use of industrial chemicals, or for those that are most damaging but less likely to occur, such as nuclear weapons or military-grade chemical or biological weapons? With respect to biological weapons, which pathogens deserve priority? Should the emphasis be on small-scale contamination attacks as opposed to large-scale aerosol releases of the worst pathogen types, such as anthrax, plague, and smallpox? What is the relative priority for allocating resources to protect critical infrastructure, especially from cyber attacks?

The answers to these and other questions have important implications for the allocation of Federal resources for training, equipment acquisition, exercises, research and development, pharmaceutical stockpiles, vaccination programs, and response plans. A coherent national strategy would provide clarity to the allocation of Federal resources across the full range of possible activities to combat terrorism. To date, these critical resource allocation decisions have been made in an ad hoc manner and without reference to meaningful national goals.

The Executive Branch has not articulated a broad functional national strategy for combating terrorism. It is, therefore, not possible for the Advisory Panel to evaluate the extent to which the current panoply of preparedness programs contributes to the achievement of strategic goals. The next Administration should address the issue as a top priority, and certainly no later than one year after taking office. The country is now at a disadvantage in that a large number of programs have already been established and may have to be reconfigured—an inevitable consequence of their ad hoc origins.

Chapter Two

Getting the Federal House in Order

IMPROVING FEDERAL EXECUTIVE BRANCH COORDINATION

To many at the State and local levels, the structure and process at the Federal level for combating terrorism appear uncoordinated, complex, and confusing. Our first report included a graphical depiction of the numerous Federal agencies and offices within those agencies that have responsibilities for combating terrorism.[5] Attempts to create a Federal focal point for coordination with State and local officials—such as the National Domestic Preparedness Office—have met with little success. Moreover, many State and local officials believe that Federal programs intended to assist at their levels are often created and implemented without consulting them.[6] Confusion often exists even within the Federal bureaucracy. The current coordination structure does not possess the requisite authority or accountability to make policy changes and to impose the discipline necessary among the numerous Federal agencies involved.

"THE NATIONAL OFFICE FOR COMBATING TERRORISM"

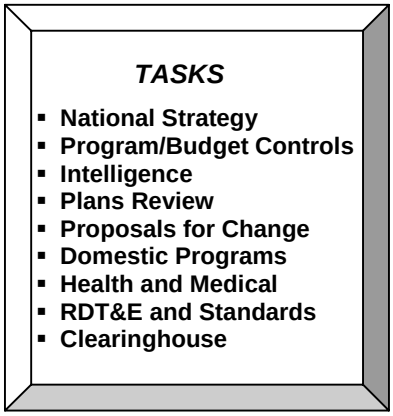
We recommend the establishment of a senior level coordination entity in the Executive Office of the President, entitled the "National Office for Combating Terrorism," with the responsibility for developing domestic and international policy and for coordinating the program and budget of the Federal government's activities for combating terrorism.[7]

[5] First Report, Appendix A.

[6] The implementation of the Nunn-Lugar-Domenici "120 Cities" training program and the initial structure of the equipment grant program are two examples.

[7] Several of the concepts contained in our recommendation were included in H.R. 4210 (the "Fowler Bill"), as it was introduced or as it passed the House of Representatives. The most obvious difference in our recommendations and those contained in H.R. 4210 involve the scope of responsibilities of the office. H.R. 4210 was only for domestic preparedness and response; our proposal covers both domestic and international and therefore includes specific provisions related to foreign programs and intelligence collection.

Principal Tasks



National Strategy. The National Office for Combating Terrorism will have several principal tasks. Foremost will be the responsibility to develop a comprehensive national strategy. That strategy must be approved by the President and updated annually. It must address the full range of domestic and international terrorism deterrence, prevention, preparedness, and response. The approach to the *domestic* part of the strategy should be "bottom up," developed in close coordination with local, State, and other Federal entities.[8]

The strategy must contain a detailed implementation plan, with specific milestones for its accomplishment. Most important, the strategy must articulate a methodology for continually measuring and monitoring domestic preparedness. That methodology must be accomplished in close coordination with the States. Preparedness efforts will vary from State to State and even among jurisdictions within States. Nevertheless, some rational system to rate our preparedness as a nation will be required, if making the most effective use of limited resources—at all levels of government—is a worthwhile goal. We do not suggest that all jurisdictions "look the same" in terms of a specific minimum number, for example, of pieces of certain personal protective equipment (PPE) per thousand population.

A simple "scorecard" for preparedness is not the answer. One city in the Los Angeles metropolitan area, for example, may not have any "Level A" chemical protective suits, but may possess the latest state-of-the-art communications equipment. A neighboring jurisdiction may recently have invested in "Level A" gear. Taking the best of each and of other nearby jurisdictions as part of a cooperative effort for mutual aid will yield dramatically different preparedness indicators than a "city-by-city" rating scheme. Cooperative efforts among jurisdictions will foster preparedness on an area basis.

That recognition suggests to us that a preparedness measurement process should be developed along regional lines. Such an approach might start with the 10 Federal Emergency Management Agency regions as a base with further subdivisions into area groupings.

Program and Budget Controls. A concurrent responsibility of the National Office for Combating Terrorism will be to work within the Executive Branch and with the Congress to ensure that sufficient resources are allocated to support the execution of the national strategy. The U.S. strategy for deterrence, prevention, preparedness, and response for terrorists acts outside the United States, developed under the leadership of the

[8] See "States' Recommendations," Nos. 11 and 23, Appendix J.

Department of State, is comprehensive and, for the most part, appropriately resourced. It is on the domestic front that much additional effort and coordination will be required.

We recommend that the National Office for Combating Terrorism be given the authority to exercise specific limited program and budget control over activities for combating terrorism within the relevant Federal departments and agencies. That authority should include the responsibility to conduct a full review of Federal agency programs and budgets, to ensure compliance with the programmatic and funding priorities established in the approved national strategy and to eliminate conflicts and unnecessary duplication among agencies. **We recommend that an Assistant Director direct the program and budget functions for Management and Budget.**

The Office of Management and Budget and the responsible element of the National Security Council staff—the Office of the National Coordinator for Security, Counter-terrorism, and Infrastructure Protection—have developed a process for submitting a composite "roll-up" of the programs for combating terrorism of the various Federal agencies. The latest submission to the Congress[9] is the most comprehensive to date. That is an important step in the right direction—a macro-level inventory of agency spending to combat terrorism. To be truly effective, however, such a process must contain specific authority to hold agencies accountable for their spending and for compliance with the national strategy. Moreover, OMB's "Annual Report" provides only general program descriptions. The Executive should provide comprehensive information to the Congress to consider in the deliberative authorization and appropriations processes. In addition to a comprehensive strategy document, supporting budget information should include a complete description and justification for each program, coupled with current and proposed out-year expenditures.

Intelligence Coordination and Analysis. We recommend that the National Office for Combating Terrorism provide coordination and advocacy for both foreign and domestic terrorism-related intelligence activities, including the development of national net assessments of terrorist threats. A critical task will be to develop, in concert with the Intelligence Community,[10] policies and plans for the dissemination of intelligence and other pertinent information on terrorist threats to designated entities at all levels of government—local, State, and Federal.[11]

We recommend that an Assistant Director for Intelligence in the National Office direct the intelligence function for Combating Terrorism, who should be "dual-hatted" as the National Intelligence Officer (NIO) for Combating Terrorism at the

[9] *Annual Report to Congress on Combating Terrorism, Including Defense against Weapons of Mass Destruction/ Domestic Preparedness and Critical Infrastructure Protection*, May 18, 2000. The requirement for the submission to the Congress of an annual report of funding efforts in the Executive Branch to combat terrorism is contained in Section 1051 of the National Defense Authorization Act for Fiscal Year 1998 (Pub. L. 105–85), as amended by Section 1403 of the National Defense Authorization Act for Fiscal Year 1999 (Pub. L. 105–261).

[10] Including its Federal law enforcement components.

[11] For more detailed recommendations in this subject area, see the section entitled "Collecting Intelligence, Assessing Threats, and Sharing Information" in Chapter Three.

National Intelligence Council. That Assistant Director/NIO and staff would be responsible for compiling terrorism intelligence products from the various agencies, for providing national-level threat assessments for inclusion in the national strategy, and for producing composite or "fused" products for dissemination to designated Federal, State, and local entities, as appropriate. The Assistant Director/NIO should be delegated, by Executive Order or in enabling legislation, tasking authority for terrorism-related intelligence collection and analysis. That person will serve as focal point for developing policy for combating terrorism intelligence matters, keeping the policymaking and operational aspects of intelligence collection and analysis separate. The Assistant Director will also be the logical interface with the intelligence oversight committees of the Congress. It is, in our view, important to have a senior-level position created for this purpose, and we recommend that the person initially chosen to fill the position be a current or former agent of the Federal Bureau of Investigation. That position can then be filled in rotation by appropriately qualified persons from law enforcement and the Intelligence Community. The intelligence office should be staffed with a small, select staff of knowledgeable and experienced personnel, who understand collection, analysis, and assessment processes, from the various intelligence and law enforcement agencies.

There is sound rationale for the legal and regulatory requirements governing the "domestic collection" of intelligence by the Intelligence Community.[12] It will be the responsibility of the Assistant Director for Intelligence and the intelligence staff to ensure strict adherence to applicable law and regulations in the administration of these activities.

To assist in this intelligence function, **we recommend the establishment of a "Council to Coordinate Intelligence for Combating Terrorism," to provide strategic direction for intelligence collection and analysis, as well as a clearance mechanism for product dissemination and other related activities.** It should consist of the heads of the various Intelligence Community entities and State and local representatives who have been granted appropriate security clearance. The Director of the Federal Bureau of Investigation and the Director of Central Intelligence should chair it in annual rotation.

Plans Review. We recommend that the National Office for Combating Terrorism be given authority to review State and geographical area strategic plans, and at the request of State entities, review local plans or programs for combating terrorism, for consistency with the national strategy. That review will allow the National Office to identify gaps and deficiencies in Federal programs. At the completion of that review, the National Office should provide an analysis of the plan or program, including any recommendations for modification, to the submitting jurisdiction.

Proposals for Change. We recommend that the National Office for Combating Terrorism have authority to propose new Federal programs or changes to existing programs, including Federal statutory or regulatory authority.

[12] For further discussion on this point, see the section entitled "Collecting Intelligence, Assessing Threats, and Sharing Information" in Chapter Three.

Domestic Preparedness Programs. We recommend an Assistant Director for Domestic Preparedness Programs in the National Office to direct the coordination of Federal programs designed to assist response entities at the local and State levels, especially in the areas of "crisis" and "consequence" planning, training, exercises, and equipment programs for combating terrorism.[13] The national strategy that the National Office should develop—in coordination with State and local stakeholders—must provide strategic direction and priorities for programs and activities in each of these areas.

Health and Medical Programs. Much remains to be done in the coordination and enhancement of Federal health and medical programs for combating terrorism and for coordination among public health officials, public and private hospitals, pre-hospital emergency medical service (EMS) entities, and the emergency management communities. **We recommend that the responsibility for coordinating programs to address health and medical issues be vested in an Assistant Director for Health and Medical Programs in the National Office for Combating Terrorism.** The national strategy should provide direction for the establishment of national education programs for the health and medical disciplines, for the development of national standards for health and medical response to terrorism, and for clarifying various legal and regulatory authority for health and medical response.

Research, Development, Test, and Evaluation (RDT&E), and National Standards. We recommend that the responsibility for coordinating programs in these two areas be assigned to an Assistant Director for Research, Development, Test, and Evaluation, and National Standards in the National Office for Combating Terrorism.[14] The national strategy should provide direction and priorities for RDT&E for combating terrorism. We believe that the Federal government has primary responsibility for combating terrorism RDT&E. Local jurisdictions and most states will not have the resources to engage in the research and development required in the sophisticated environment that may be a part of the nation's response to terrorism. Moreover, we have essentially no nationally recognized standards in such areas as personal protective equipment, detection equipment, and laboratory protocols and techniques.

Clearinghouse Function. We recommend that the National Office for Combating Terrorism should serve as the information clearinghouse and central Federal point of contact for State and local entities. We heard many comments about how difficult it is for local jurisdictions and State agencies, even those with experience in complex Federal programs, to navigate the maze of the Federal structure. The National Office for Combating Terrorism should assume that role and serve as the "one-stop shop" for

[13] For more detailed recommendations in this subject area, see the sections entitled "Training, Equipping, and Exercising" and "Planning, Coordinating, and Operating Cooperatively" in Chapter Three.

[14] For more detailed recommendations on RDT&E, see the section entitled "Promoting Better Research and Development, and Developing National Standards" in Chapter Three.

providing advice and assistance on Federal programs for training, planning, exercises, equipment, reporting, and other information of value to local and State entities.

Structure and Characteristics

The National Office for Combating Terrorism should possess certain essential attributes, as follows:

Political Accountability and Responsibility. The person designated as the focal point for developing a national strategy and for coordinating Federal programs for combating terrorism must have political accountability and responsibility. That person should be vested with sufficient authority to accomplish the purposes for which the office is created and should be the senior point of contact of the Executive Branch with the Congress. In that way, the Congress will have the opportunity to discuss the government's overall policy and programs for combating terrorism with the senior official responsible. For these reasons, **we recommend that the President appoint and the Senate confirm the Director of the National Office for Combating Terrorism, who should serve in a "cabinet-level" position**.

Program and Budget Authority. The National Office for Combating Terrorism should have sufficient budget authority and programmatic oversight to influence the resource allocation process and ensure program compatibility. That process should include a structured certification/decertification process to formally "decertify" all or part of an agency's budget as noncompliant with the national strategy. A decertification would require the agency to revise its budget to make it compliant or, alternatively, to allow the agency head to appeal the decertification decision to the President. This recommendation does not give the Director of the National Office authority to "veto" all or part of any agency's budget, or the authority to redirect funds within an agency or among agencies

Multidisciplinary Staffing. We recommend that the National Office for Combating Terrorism have full-time multidisciplinary expertise, with representation from each of the Federal agencies with responsibilities for combating terrorism, and with resident State and local expertise. The National Office can ensure Federal agency representation by directly hiring personnel from the various agencies. A better approach would be the directed detail of various Federal agency personnel on a term basis. That would allow for the rotation of incoming personnel who bring current perspectives from their respective agencies and the return to those agencies of personnel who will have a national-level perspective. Moreover, the personnel and the agencies involved must view such assignments as "career enhancing."

For programs with a domestic focus, the National Office for Combating Terrorism must have sufficient resources to employ persons with State and local expertise and from each of the response disciplines. The National Office should enter into agreement with State and local jurisdictions for a leave of absence for certain personnel, to be employed by the

National Office for a specified term. With that approach, there would be a constant flow of personnel with perspectives "fresh from the street."

No Operational Control. While the National Office for Combating Terrorism should be vested with specific program coordination and budget authority, it is not our intention that it have "operational" control over various Federal agency activities.

We recommend that the National Office for Combating Terrorism not be "in charge" of response operations in the event of a terrorist attack. The National Office should provide a coordinating function and disseminate intelligence and other critical information. The word "czar" is inappropriate to describe this office. The Director should not be empowered to order any Federal agency to undertake any specific activity.

Lead Federal Agency responsibility will normally fall to the Department of Justice for "crisis management" and to the Federal Emergency Management Agency for "consequence management." Other than its continuing responsibility in facilitating the flow of information and intelligence, this recommendation does *not* envision any operational role for the National Office for Combating Terrorism during an actual response.

> "Lead Federal Agency" and "Lead Agency" are defined as follows:
>
> "2. Several of these plans designate a Lead Federal Agency (LFA) to coordinate the Federal response. The LFA is determined by the type of emergency. In general, an LFA establishes operational structures and procedures to assemble and work with agencies providing direct support to the LFA in order to obtain an initial assessment of the situation, develop an action plan, and monitor and update operational priorities. The LFA ensures that each agency exercises its concurrent and distinct authorities and supports the LFA in carrying out relevant policy. Specific responsibilities of an LFA vary according to the agency's unique statutory authorities."[15]
>
> . . . . . .
>
> "G. Lead Agency. The FBI defines lead agency, as used in PDD-39, as the Federal department or agency assigned lead responsibility to manage and coordinate a specific function—either crisis management or consequence management. Lead agencies are designated on the basis of their having the most authorities, resources, capabilities, or expertise relative to accomplishment of the specific function. Lead agencies support the overall Lead Federal Agency during all phases of the terrorism response."[16]

With few exceptions, we recommend that existing programs remain in the agencies in which they currently reside. One notable exception will be the functions of the National Domestic Preparedness Office (NDPO), currently housed in the Federal Bureau of Investigation. The new office should subsume all of the *intended* functions of the

[15] Federal Response Plan, Basic Plan, Chapter IV. Concept of Operations, Section B, Concurrent Implementation of Other Federal Emergency Plans, paragraph 2.
[16] Federal Response Plan, Terrorism Incident Annex, Section VIII, Terms and Definitions, paragraph G.

NDPO—coordination, information clearinghouse, advice and assistance to State and local entities.

The National Office for Combating Terrorism should also assume many of the interagency coordination functions currently managed by the National Security Council office of the National Coordinator for Security, Counter-terrorism, and Infrastructure Protection. For example, the responsibility for coordination of certain functions related to combating terrorism—Assistance to State and Local Authorities, Research and Development, Contingency Planning and Exercises, and Legislative and Legal Issues, among others—will devolve to the National Office for Combating Terrorism.[17] We also recommend that the National Office for Combating Terrorism absorb certain entities as adjuncts to its office, such as the Interagency Board for Equipment Standardization and InterOperability.

<u>Advisory Board for Domestic Programs</u>. To assist in providing broad strategic guidance and to serve as part of the approval process for the domestic portion of strategy, plans, and programs of the National Office for Combating Terrorism, we recommend the establishment of a national "Advisory Board for Domestic Programs." That Board should include one or more sitting State governors, mayors of several U.S. cities, the heads of several major professional organizations,[18] and a few nationally recognized terrorism subject matter experts, as well as senior officials from relevant Federal agencies. The President and the Congress should each appoint members to this board.

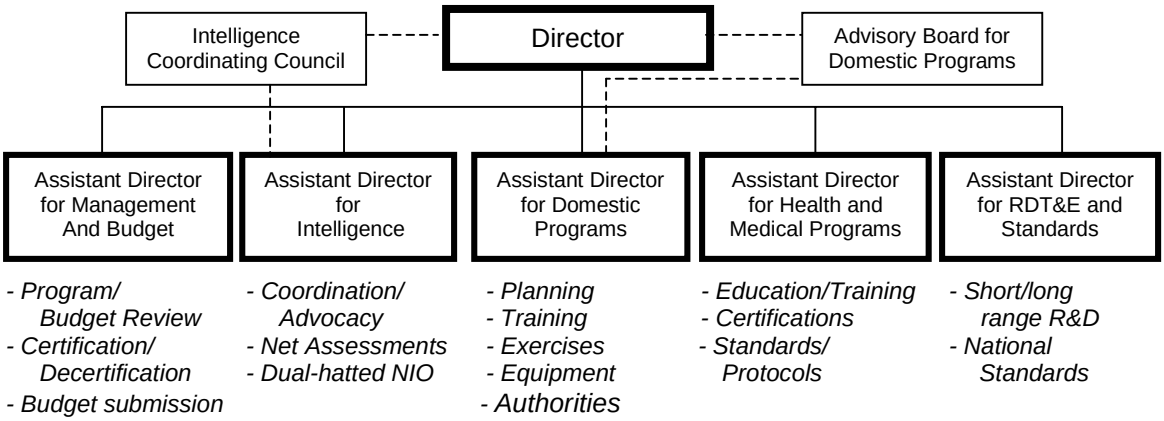


Figure 1. National Office for Combating Terrorism

[17] To avoid confusion, we recommend the removal of the "counter-terrorism" element of the "coordinator's" title. The "coordinator" will continue to be Special Assistant to the President and Senior Director for Transnational Threats. That office should coordinate with the new National Office on terrorism issues.

[18] Potential organizations would include the International Association of Chiefs of Police, the International Association of Fire Fighters, the International Association of Fire Chiefs, the National Association of Emergency Medical Technicians, the National Emergency Management Association, the Council of State and Territorial Epidemiologists, the National League of Cities, the National Association of Counties, and the International City/County Management Association.

Relationship with Other Federal Entities and Agencies. The nature of the relationship of the National Office for Combating Terrorism with other Federal entities and the lines of authority for all involved must be clear.

- National Security Council (NSC)—The Director of the National Office for Combating Terrorism should attend meetings of the National Security Council when terrorism is a topic for consideration. Appropriate elements of the National Security Council structure will provide direct input into the national strategy development and program and budget activities for combating terrorism for national security issues.[19]

- Office of Management and Budget (OMB)—The program and authorities of the National Office for Combating Terrorism are not intended to supplant or usurp the authorities of OMB. Agencies with responsibilities for combating terrorism will continue to submit complete budgets, including those parts of the budget related to programs for combating terrorism, to OMB. In parallel, the portions of agency budgets related to programs for combating terrorism will also be submitted to the National Office for Combating Terrorism.

- Federal Cabinet Departments and Other Federal Agencies—"Lead Federal Agency" and "Lead Agency" designations and roles related to Federal programs and activities for combating terrorism will continue to apply.

Alternative Structures Considered

During the course of our deliberations on the issue of improving Federal Executive Branch coordination, we considered and rejected other alternatives to the creation of an entity in the Executive Office of the President. We set forth those various alternatives in Appendix E and explain why each was rejected.

[19] An analogy is the current relationship between the National Security Council staff and the Office of National Drug Control Policy. The director of that office likewise attends NSC meetings pertaining to drug control matters. There are other similarities as well. The current statutory provisions for the structure and authority of the Office of National Drug Control Policy are contained in 22 U.S. Code, Chapter 22 (22 U.S. Code, Sections 1701 - 1712).

IMPROVING COORDINATION IN THE CONGRESS

In our first report, we were critical of the Congress for its propensity to make "decisions for authority and funding to address domestic preparedness and response issues [for combating terrorism] with little or no coordination." We noted that 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."[20] Those observations still pertain.

The Congress has been active in proposing legislative "fixes" to the problem of Interagency coordination. Two recent examples are the unanimous passage by the House of Representatives of a bill to create the "Office of Terrorism Preparedness" in the Executive Office of the President,[21] and of a provision to create a new "Deputy Attorney General for Combating Domestic Terrorism."[22] Numerous Congressional panels on both sides of Capitol Hill have held hearings on the subject of terrorism. The Congress has also commissioned various studies and reports on combating terrorism by the General Accounting Office (GAO).[23] One Act noted that Members "continue to be concerned about the threat of domestic terrorism, particularly involving the use of weapons of mass destruction (WMD) and the ability of the Federal Government to counter this threat." As a consequence, the Congress directed a comprehensive report from the GAO:

> The conferees agree to a provision that would require the Comptroller General to provide an updated report to Congress, not later than 180 days after enactment of this Act, on federal strategy, policy and programs to combat domestic terrorism. The conferees direct the Comptroller General to include in the report on combating domestic terrorism a discussion of the following issues: lead agency responsibility for crisis and consequence management; adequacy of existing plans formulated by the various federal agencies; threat and risk assessments; command and control structures; exercises, including a thorough assessment of the recent Top Official Exercise 2000; cyberterrorism; and research and development efforts of new technologies.[24]

---

[20] First Report, Chapter IV, Conclusions and Recommendations, section on Congressional Responsibilities, p. 57

[21] H.R. 4210 passed on voice vote under suspension of the rules of the U.S. House Representatives on July 25, 2000. The bill was transmitted to the Senate and referred to the Committee on Environment and Public Works, where no further action has been scheduled.

[22] Contained in the U.S. Senate version of the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act for Fiscal Year 2001 (H.R. 4690). The provision was not contained in the version that emerged from the conference between the House and Senate. H. Rept. 106-1005. That version, which has now passed both houses, is awaiting Presidential signature or a threatened veto for other reasons.

[23] The GAO combating terrorism reports may be accessed at: http://www.gao.gov

[24] Section 1035, National Defense Authorization Act for Fiscal Year 2001 (NDAA FY01)(H.R. 4205, Pub. L. 106–398). See discussion in Conference Report to accompany NDAA FY01, p. 849.

The Congress continues to direct the creation and funding of specific programs with little coordination among the various committees. Some programs are funded with little apparent consideration for the impact of those decisions on a comprehensive national effort.

Moreover, appropriations committees, through their various agency appropriations bills, occasionally create and fund programs that were not subject to the normal authorization processes. The result of such action is often lack of detail and clarity in the structure and execution of programs, as well as a lack of continuity and sustainability, as most such programs are only funded year by year. Examples of major programs created and funded in appropriations bills, which have no parallel authorizing language, include most of the programs for combating terrorism administered by the Office of State and Local Domestic Preparedness Support in the Department of Justice: equipment grant programs totaling $75 million; and training programs, including grants to the national training consortium[25] and the Center for Domestic Preparedness totaling $37 million; and earmarks to two institutes totaling $30 million.[26]

The Congress may, however, be foundering on the issue in large measure because of the absence of a comprehensive "national strategy" for combating terrorism. We do not suggest that Congress has or should have the responsibility for creating such a national strategy. That is, in our view, clearly the responsibility of the Executive Branch.

Special Committee for Combating Terrorism

We recommend the establishment of a Special Committee for Combating Terrorism—either a joint committee between the Houses or separate committees in each House[27]—to address authority and funding, and to provide Congressional oversight, for Federal programs and authority for combating terrorism.

We do not make this proposal lightly, and do so with the full recognition that such change may be difficult but is no less meritorious.

Committee Functions and Structure

The joint or separate committee of each House should consist of bipartisan representation from Members of all relevant authorization, oversight, budget, and appropriations committees and subcommittees that currently have cognizance over Federal programs and activities to combat terrorism. It should have a full-time staff either detailed from

[25] New Mexico Institute of Mining and Technology; Texas A&M; Nevada Test Site (NTS); and Louisiana State University

[26] For FY 2000 programs. Funds for FY 2001 programs will likely be higher.

[27] Similar to the processes of permanent select committees on intelligence - the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence.

those relevant committees and subcommittees or new employees who have the requisite experience and expertise.[28]

The joint or separate panel should perform several critical functions. *First*, it would constitute a forum for reviewing all aspects of a national strategy and supporting implementation plans for combating terrorism, developed and submitted by the National Office for Combating Terrorism. As part of that process, the joint or each separate committee should develop a consolidated legislative plan, including authorizing language and corresponding budget and appropriations "benchmarks" in response to the national strategy to combat terrorism and accompanying program and budget proposals.

Second, it would serve as the "clearinghouse" for all legislative proposals for combating terrorism. For separate bills (unrelated to the omnibus package related to the strategy), the committee should have first referral of such legislation, prior to the referral to the appropriate standing committee.

Such a structure, with the direct testimony from Executive Branch representatives, State and local officials, private industry, and terrorism experts, could help to eliminate duplication in programs and funding, and to promote an effective national program.

[28] The "relevant committees and subcommittees" would include as a minimum:

Agriculture (House and Senate)
Appropriations Committee (House and Senate)
- Subcommittee on Commerce, Justice, State, and the Judiciary
- Subcommittee on Defense
- Subcommittee on Transportation
- Subcommittee on Treasury, Postal Service, and General Government
- Subcommittee on Labor, Health and Human Services, and Education
- Subcommittee on Foreign Operations
- Subcommittee on Energy and Water Development
- Subcommittee on Agriculture and Rural Development

Armed Services Committee (House and Senate)
Budget Committee (House and Senate)
Commerce Committee (House and Senate)
Energy And Natural Resources Committee (Senate)
Resources Committee (House)
Foreign Relations Committee (Senate)
International Relations Committee (House)
Governmental Affairs Committee (Senate)
Government Reform Committee (House)
Health, Education, Labor, and Pensions Committee (Senate)
Science Committee (House)
Judiciary Committee (House and Senate)
Transportation and Infrastructure Committee (House)
Ways and Means Committee (House)
Senate Select Committee on Intelligence
House Permanent Select Committee on Intelligence

Chapter Three

Improving Functional Capabilities

In Chapter Two, we addressed improving coordination within the Executive Branch and the Congress. We now turn to improving selected functional capabilities. Our focus, in keeping with our Congressional mandate, continues to be on the needs of local and State response entities. We assess how well the Federal government is doing in those areas and recommend specific priorities for focus and allocation of resources.

Building on existing emergency and disaster response capabilities, structures, and systems is the foundation of our approach. The nation has developed a reasonably effective system for responses to natural disasters, naturally occurring disease outbreaks, accidents, and for most criminal acts. It is not necessary, in our view, to create a completely separate set of capabilities for combating terrorism. Moreover, we based our recommendations on the premise that pursuing capabilities that have at least dual-purpose applications is the better approach.

The National Office for Combating Terrorism, described in Chapter Two, will play the key role in planning and synchronizing these initiatives.

COLLECTING INTELLIGENCE, ASSESSING THREATS, AND SHARING INFORMATION

From the inception of our deliberations, we have said that "more can and must be done to provide timely information—up, down, and laterally, at all levels of government—to those who need the information to provide effective deterrence, interdiction, protection, or response to potential threats."[29]

The potential connection between terrorism originating outside the United States and terrorist acts perpetrated inside the United States, means that "foreign" terrorism and "domestic" terrorism may not be easily distinguished. The need for lawful, timely collection and analysis of intelligence on foreign terrorist plots, outside or inside our borders, is accordingly one of the most critical functional capabilities needed by this nation. Moreover, any improvement in our ability to detect terrorist activity will provide added capability in detecting similar activities by adversarial nation-states.

[29] First Report, p. 57.

Based on classified briefings as well as "open-source" information, it is clear that the U.S. Intelligence Community's foreign intelligence collection and analysis against terrorism has been excellent. There is, however, room for improvement.

Improve Human Intelligence (HUMINT)

Recent events worldwide emphasize the need for the best possible intelligence. Moreover, reliance on sophisticated "National Technical Means" or other high-technology systems is not always sufficient to provide the necessary and timely "indication and warning" to forestall or to defend against a terrorist attack.

Certain procedures, well intentioned when implemented, are now hampering the nation's ability to collect the most useful intelligence. For that reason, we agree with the conclusion of a parallel commission—the National Commission on Terrorism[30]—and **recommend the rescission of that portion of the 1995 guidelines, promulgated by the Director of Central Intelligence, which prohibits the engagement of certain foreign intelligence informants who may have previously been involved in human rights violations.** We should return to the restrictions in place prior to the 1995 guidelines, which afforded sufficient protections, oversight, and an approval mechanism that will prevent abuse.

Improve Measurement and Signature Intelligence (MASINT)[31]

As the potential grows for terrorists to use more unconventional and sophisticated weapons, especially with chemical or biological agents, our capability to detect such agents assumes greater urgency and requires new technology to provide needed capability.

To meet that challenge, **we recommend an expansion and improvement in research, development, test, and evaluation (RDT&E) of reliable sensors and rapid readout capability, and the subsequent fielding of a new generation of MASINT technology based on enhanced RDT&E efforts**. Our goal for sensors and rapid readout technology for chemical and biological agents should be no less than our current capability for nuclear and radiological agents.

Review Statutory and Regulatory Authorities

The following observations and recommendations do not diminish those rights and liberties but are intended to allow the nation to be more effective in combating terrorism while fully protecting those rights and liberties.

[30] Report of the National Commission on Terrorism, *Countering the Changing Threat of International Terrorism*, p. 8.
[31] This recommendation is directed to national technical means, not capabilities for response entities.

We recommend a thorough review, by a panel of Department of Justice (DOJ) officials and knowledgeable citizens outside the Federal government, of the terrorism portion of the Attorney General's "Domestic Guidelines." We examined the guidelines, which establish conditions under which an FBI agent can open an inquiry into possible terrorist activity inside the United States. The guidelines appear to us to be adequate in scope but have been rendered confusing and ambiguous by successive redrafting over the years, leading to misunderstanding and uneven application among law enforcement agents. We do not suggest that the guidelines be rescinded or that the underlying requirement for them is not sound. **We recommend that the panel review the domestic guidelines for clarity, in the interests of strengthening them, while providing for the protection of civil rights and liberties.** We also recommend that the guidelines provide examples of permissible and impermissible activity as further information for agents' decisions.

The Foreign Intelligence Surveillance Act (FISA) governs domestic national security investigations.[32] The procedures of the Office of Intelligence Policy and Review (OIPR) in the Department of Justice, required to present a matter to the special Foreign Intelligence Surveillance Court established under FISA, require far more justification than the Act does. **We recommend that the Attorney General direct OIPR to modify its procedures to conform to the FISA statutory requirements**.

Moreover, controls inside our borders that can hamper efforts of potential terrorists—be they foreign or domestic—by denying them their "tools of the trade," can be established or strengthened without additional authority. **We recommend that the Department of Justice, in consultation with appropriate committees of the Congress as well as knowledgeable members of the scientific, health, and medical communities, and State and local government, continually review existing statutory authorities and regulations**. **The purpose would be to propose specific prohibitions, or at least mandatory reporting procedures, on the domestic sale and purchase of precursors and special equipment that pose a direct, significant risk of being used to make and deliver CBRN weapons or agents**.[33]

Improve Forensics Capabilities to Identify Terrorist Unconventional Weapons

We have today effective forensic capabilities to detect and identify conventional weapons, including high-explosive devices and associated mechanisms, as well as sophisticated techniques for identifying perpetrators.[34]

Given the potential for terrorists to resort to chemical and biological weapons, developing a comparable forensics capability for such weapons is a clear priority. **We recommend that the National Office for Combating Terrorism foster research and development in forensics technology and analysis**. Those steps will involve either the development

[32] 50 U.S. Code, Sections 1801–1863.
[33] An identification of such precursors and equipment should be made in an Executive Order or regulations, coordinated with all relevant Federal health and law enforcement agencies.
[34] The FBI's internal laboratory and others available to it collectively are, without question, the best in the world.

of a new program in a specific agency, or the consolidation of several existing programs. **We also recommend that the National Office implement an Indications and Warning System for the rapid dissemination of information developed by enhanced forensics**.

These efforts should include Federal assistance to State and local forensics capabilities. Some terrorist threats or actual attacks may initially appear to be some other form of criminal conduct, and Federal involvement may not be implicated. Enhancements at State and local agencies will not only facilitate early identification, but will also support subsequent criminal investigations.

If terrorists know that the nation has the capability to detect and identify devices and perpetrators—so that the "return address" can be determined—deterrence is enhanced accordingly.

Expand Information Sharing and Improve Threat Assessments

Several agencies have made strides in enhancing information sharing. Notable examples include efforts by the FBI to implement fully its Joint Terrorism Task Force (JTTF) program and to provide information on combating terrorism to response entities through its web-based system, Law Enforcement Online ("LEO").

An even more comprehensive dissemination system must be developed to provide information through expanded law enforcement channels, and through regional FEMA offices into State emergency management channels, for further dissemination to local response entities. **As part of that process, the National Office should promote a system for providing some form of security clearance to selected State and Local officials nationwide, and methods for disseminating classified information to those officials in near real time**. One product of that process will be timely threat assessments, in which the FBI must be an integral part. The FBI has undergone a reorganization that consolidated several related entities into a new Counterterrorism Division, with an Assistant Director at its head. That division needs more internal analytic capability. **We recommend that the FBI consider implementing a "Reports Officer" or similar system, analogous to the process used by the Central Intelligence Agency, for tracking and analyzing terrorism indicators and warnings.**

To promote the broadest dissemination of information to the largest audience of response entities, **we recommend that the National Office for Combating Terrorism foster the development of a protected, Internet-based, single-source web page system, linking appropriate combating terrorism information and databases across all applicable functional disciplines**. The FBI's LEO system is one example of many single-function capabilities that should be part of an integrated system. The Department of Defense is also developing related capabilities that would be valuable components of such a system. The system will entail a multi-agency intergovernmental and private sector cooperative arrangement.

PLANNING, COORDINATING, AND OPERATING COOPERATIVELY

For all of the advantages of our "federal" system of government, coordination among its levels for major undertakings presents challenges beyond those inherent in the undertaking itself.[35]

Prior to an attack, the Federal government must provide national leadership, guidance, and assistance to response entities at all levels. Federal entities can facilitate nationwide preparedness by helping to develop national standards for training, exercising, and equipment programs. The Federal role is preeminent, perhaps exclusive, in the areas of research, development, test, and evaluation. Moreover, the Federal government must have the lead in collecting and analyzing intelligence and in fostering sharing intelligence and information.

When a terrorist attack occurs, the Federal role for criminal investigation and prosecution is already very specific. The FBI has responsibility for investigations of terrorist threats and attacks. The U.S. Department of Justice then has responsibility for prosecution under various Federal criminal statutes on terrorism. Terrorist threats or attacks may also be violations of State or local law, so jurisdiction over investigations and prosecutions can be concurrent. State and local officials recognize that the FBI and DOJ have paramount though not exclusive jurisdiction in both terrorism investigation and prosecution.

Otherwise, the Federal role in a response to an actual attack should be to assist when requested and to meet response requirements that exceed local and State capabilities. Response to an attack must be layered and sequential: Local entities will respond first, supplemented as necessary by State capabilities. When local capabilities are exceeded, the response shifts to the State (perhaps multi-state) level. The Federal response should come only after local and State capabilities are exceeded. The Federal response should not be a major one—with the Federal entities "in the lead" for operations—except in the most extreme situation. For such cases, detailed planning and close coordination will lessen the prospect for overreaction that could infringe civil liberties. Moreover, relying on assets at the Federal level that are many hours—perhaps days—from deployment in an actual response is problematic.

We recommend that the senior emergency management entity in each State function as the prime *Focal Point* for that State for domestic preparedness for terrorism. The focal point should solicit input and representation from local jurisdictions and agencies. The State emergency management entity should oversee the lines of communications between the Federal government and local response entities. State entities are more likely to have the total picture of preparedness and requirements throughout the State and can better establish priorities for the allocation of resources and for other requirements. This arrangement will reduce potentially counterproductive direct communication between the Federal government and local jurisdictions.

[35] For comparison purposes, support staff conducted a case study of the way the nation of Israel is organized for and coordinates responses to terrorism. That case study is set forth in Appendix F.

Improve Collective Planning Among Federal, State, and Local Entities

Many Federal entities plan for a variety of emergency responses, including terrorism. The Federal Response Plan (FRP)[36] is intended to be the single source for "all-hazards" responses but does not necessarily contain all plans for terrorism. The bifurcation between "crisis" and "consequence" management further complicates the problem.[37] State and local entities find it difficult to keep track of all the plans, and are often not consulted in the plan development process.

We recommend that the Federal Response Plan (FRP) be the single source Federal document for "all-hazards" response planning.[38] All applicable Federal departments and agencies should include their plans to respond to terrorist attacks as annexes to the FRP, in accordance with a specific FRP template. The FRP and the relevant Federal agency plans should include input from State and local entities. For clarity, we recommend renaming the FRP the "Federal Support Plan."

Several States have developed excellent plans and processes for combating terrorism.[39] Any of these would serve as a useful model for other States. Because States may have to assist each other in response to a terrorist attack, coordination would obviously be enhanced if State plans followed a standard format. **We recommend that the National Emergency Management Association, in conjunction with the Federal Emergency Management Agency, develop a "model" State plan, flexible enough to fit any State's specific circumstances, but with certain standard features.**[40] In this regard, the National Office for Combating Terrorism should play a lead role.

Enhance Coordination of Programs and Activities

The complexities of the Federal structure for combating terrorism create daunting challenges for a State entity, e.g., to know whom to call at the Federal level for

---

[36] The Federal Response Plan (FRP) "establishes a process and structure for the systematic, coordinated, and effective delivery of Federal assistance to address the consequences of any major disaster or emergency declared under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended (42 U.S.C. 5121, et seq.)." FRP, Chapter 1, Introduction. Our recommendation would expand its scope to include responses to terrorism under the Stafford Act and other Federal authority.

[37] For example, the FBI's "U.S. Government Interagency Domestic Terrorism Contingency Plan " (CONPLAN) is not designed to be part of the FRP. The FBI is in the final stages of publishing the CONPLAN, its operational plan for "crisis management," separate from the FRP, despite the fact that it says that it was "developed consistent with . . . the Federal Response Plan and its Terrorism Incident Annex," among other documents and directives. CONPLAN, p. iii. It should be included as a part of a total plan. And see "States' Recommendations," Nos. 7, 11, and 19, Appendix J.

[38] We considered recommending that the National Office promulgate a "Federal Terrorism Response Plan" for Combating Terrorism. We did not favorably consider that approach for two reasons: (1) The response plan should be operationally oriented, and the National Office for Combating Terrorism is not an operational entity; and (2) A fundamental principle in our approach is building on existing emergency response systems. Creating an entirely separate plan for response to terrorism could result in ineffectiveness and potentially conflicting plans. By the same token, the FRP should not be a strategic policy document, and the National Office should therefore, formulate policy for combating terrorism.

[39] California, Iowa, New Hampshire, and New Mexico, to mention a few.

[40] See "States' Recommendations," No. 15, Appendix J.

assistance. The National Office should foster clear lines of coordination must be established, vertically and horizontally across disciplines, and promote "best practices" to eliminate unnecessary redundancies. Creating the National Office for Combating Terrorism and designating State emergency management entities as the "focal point" for State and local coordination will help. Each Federal agency should also designate a "single point of contact" for State and local entities to obtain assistance from that Federal agency.[41]

While well intended, the Federal government has in some cases created new programs to assist State and local response entities, such as training and exercises, without a full understanding of similar programs that already exist and that could be leveraged more effectively with resources already available.[42] **We recommend that the National Office for Combating Terrorism conduct inventories of State and local programs for capabilities that can be utilized in a national context, especially training and exercise programs**.[43]

We recommend that the National Office for Combating Terrorism promote multi-jurisdictional mutual assistance compacts, using the FBI Joint Terrorism Task Forces as one model, and facilitate the implementation of interstate mutual assistance compacts among states, through FEMA Regional Offices.[44] Such compacts should encompass Federal, State, and local public health entities in all aspects of planning, coordination, and operations, especially for multi-jurisdictional and multi-state operations.

A terrorist attack may require a response lasting days, and possibly weeks. Many local entities have some capability for "shift changes" to allow personnel to rest and return to work, but that capability is likely to be taxed quickly. As a result, **we recommend more intense tactical and operational planning to facilitate "second wave" capabilities from outside entities after the depletion of local resources**.

In our first report, we cited the multi-jurisdictional organizational structure that exists in the Los Angeles metropolitan area, called the "LA Operational Area." More than 80 municipal and county jurisdictions participate in the LA Operational Area Terrorism Working Group (TWG) and a related structure, the Terrorism Early Warning Group (TEWG). Our support staff has conducted a case study of the LA Operational area to provide "lessons learned."[45] **We recommend that States utilize one of the standardized multi-state compacts, either the Emergency Management Assistance Compact or the States Compact.**[46]

---

[41] In keeping with our earlier reasoning and recommendations, local jurisdictions are encouraged to coordinate assistance from Federal agencies through the designated State agency.
[42] See "States' Recommendations," No. 7, Appendix J.
[43] See further discussions on training and exercise programs below.
[44] See "States' Recommendations," Nos. 11 and 30, Appendix J.
[45] That case study is included in Appendix G.
[46] The Emergency Management Assistance Compact (EMAC) is an interstate mutual aid agreement that provides a mechanism for States to assist each other in response to natural or man-made disasters. EMAC is administered by the National Emergency Management Association (NEMA) and is recognized by the

Improve Operational Command and Control of Domestic Responses

In response to an attack, lines of authority and responsibilities among the entities involved must be clear. The responder community has made progress in establishing command structures for response, but more is needed.

We recommend that the National Office for Combating Terrorism identify and promote a standardized Incident Command System (ICS) model for *tactical* operations for response to terrorist incidents that is part of an all-hazards approach. The model should capture the best elements and "best practices" of the ICS already in place in a number of jurisdictions but should always have two essential characteristics: flexibility for adaptation to local circumstances and a configuration that includes State and Federal liaison functions. As we noted in Chapter One, every local jurisdiction (either individually or as part of a multi-jurisdictional agreement) should adopt a standard ICS, and all levels of government above the local level should recognize that system.[47]

The terms "Incident Command System" and "Unified Command System" are often used synonymously. We distinguish the two terms and **recommend the identification and promotion, by the National Office for Combating Terrorism, of a standardized Unified Command System (UCS) model for operations and multi-agency, multi-jurisdictional coordination *above* the tactical operations level**. The UCS that we envision would be required when Federal resources are involved in more than an advisory or liaison capacity and when significant State assets are brought to bear.

When significant Federal resources are employed that involve two or more Federal agencies, we recommend a single Federal Emergency Operations Center (EOC) be established as part of the UCS.[48] We recognize that certain Federal agencies will need to conduct operations that cannot be open to all response entities. A standardized UCS can be designed with flexibility for "compartmented" operations within the EOC to protect classified or law enforcement sensitive information. The Federal EOC should include the FBI, FEMA, and any other Federal agency that has a significant role, geographically co-located to the extent feasible. Ideally, the State EOC should be located in geographical proximity to the Federal EOC.

The ultimate goal for the implementation of ICS and UCS, and the co-location of EOCs, is to delineate clear lines of authority for the conduct of operations at tactical and higher levels and to provide maximum coordination. To enhance that process, **we recommend that each jurisdiction with an ICS and UCS develop operational templates to**

Congress (Pub. L. 104-312). According to NEMA, 34 states and Puerto Rico have adopted EMAC. The "States Compact" refers to the Interstate Civil Defense and Disaster Compact, promulgated by the "Federal Civil Defense Act of 1950," Jan. 12, 1951, ch. 1228, 64 Stat. 1245 (Title 50 App., Sec. 2251 et seq.), and carried forward into the Stafford Act, 42 U.S. Code, Section 5196 (h). We also append to this report the framework of the New England Multi-State Compact, as an additional model for consideration. Appendix I.

[47] See "States' Recommendations," Nos. 7 and 8, Appendix J.

[48] This concept was used during TOPOFF 2000, and worked reasonably well.

provide for alignment of decision-making structures based on the weapon, means of delivery, and severity of the attack.[49]

Use of U.S. Armed Forces for Response to a Terrorist Attack Inside the Borders of the United States[50]

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

The civil rights and liberties of Americans must be paramount in all of the nation's efforts to combat terrorism. That fundamental precept is critical in any contemplation of the use of U.S. Armed Forces domestically; most traditional military operations are not planned with such considerations in mind, and most military personnel are not trained to deal with such issues.

A major attack by terrorists using unconventional weapons resulting in casualties in the tens of thousands is far less likely than a smaller-scale attack. Such an attack is, however, possible and must not be ignored. In such an extraordinary and catastrophic circumstance, the President may feel compelled, as a result of urgent requests from one or more Governors following the exhaustion of local and State capabilities, to resort to the use of military assets. In any such case, use of our armed forces must be made with the expressed condition that the military will always be strictly under civilian control.

Clear Constitutional and statutory authority exists for using the U.S. Armed Forces in a support role to provide significant assistance to civilian agencies.[51] The American people

[49] See "States' Recommendations," Nos. 8, 15, and 26, Appendix J.

[50] Advisory Panel Member L. Paul Bremer provided the following dissent:

"This section of the report contains much with which I agree. In almost all foreseeable circumstances, a Federal civilian agency should be the 'Lead Federal Agency' in responding to catastrophic terrorist attacks in the U.S. More must be done to improve those agencies' capabilities and the ability of the U.S. military to act in support of the 'Lead Federal Agency.' The U.S. military must always be under civilian leadership. And respect for civil liberties should be a primary goal of the Federal response to a terrorist incident.

"The question is how best to deal with the remote, but nonetheless imaginable, circumstance that a terrorist attack causes so much damage that it outruns the existing capabilities of Federal, State and local civilian entities. It is possible in such circumstances that the President may want to consider identifying, on an exceptional and temporary basis, the Department of Defense (DoD) as the 'Lead Federal Agency' under civilian leadership.

"Inserting DoD into such a role without preparation could have potentially serious implications for the protection of Americans' civil liberties. Effective crisis management depends on anticipating and planning for even the worst-case scenario and requires training and regular exercises to allow responders to practice and understand their appropriate roles.

"At present, the Federal government has no plans for DoD to be the 'Lead Federal Agency' under any circumstances, so that role is never exercised. This increases the possibility that, if called on by the President to be the 'Lead Federal Agency,' DoD will not be sensitive to protecting civil liberties.

"These vital liberties are more likely to be respected if our government 'thinks about the unthinkable' ahead of time and is not forced to deal with these crucial issues for the first time in the emotional wake of a national trauma. That is why I believe that the Federal government should plan for and exercise the possibility that the President may want to designate DoD as 'Lead Federal Agency' in such circumstances."

must be assured that civilian leaders will always direct and oversee the employment of military capability and will limit it to restoration of order, mitigation of consequences, and apprehension or interdiction of the perpetrators. Whether for "crisis management" or for "consequence management," military activities must, therefore, always be in support of the "Lead Federal Agency," as designated by the President.[52] In almost any conceivable scenario, the Lead Federal Agency will be either the Department of Justice (DOJ)(the lead for "crisis" management) or the Federal Emergency Management Agency (FEMA)(the lead for "consequence" management). No component of the U.S. Armed Forces should ever be the lead agency.

We recommend that the President always designate a Federal civilian agency other than the Department of Defense (DoD) as the Lead Federal Agency. Many Americans will not draw the technical distinction between the Department of Defense—the civilian entity—and the U.S. Armed Forces—the military entity. Although the Department of Defense and every major component of that department have civilian leaders, the perception will likely be that "the military" is in the lead. This recommendation does not ignore the fact that the DoD, through all of its various agencies—not just the Armed Forces—has enormous resources and significant capabilities for command, control, communications, intelligence, logistics, engineer, and medical support and may play a major role in response to a terrorist attack, especially one with potentially catastrophic consequences. Those resources can still be brought to bear but should always be subordinated to another civilian agency.

Our national civilians leader must ensure that plans for any use of the U.S. Armed Forces in a domestic terrorism context are thoughtfully developed and include a comprehensive description of the relationships with all levels of government. Military leaders at all levels must clearly understand those plans. Sufficient training and exercises must be conducted prior to the application of military capabilities in response to a domestic attack. This is especially important for the most catastrophic attack and in the event that the military provides significant support to a Federal civilian lead agency. In that case, the best way to ensure protection of our civil rights and liberties is not by reacting after the incident has occurred, but through comprehensive advance planning, rigorous training, and realistic exercises.[53]

In the event of a concerted effort by our adversaries both internationally and domestically, our armed forces will be committed elsewhere and not available at home. The more the nation enhances preparedness and capabilities to respond to terrorist acts with civilian assets—especially local and State response entities—the less likely the necessity to employ military assets in any situation.

---

[51] A full discussion of the various Constitutional and legal authorities is contained in Appendix R to the report.

[52] See page 13, above, for definitions of "Lead Federal Agency" and "Lead Agency."

[53] We are not yet satisfied that the requisite plans are in place to employ the military in a "crisis" response. We will delve into that issue in detail and provide our conclusions and recommendations in our third report.

TRAINING, EQUIPPING, AND EXERCISING

One of our fundamental assumptions has been that no single jurisdiction can handle a major terrorist attack. That assumption reinforces the importance of mutual assistance agreements and highlights the necessity for directly applicable training, equipment, and exercises. Proponents of such programs must coordinate with the intended recipients and meet national standards.

In Chapter Two, as part of the recommendation for the creation of the National Office for Combating Terrorism, we proposed that an Assistant Director of that office oversee Domestic Preparedness Programs, especially those designed to provide training, exercise, and equipment assistance to State and local entities. That Assistant Director should rely on the "Advisory Board for Domestic Programs"[54] for input to the national strategy and for continuing advice on training, exercises, and equipment programs.

Training

With respect to training, one of the first tasks for that Assistant Director will be to design a national training plan to address, at a minimum, the following fundamental questions:

- Training to do what?
- To what standards?
- Who is to provide the training and to whom?
- What is the goal of such training?
- How is the necessary level of training maintained?

The training directed in the Nunn-Lugar-Domenici (NLD) Act—the so-called "120 Cities" training—has been valuable but could have been even more effective. It was implemented with little input from the proposed training recipients. Many cities that received NLD training did not necessarily require the training provided. Additionally, planners assumed that the 120 most populous cities in the country all needed the same level and type of training as all others. That determination left some states completely out of the training plan. Moreover, the program initially targeted specific municipalities. In the early stages, recipient municipalities were not allowed to include representatives of surrounding communities, even though mutual assistance agreements among jurisdictions had predated the commencement of the training. Some of those problems were resolved as the program matured. One important lesson here is that future training programs must be responsive to the needs identified by those to be trained.

Another lesson further reinforces the need for a comprehensive national strategy, one that establishes goals and sets priorities across a broad array of functions. In the absence of an overarching Executive Branch plan, the Congress directed the Department of Defense to conduct the "120 Cities" training," a task from which senior leaders in the Pentagon sought relief.

[54] Recommended in Chapter Two.

A Presidential directive of May 2000 transferred the responsibility for most of the NLD training (the "Domestic Preparedness Program") to the Department of Justice. Funding for the program did not follow the transfer, however, and DOJ had not budgeted for it. Despite attempts to obtain funding for DOJ to complete most of the balance of the training,[55] as of this writing, the FY 2001 funding for DOJ has not been enacted.[56]

To compound matters, the DoD entity that conducted the NLD Domestic Preparedness Program—the U.S. Army Soldier and Biological Chemical Command—had established a "24-Hour Hotline" and a "First Responders Chemical-Biological Helpline." As of October 31, those services have been terminated.[57] Many response entities had used those services and had included that capability in their response plans. This is one more example of the direct impact on first responders of disorganization at the Federal level. State and local entities have developed protocols and response doctrine based on DoD Domestic Preparedness Program guidance and education programs. Eliminating this service creates a void in rapid access to essential information for emergency service entities and will require numerous changes to plans nationwide.

In the fire services and emergency medical services disciplines, the vast majority of the personnel involved—especially those in rural areas—are *volunteers*. The same holds true for reserve law enforcement personnel, who will undoubtedly assist in the response to any major terrorist attack. Many training programs for local responders follow a "Monday through Friday, 9-to-5" schedule. That time constraint may prevent many volunteer responders from participating in important training. **We recommend restructuring education and training opportunities to account for the high number of volunteer personnel in these "first responder" disciplines.** Distance learning applications would be very useful in this regard.

Exercising

Similar coordination and standardization problems exist with exercise programs. Many Federal entities[58] conduct or facilitate various exercises and offer State and local response entities opportunities to participate. Most agencies develop their own scenarios for such exercises, and in many cases, they are of the "worst case," mass-casualty variety. **We recommend that the Assistant Director for Domestic Programs in the National Office for Combating Terrorism develop exercise scenarios that are realistic and**

[55] DoD will continue to have responsibility for certain courses but not the full program.
[56] Neither the DoD nor DOJ had included funds for the completion of the program in its FY 2001 budget submission. Disagreements between the Senate and the House were only resolved in the final compromise of conferees on the Commerce, Justice, State Appropriations Act (CJS), which provides almost $21 million "for the NLD Domestic Preparedness Program authorized under the National Defense Authorization Act, 1997, and previously funded by the Department of Defense, to provide training and other assistance to the 120 largest U.S. cities." CJS, Conference Report to accompany H.R 4942. For a complete breakdown of DOJ funding for combating terrorism, see Appendix N.
[57] See the notice at: http://dp.sbccom.army.mil/fr/dp_technical.html
[58] Including numerous agencies in the Department of Defense, the Federal Emergency Management Agency, the Department of Energy, the Environmental Protection Agency, the Centers for Disease Control and Prevention, and the Department of Justice.

meet the needs of the State and local response entities. Exercises should be a logical extension of realistic training to aid in identifying weaknesses for which additional training may be indicated. Training and exercises should also include as scenarios the more likely, but less catastrophic, smaller scale CBRN attacks, and exercises must include *all* disciplines and all levels of response.

Members of the Advisory Panel observed significant portions of the national exercise called "Top Officials 2000,"[59] and based on those observations, **we recommend that all major exercises include an independent evaluation.**

Equipping

We support the decision to provide Department of Justice grants to States and localities based on equipment requirements identified at the State level. Prior to that change, DOJ provided grants directly to cities, a procedure with two disadvantages. First, it gave cities with greater expertise and capability for writing grant applications a significant advantage, and second, it did not take into consideration possible statewide deficiencies.

No standard should require any jurisdiction to possess specific types and numbers of equipment—sensors, personal protection equipment, communications, etc. With the growth of multi-jurisdictional mutual assistance compacts, and State-level oversight of sub-state jurisdictions, programs should provide maximum flexibility for State and local jurisdictions to address deficiencies.

Federal programs to assist State and local entities must have three core elements. First, programs should be based on the "best practices" of programs at any level of government. Second, plans must contain a requirement for evaluation, including feedback from the "end user" that will support certification of Federally supported programs by the National Office for Combating Terrorism. Finally, plans must identify deficiencies and proposals to correct them.

In April of this year, the Department of Justice Office for State and Local Domestic Preparedness Support (OSLDPS) published and distributed to the States an "Assessment and Strategy Development Tool Kit," in connection with the Fiscal Year 1999 State Domestic Preparedness Program. That document makes the "[r]eceipt of additional [Federal] funds under the [equipment] program[60]. . . contingent on the State's development of two separate, but related, documents. . . A State-wide Needs Assessment, and. . . a Three-Year Statewide [*sic*] Domestic Preparedness Strategy." Such tools as this, which provide for States to articulate their needs in accordance with a standard set of criteria, will be valuable in designing and implementing training, exercise, and equipment programs.

[59] A more thorough discussion of the observations is contained in Appendix L.
[60] FY 1999, FY 2000, and presumably "out-year" program funds.

IMPROVING HEALTH AND MEDICAL CAPABILITIES

Complete coordination among public health officials, public and private hospitals, pre-hospital emergency medical service (EMS) entities, law enforcement, fire services, and the emergency management communities is lacking. While coordination in some States and localities has improved dramatically, in others coordination is either nonexistent or in its infancy. State and local efforts to improve those relationships should continue.

Debate continues about how prepared the nation is to deal, from a medical and health standpoint, with a terrorist attack involving CBRN devices. In some medical institutions, especially those well funded in major metropolitan areas, there is significant capability to deal with disease outbreaks. That capability is not, however, consistent nationwide. The level of expertise in recognizing and dealing with a terrorist attack involving a chemical or biological agent is even more problematic.

Fundamental to our consideration is the premise that the nation must have a robust public health system. But that system, and additional resources required to improve it, should follow the multi-purpose approach that we have previously stressed. Combating terrorism is a compelling reason for such efforts but should not be the exclusive impetus. Strengthening the public health infrastructure to deal with accidental chemical injuries, emerging infectious diseases, and a pandemic outbreak of any kind should be the fundamental goal. Such efforts will expand the capability for decontamination, mass trauma cases, and other surge requirements to deal with terrorism mass casualty incidents.

Dual- and multi-purpose applications must be the goal. The nation should not expend vast additional resources only to a discrete issue, such as clinical research into biological terrorism. Conversely, improvements in prevention and in treatment of "all hazards" victims correspondingly enhance the capability to treat victims of terrorism and to prevent the spread of terrorists' agents.

We do not intend that our recommendations involving public health and medical care increase the burden on that system. Our goal is to include the elements of our recommendations into existing processes and to urge financial support where it is needed. As part of our work next year, we will examine health and medical issues in greater detail.

We recommend that the Assistant Director for Health and Medical Programs seek advice and input from Federal, State, and local public health officials, and from representatives of public and private medical care providers, to ensure that such issues are an important part of the national strategy.

Improve Education Programs

For hospitals, programs for domestic preparedness must include initial and continuing education in essential disciplines for the public health and medical response to terrorist

attacks, especially for chemical and biological devices. Training recipients should include emergency room doctors, nurses, and staff; other hospital personnel who may interact with pre-hospital EMS care providers; disease specialists; and pathologists. Medical examiners should also be included in this directed training. It will not be necessary to create major separate training programs on terrorism; special terrorism considerations can be imbedded in multi-purpose training in infectious diseases and for hazardous materials injuries.

One way to ensure the implementation of such training is to include terrorism-related subjects as part of professional licensing and certification processes, e.g., certification of designated medical personnel by such entities as the American Board of Emergency Medicine, the American Board of Internal Medicine, and the American Board of Pathologists.

We recommend that the National Office for Combating Terrorism consult with professional organizations, especially those with licensing or certification requirements, to find acceptable methods to implement such programs, including the prospect of providing Federal resources to support certified training programs.

Establish Standards and Protocols

Timely dissemination of accurate information on a terrorist attack is obviously crucial, especially for an attack involving a chemical or biological device. Most States require some mandatory reporting for diseases and for certain criminal conduct, but they are not well coordinated and the criteria are inconsistent. **Medical and health authorities should establish critical information gathering and dissemination, especially for CBRN attacks. They should simplify and standardize mandatory reporting.** Several major metropolitan areas, including New York City, Baltimore, and Los Angeles, have developed communications systems that, along with the Centers for Disease Control and Prevention (CDC) National Electronic Disease Surveillance System (NEDSS) and the emerging CDC EPI-X system,[61] can collectively serve as a national standard. Those procedures should also include exacting protocols for surveillance, identification, palliation, and follow-up.

Medical laboratories do not have consistent, nationally recognized standard protocols for the collection, identification, and referral of terrorists' CBRN agents, which increases the probability for incorrect identification and false positives. Medical and public health authorities must establish rapid, reliable methods (such as DNA fingerprinting) to determine whether an organism might be naturally occurring or the result of an intentional act. Explicit and uniform laboratory protocols must be designed and implemented at the Federal,[62] State,[63] and local[64] levels to facilitate such determinations.

[61] For descriptions of NEDSS and EPI-X, see Appendix H.
[62] For example, CDC, U.S. Department of Agriculture, and U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) laboratories.
[63] State laboratories.
[64] Hospital and reference laboratories.

In any terrorist attack, some conflict will inevitably occur between the special requirements of law enforcement and those of public health. The standard procedures should set forth the essential protocols to be followed to accommodate these competing interests, by providing for more complete sharing of information.

For almost every terrorist attack, pre-hospital emergency medical services (EMS) will be one of the "first responders," perhaps before an event has been identified as terrorism. EMS providers will need decisions early about where to transport victims, and what additional precautions may be needed. Standard procedures must include explicit decision-making protocols for medical, public health, and EMS providers.

In the same way that medical personnel should be held to certain standards for certification, **medical authorities must establish standards for hospital facilities that include minimum capabilities in every hospital to treat victims of a terrorist attack**. An attainable near-term goal should be the requirement that each hospital have at least one chemical decontamination facility; that requirement should be included as part of the periodic certifications by such entities as the Joint Commission on Accreditation of Healthcare Organizations and the National Commission on Quality Assurance.

The nexus between foreign terrorist threats and domestic vulnerabilities is particularly noteworthy in the context of infectious diseases. The more that the U.S. health community can be aware of infectious diseases anywhere in the world and from whatever source, the more likely it can prevent or respond to the intentional introduction of a disease domestically. CDC works with the World Health Organization (WHO) to identify, track, and respond to infectious disease outbreaks of international significance. The Department of Defense also contributes to what the WHO calls its "networks of networks" throughout the global health community.[65] Although not specifically designed for combating terrorism, these efforts provide the U.S health community with a foundation for heightened awareness of and response to biological terrorist threats.

Clarify Authorities and Procedures for Health and Medical Response

State public health entities have the primary role in the control of disease outbreaks, including those intentionally inflicted. The Federal role is almost exclusively one of support to States upon request.[66] The corollary is that public health entities will have a primary role in response to a terrorist attack with a biological agent.

Virtually all States have some statutory basis for undertaking extraordinary measures, such as quarantine, in the event of a major attack. In several cases, however, the statutes are ambiguous, because of the broad authority given to State public health officials to take whatever steps necessary to respond to such an incident.

---

[65] For more information, see *Global Health: Framework for Infectious Disease Surveillance,* GAO/NSIAD–00 –205R.

[66] There is, however, authority for Federal quarantine in exceptional circumstances. See 42 U.S. Code, Section 264 and related regulations, 42 CFR Chapter 1, Part 70.

The National Office for Combating Terrorism should review existing Federal and State authorities for mandatory or prescriptive activities, such as vaccinations, quarantine, containment, and observation. As a result of that review, "model" legislation and regulations should be promulgated for the consideration of the States. The National Office for Combating Terrorism should also provide, as part of its information "clearinghouse" function, reports that will ensure that Federal, State, and local response entities have a mutual understanding of the authorities and procedures at all levels of government.[67]

Improve Stockpiles

Adequate stockpiles of vaccines should be created and made accessible for rapid response to a terrorist biological attack. Such stockpiles include 40 million doses of effective smallpox vaccine[68] and officials should make provisions for improved storage and dissemination[69] of these and other vaccines, including new ones as they are developed and perfected. Much remains to be done to ensure effective distribution of vaccines, including better coordination with State and local agencies, improving the technical infrastructure for the actual distribution, developing technical protocols for mass distribution, and informing the public about vaccines and other medication.

Evaluate and Test Response Capabilities

As part of a broader program for evaluating preparedness, medical entities such as the Joint Commission on Accreditation of Healthcare Organizations should conduct periodic assessments of medical facilities and capabilities. Evaluation criteria should include a comprehensive, clear, coordinated, and testable response plan.

Given the fact that multiple hospitals and other treatment facilities may be involved in treating the victims of a terrorist attack, such facilities should jointly develop hospital networking processes (using, for example, a "lead hospital" concept, with other hospitals in support).

Once established, medical facilities should test their plans, preferably annually, and ideally through a multi-disciplinary exercise with all response disciplines—law enforcement, fire services, pre-hospital emergency medical services, emergency managers, medical care providers, and public health.

[67] We have learned that a number of State and local public health agencies do not realize that there is Federal quarantine authority in 42 U.S. Code, Section 264.
[68] CDC recently contracted for the 40 million doses.
[69] The recent TOPOFF exercise highlighted existing problems in the delivery and distribution of vaccines, antidotes, and prophylaxes.

PROMOTING BETTER RESEARCH AND DEVELOPMENT AND DEVELOPING NATIONAL STANDARDS

The sophistication of CBRN weapons and the ambiguity of terrorists' motives and capabilities highlight the need for better coordination in research, development, testing, and evaluation (RDT&E). The costly nature of in-depth RDT&E and the need for rigid protocols and consistency make it unlikely that individual States can undertake this task.

Federal agencies conduct or fund RDT&E that has some application in combating terrorism—the Department of Justice; numerous entities in the Department of Defense;[70] the Department of Health and Human Services, especially several entities of the Centers for Disease Control and Prevention, the National Institutes of Health, and the Food and Drug Administration; the Department of Energy, including most of the National Laboratories; the Department of Agriculture; the Department of Transportation; the Department of the Treasury; the Environmental Protection Agency; and major national not-for-profit entities such as the National Academy of Sciences and the Institute of Medicine. The Congress has also provided major RDT&E funding directly to educational or other not-for-profit institutions, including the Dartmouth College Institute for Security Technology Studies and the Oklahoma City National Memorial Institute for the Prevention of Terrorism. In addition, private commercial and industrial sectors conduct significant related research, some of it Federally funded.[71]

The Technical Support Working Group (TSWG), an interagency body with oversight from the Department of State and program management and support from the Department of Defense, is accomplishing significant technical work in research and development for combating terrorism. Its "technical co-chairs" are the Department of Defense, the Department of Energy, and the Federal Bureau of Investigation. It has members from numerous Federal agencies. Its stated mission is to "Conduct the national interagency research and development program for combating terrorism through rapid research, development, and prototyping."[72] It serves as an adjunct of the "Interagency Working Group on Counterterrorism"[73] under the NSC structure. It does not, however, conduct or coordinate *all* R&D for combating terrorism, but only those projects that member agencies choose to have it coordinate. The TSWG represents an important activity. **We recommend that the TSWG become an adjunct to the National Office for Combating Terrorism in the same manner that it now serves in the NSC process**

[70] Including special programs in the Office of the Undersecretary of Defense for Acquisition, Technology and Logistics; the Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict; the Defense Research and Engineering Directorate; Defense Advanced Research Projects Agency; the Defense Threat Reduction Agency; the Joint Program Office for Biological Defense; the U.S. Army Medical Research Institute for Infectious Diseases; the U.S. Army Medical Research Institute for Chemical Defense; the U.S. Army Soldier and Biological Chemical Command; the U.S. Air Force; the U.S. Navy Force Protection Division; and the U.S. Marine Corps.

[71] It is not apparent that the OMB/NSC budget submission includes combating terrorism RDT&E funding in all Federal agencies.

[72] TSWG Mission Statement from: www.tswg.net

[73] Presumably the NSC Counter-Terrorism Security Group.

and that it expand its coordination role for technical aspects of RDT&E for combating terrorism.

There is, however, no comprehensive national plan—one that establishes clear priorities and precludes unnecessary duplication—for RDT&E for combating terrorism. The White House Office of Science and Technology Policy (OSTP) has spent many months simply taking inventory of the various Federal RDT&E programs that have application for combating terrorism.

Improve Plans for Research, Development, Test and Evaluation for Combating Terrorism

The national strategy developed by the National Office for Combating Terrorism must contain a clear set of priorities for RDT&E. The program and budget authority of that office must be exerted to ensure effective application of Federal funds devoted to this purpose.

The White House Office of Science & Technology Policy should play a major role in the effort. **We recommend that the Assistant Director for RDT&E and National Standards of the National Office for Combating Terrorism either enter into a formal relationship with OSTP or have appropriate members of the OSTP staff detailed to the National Office for Combating Terrorism on a rotational basis.**

Wide varieties of equipment that have potential application for combating terrorism[74] are available from commercial vendors. Nevertheless, many local responders have told us that some equipment they purchased does not meet the specifications described by the vendor. At present, no viable program is in place for testing and evaluating the effectiveness of equipment for combating terrorism. **We recommend that the Assistant Director for RDT&E and National Standards develop equipment testing protocols and continue to explore the prospect of financial support from vendors for equipment live agent test and evaluation, leading to Federal certification**.

We recommend that the Assistant Director for RDT&E and National Standards develop, as part of the national strategy, a comprehensive plan for long-range research for combating terrorism; this should include better coordination among the National Laboratories. The focus of those efforts by National Laboratories should be dual- or multi-purpose applications.

The National Office for Combating Terrorism should also integrate other indirect, yet applicable, research and development projects into its information-dissemination process. For example, the Deputy Directorate for Operations (Combating Terrorism) within the Joint Staff provides executive seminars on its *Best Practices Study* for anti-terrorism and force protection. This program also collects information on "commercial off the shelf" resources and equipment to support its anti-terrorism mission. These studies and

[74] According to the National Institute for Occupational Safety and Health, at least 2,000 different pieces of respiratory equipment have potential use in chemical environments.

resources may not directly relate to policy and standards for combating terrorism at the State and local level but may well contribute to State and local preparedness.

The top priorities for targeted research should be responder personnel protective equipment (PPE); medical surveillance, identification, and forensics; improved sensor and rapid-readout capability; vaccines and antidotes; and communications interoperability.

Develop National Standards for Equipment, Training, and Laboratory Processes

One of our basic assumptions is that no single jurisdiction is likely to be capable of responding to a major terrorist attack without outside assistance. That leads to the inescapable conclusion that the development of national standards is a critical element of any national plan. Firefighters or EMS technicians in the jurisdiction where an attack takes place must not be concerned that responders from other jurisdictions, providing "mutual assistance," will arrive with equipment of a different standard than local responders, even at risk of becoming casualties themselves.

We recommend that the Assistant Director for RDT&E and National Standards in the National Office for Combating Terrorism establish a national standards program for combating terrorism, focusing on equipment, training,[75] and laboratory processes. The fundamental objectives for equipment standards will be nationwide compatibility, and dual-/ multi-purpose applications. For training, they will be interdisciplinary curricula, and training exercises based on realistic scenarios. For laboratories, the focus should be clear, strict protocols for identification, forensics, and reporting. The ultimate goal of the national standards program should be certification of the specific equipment, training, or laboratory and a recapitulation of certifications in a "Consumers Digest," for use by response entities nationwide.

We recommend that the National Institute for Standards and Technology (NIST) and the National Institute for Occupational Safety and Health (NIOSH) be designated as Federal "co-lead agencies" for the technical aspects of standards development. The Executive Branch and the Congress should provide resources for the development of national standards, and Congress should be presented with a detailed budget request for that purpose at the earliest opportunity. In addition, the Interagency Board for Equipment Standardization and InterOperability should be subordinated to the National Office for Combating Terrorism.

The Federal co-lead agencies should develop certification standards in coordination with appropriate Federal agencies and with advice from State and local response entities, professional organizations that represent response disciplines, and private and quasi-public certifying entities.

[75] In this context, we intend "training" to include initial and continuing training and education, as well as training exercises.

ENHANCING EFFORTS TO COUNTER AGRICULTURAL TERRORISM

In our first report, we noted that terrorists could cause economic and social damage by targeting a State or regional agricultural sector. There we said:

> [A] concerted biological attack against an agricultural target offers terrorists a virtually risk-free form of assault, which has a high probability of success and which also has the prospect of obtaining political objectives, such as undermining confidence in the ability of government or giving the terrorists an improved bargaining position. This may be especially true if the agricultural bioterrorism attack is part of a carefully planned escalation . . . to attain the terrorists' ultimate objectives . . . with minimal risk to the terrorists themselves.[76]

A successful attack on a sector of U.S. agriculture could cause economic destabilization at home and disrupt overseas commerce, as well as create fear and panic. The U.S. agricultural sector continues to be vulnerable to agroterrorism, given the vertical integration of livestock breeding, transportation, and marketing, and the high degree of genetic homogeneity and concentration found in the nation's main crop-growing regions.

In the coming year, the Advisory Panel will consider the adequacy of efforts to counter such threats, through a continuing examination of programs of the various entities of the U.S. Departments of Agriculture[77] and of Health and Human Services[78] for prevention, preparedness, response, and recovery for agricultural bioterrorist attacks. That review will include capabilities for surveillance and response for plant and animal diseases, laboratory protocols and standards, and information sharing. The Advisory Panel will consult with veterinarian and other professional organizations as part of that process.

[76] First Report, p. 13–14.
[77] Including the Animal and Plant Health Inspection Service, the Food Safety Inspection Service, and the Agricultural Research Service.
[78] For example, the Food and Drug Administration for food safety issues.

PROVIDING CYBER SECURITY AGAINST TERRORISM

The cyber attacks incident to the current conflict in the Middle East emphasize the potentially disastrous effects that such concentrated attacks can have on information and other critical government and private sector electronic systems. In addition, several Distributed Denial of Service attacks[79] in early 2000 against high profile Web-based businesses (e.g., Yahoo, Amazon, Ebay, and CNN) demonstrated the vulnerabilities of the "e-commerce" infrastructure. Law enforcement responses to such attacks similarly illustrate the great difficulty of quickly identifying the perpetrators.

In a terrorism context, cyber attacks inside the United States could have "mass disruptive," if not "mass destructive" or "mass casualty" consequences. It is easy to envision a coordinated attack by terrorists, using a conventional or small-scale chemical device, with cyber attacks against law enforcement communications, emergency medical facilities, and other systems critical to a response. Moreover, it is conceivable that terrorists could mount a cyber attack against power or water facilities or industrial plants—for example, a commercial chemical plant that produces a highly toxic substance—to produce casualties in the hundreds or thousands. The most likely perpetrators of cyber-attacks on critical infrastructures are terrorists and criminal groups rather than nation-states. That view has led to an assumption that detection of such attacks might fall to law enforcement agencies rather than to traditional national security authorities or, more probably, to the private sector.

Beginning with the report of the President's Commission on Critical Infrastructure Protection (PCCIP) in October of 1997, the Federal government has sought to mitigate critical infrastructure vulnerabilities and potential disruptions to critical services. Government officials recognized immediately that the vulnerabilities in cyber-dependent critical infrastructures[80]—those deemed vital to the economic and national security of the United States—require unprecedented collaboration with the private sector, because most critical infrastructures are under private ownership. A crucial dimension is the extent to which the defense establishment is becoming more dependent on private infrastructures.

---

[79] A distributed denial of service attack (DDOS) is one in which a cyber attacker first compromises a number of electronic "host" networks, and installs a "daemon" on those hosts. A "daemon" is a computer process that runs in the background and performs a specified operation at predefined times or in response to certain events. Later, the attacker sends a request to the daemon on the compromised hosts asking it to begin flooding a target host with various types of electronic packets. The ensuing massive stream of data overwhelms the victim's hosts or routers, rendering them unable to provide service. For further information, see http://staff.washington.edu/dittrich/misc/ddos/elias.txt; http://www.sans.org/ddos_roadmap.htm; and http://packetstorm.securify.com/distributed/TFN2k_Analysis-1.3.txt

[80] Non-defense critical information infrastructures include the banking and financial services infrastructure, the electric power generation and distribution system, the oil and natural gas pipeline and storage system, the air and rail transportation systems, water supply systems, vital human services, and continuity of government.

Two documents serve as a foundation for a national framework. The first, released in May of 1998, is Presidential Decision Directive 63 (PDD-63). That document established specific Federal agency responsibilities, response timelines, and milestones for Federal government planning for critical infrastructure protection (CIP). A key milestone was the publication of a national plan for the defense of U.S. critical infrastructures by the beginning of calendar year 2000. In January 2000, a plan was released: *Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0–An Invitation to Dialogue* (the "National Plan").

PDD-63 called for the establishment of Information Sharing and Analysis Centers (ISACs) to facilitate information sharing between government and industry on infrastructure vulnerabilities and threats. To date, the electric power, telecommunications, banking and financial services, and oil and gas storage and distribution sectors have established such entities. While still embryonic, ISACs have the potential to increase greatly the effectiveness of Federal government responses to critical infrastructure threats, including terrorism.

The Congress has not funded many of the initiatives proposed by the Executive Branch in the last two fiscal years to implement elements of the "National Plan." The Congress has recognized that critical infrastructure protection is a vital area for governmental activity but has withheld certain funding pending the receipt of information from the Executive Branch and further debate.[81]

Much more needs to be done to establish effective partnerships with the private sector and to improve planning and coordination with State and local government entities. Private sector collaboration is vital to an effective longer-term response to all aspects of CIP—deterrence, detection, identification, prevention, response, recovery, and restoration. The private sector remains skeptical of the Federal government's intentions in CIP. Mistrust and a fear that CIP may provide a rationale for re-regulating recently deregulated industries have slowed industry responses to Federal government coordination and problem-solving initiatives.

As the Y2K remediation process clearly indicated, many of the critical infrastructures requiring protection are owned or in some way regulated by State and local governments. In almost every case, those governmental entities provide some measure of physical protection for facilities and for people who work there. In any attack, they will play important roles in response, recovery, and restoration. We urge all Federal entities with CIP responsibilities to include State and local representatives in the planning and implementation of CIP programs.

[81] A bill requiring a comprehensive report from the President to the Congress on the implementation of the requirements of PDD-63, presumably including the status of the various activities directed in the "National Plan" (originally introduced as S. 2702 - the "Bennett-Schumer Bill") was added as Section 1032 of the National Defense Authorization Act for Fiscal Year 2001 (H.R. 4205), which was signed into law on October 30, 2000 (Pub L. 106–398)

During the coming year, the Advisory Panel will focus on specific aspects of CIP, as they relate to the potential for terrorist attacks. We have identified several areas for further deliberation. We will make specific policy recommendations in our next report.

CIP Policy Coordination at the Federal Level With Sufficient Authority to Oversee CIP Programs

Currently, the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, has certain CIP policy oversight responsibilities, among many others. Those various responsibilities are very broad, and may prevent the Coordinator from giving sufficient attention to the CIP challenge. Moreover, the person with policy oversight of CIP programs needs program and budget authority, perhaps similar to the authority that we have recommended for programs to combat terrorism generally. We have chosen not to include CIP within the purview of direct responsibilities in the National Office for Combating Terrorism. The nature of the threats to our critical infrastructure and the processes required to defend against and mitigate attacks are much broader than terrorism.

Standards

The nation lacks an overarching framework for coordinating with industry and various entities in Federal, State, and local government on the development of cyber and information technology standards. This includes, in particular, security standards for emerging technologies (*e.g.*, wireless) and for significant Internet applications, such as business-to-business transactions for critical infrastructure services.

Currently, the responsibility to coordinate cyber standards development rests, both directly and indirectly, in three offices in the Executive Office of the President:

Office of Management and Budget—Coordinates development of minimum computer security guidelines and standards for the Federal government, in concert with the National Institute for Standards and Technology, pursuant to multiple statutes and authorities; and with the Department of Defense, through the National Security Agency, for the development of security standards for *national security systems*.[82]

National Security Council—Coordinates national and economic security policy issues associated with cyber security.

White House Office of Science and Technology Policy—Coordinates research and development associated with cyber security standards.

[82] See, *e.g.*, Computer Security Act of 1987 (Pub. L. 100–235), Clinger-Cohen Act of 1996 (Pub. L. 104–106), and the National Defense Authorization Act for FY 2000 (Pub. L. 106–65).

The Advisory Panel will consider the extent to which those entities and appropriate standards-setting bodies within the Executive Branch[83] should develop a single framework to coordinate efforts with similar industry-led efforts.

CIP Alert, Warning, and Response

The National Infrastructure Protection Center (NIPC) at the Federal Bureau of Investigation (FBI) has certain responsibilities for critical infrastructure alert, warning, and response coordination, including cyber attacks by terrorists. The NIPC has been told that many of the intended activities will present insurmountable legal issues. Moreover, there are inherent difficulties in achieving a close trust relationship between elements of the private sector and any governmental agency. That problem is magnified when it is essentially a law enforcement agency such as the NIPC.

There have been discussions in the Executive Branch and in the Congress about shifting the forensic and technical support functions of the NIPC to other centers—perhaps to an expanded Computer Emergency Response Team Coordination Center (CERTCC) (currently housed at Carnegie Mellon University)[84] or to the General Services Administration Federal Computer Incident Response Center (FedCIRC)[85]—with the suggestion that such a move could leverage cyber-investigative expertise already present and would lower barriers to acceptance of a more central Federal role in CIP preparedness. Nevertheless, it is not obvious that either of those entities currently possesses the requisite capabilities, in personnel, equipment, expertise, or authority, to perform the functions. It has also been suggested that another non-law-enforcement component of the Treasury Department or an entity in the Commerce Department or in the Defense Department could be given the mission. The Advisory Panel will consider these and other potential solutions in its future deliberations.

Liability and Other Legal Issues

A number of entities have identified legal and practical impediments to cyber security cooperation. The President's Commission on Critical Infrastructure Protection, the Defense Science Board, and, most recently, the "National Plan," each identified a range of legal authorities and policies that may undermine CIP collaboration. Private sector institutions focusing on CIP, such as the Partnership for Critical Infrastructure Security[86] and the Financial Services ISAC,[87] similarly argue that Federal and State governments should identify and remove significant legal impediments to greater cyber security

[83] For example, the National Institute for Standards and Technology, for minimum computer security standards, and the National Communications Systems, for public telephone network standards.
[84] CERTCC coordinates the nationwide CERT community, an ad hoc collection of CERTs from universities, the private sector, and governments agencies.
[85] FedCIRC is the government-wide computer emergency response facility housed at GSA. It is charged with coordinating federal agency computer virus outbreak and intrusion detection announcements and responses. FedCIRC concentrates on U.S. government computer systems outside of DoD.
[86] See http://www.pcis-forum.org/.
[87] See http://www.fsisac.com/.

cooperation.[88] Issues frequently identified include tort liability, antitrust implications, patent and copyright protection, Freedom of Information Act and Privacy Act issues, and the lack of insurance to cover these and other cyber-related matters.

In its deliberations in the coming year, the Advisory Panel will consider legal implications that may be raised in the context of cyber terrorism.

Additional Research into Terrorist Threats to Critical Infrastructure

The Advisory Panel will also consider whether significant additional research is needed for terrorism aspects of CIP. Areas to be considered include threat analytical capabilities (with a focus on tracking technical capabilities of terrorist organizations, along with their propensity to utilize such tools) and emerging technologies for defensive, recovery, and restoration operations. We will also consider the advisability of independent research and development initiatives for CIP, where the private sector could, for example, receive tax credits or grants to conduct research in critical infrastructure assurance and protection.

[88] See, for example, *Critical Foundations: Protecting American's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection* at Chapters 4 - 7 (October 1997) (emphasizing the significance of fostering private sector information-sharing processes and, ultimately, greater information sharing between industry and government at all levels.); and *Information Warfare Defense*, Defense Science Board Task Force on Information Warfare (November 21, 1996) (recommendations to the Department of Defense on supporting the Defense Information Infrastructure; information-sharing was identified as a significant issue).

Conclusion

The work of the Advisory Panel will continue in 2001, and will culminate with the submission of our third and final annual report to the President and the Congress on December 15, 2001.

The Advisory Panel will proceed with its review and analyses of existing Federal programs that are designed to support or enhance domestic preparedness programs for terrorist incidents, with emphasis on those specifically mentioned in the enabling legislation: training, communications, equipment, planning requirements, the needs of maritime regions, and coordination among the various levels of government.

We will devote considerable attention to issues involving the use of the military, cyber terrorism aspects of critical infrastructure protection, and health and medical programs, especially those of the Centers for Disease Control and Prevention.

APPENDICES

APPENDICES

APPENDIX A—ENABLING LEGISLATION

Following is an extract of the legislation that created the Advisory Panel and provided its mandate. The provision originated in the U.S. House of Representatives and was sponsored by Representative Curt Weldon of Pennsylvania.

- -

An Extract of
PUBLIC LAW 105-261 (H.R. 3616, 105th Congress, 2nd Session) (October 17, 1998)

An Act

To authorize appropriations for fiscal year 1999 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe personnel strengths for such fiscal year for the Armed Forces, and for other purposes.

- -

SECTION 1. SHORT TITLE; FINDINGS.

a. **SHORT TITLE-** This Act may be cited as the "Strom Thurmond National Defense Authorization Act for Fiscal Year 1999."

- -

SEC. 1405. ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION.

a. **REQUIREMENT FOR PANEL-** The Secretary of Defense, in consultation with the Attorney General, the Secretary of Energy, the Secretary of Health and Human Services, and the Director of the Federal Emergency Management Agency, shall enter into a contract with a federally funded research and development center to establish a panel to assess the capabilities for domestic response to terrorism involving weapons of mass destruction.
b. **COMPOSITION OF PANEL; SELECTION-** (1) The panel shall be composed of members who shall be private citizens of the United States with knowledge and expertise in emergency response matters. (2) Members of the panel shall be selected by the federally funded research and development center in accordance with the terms of the contract established pursuant to subsection (a).

c. **PROCEDURES FOR PANEL-** The federally funded research and development center shall be responsible for establishing appropriate procedures for the panel, including procedures for selection of a panel chairman.

d. **DUTIES OF PANEL-** The panel shall--
   1. assess Federal agency efforts to enhance domestic preparedness for incidents involving weapons of mass destruction;
   2. assess the progress of Federal training programs for local emergency responses to incidents involving weapons of mass destruction;
   3. assess deficiencies in programs for response to incidents involving weapons of mass destruction, including a review of unfunded communications, equipment, and planning requirements, and the needs of maritime regions;
   4. recommend strategies for ensuring effective coordination with respect to Federal agency weapons of mass destruction response efforts, and for ensuring fully effective local response capabilities for weapons of mass destruction incidents; and
   5. assess the appropriate roles of State and local government in funding effective local response capabilities.

e. **DEADLINE TO ENTER INTO CONTRACT-** The Secretary of Defense shall enter into the contract required under subsection (a) not later than 60 days after the date of the enactment of this Act.

f. **DEADLINE FOR SELECTION OF PANEL MEMBERS-** Selection of panel members shall be made not later than 30 days after the date on which the Secretary enters into the contract required by subsection (a).

g. **INITIAL MEETING OF THE PANEL-** The panel shall conduct its first meeting not later than 30 days after the date that all the selections to the panel have been made.

h. **REPORTS-** (1) Not later than 6 months after the date of the first meeting of the panel, the panel shall submit to the President and to Congress an initial report setting forth its findings, conclusions, and recommendations for improving Federal, State, and local domestic emergency preparedness to respond to incidents involving weapons of mass destruction. (2) Not later than December 15 of each year, beginning in 1999 and ending in 2001, the panel shall submit to the President and to the Congress a report setting forth its findings, conclusions, and recommendations for improving Federal, State, and local domestic emergency preparedness to respond to incidents involving weapons of mass destruction.

i. **COOPERATION OF OTHER AGENCIES-** (1) The panel may secure directly from the Department of Defense, the Department of Energy, the Department of Health and Human Services, the Department of Justice, and the Federal Emergency Management Agency, or any other Federal department or agency information that the panel considers necessary for the panel to carry out its duties. (2) The Attorney General, the Secretary of Defense, the Secretary of Energy, the Secretary of Health and Human Services, the Director of the Federal Emergency Management Agency, and any other official of the United States shall provide the panel with full and timely cooperation in carrying out its duties under this section.

APPENDIX B—PANEL CHAIR AND MEMBERS

Name and Affiliation	Expertise
The Honorable James S. Gilmore, III, Governor of the Commonwealth of Virginia, Chair	State perspective
James Clapper, Jr. (Lieutenant General, U.S. Air Force, Retired), Corporate Executive, and Former Director, Defense Intelligence Agency, Vice Chair	Intelligence
L. Paul Bremer, Corporate Executive, and Former Ambassador-at-Large for Counter-Terrorism, U.S. Department of State	Terrorism, counter terrorism
Raymond Downey, Commander, Special Operations, City of New York Fire Department	Emergency response - local
Richard Falkenrath, Associate Professor, John F. Kennedy School of Government, Harvard University	Terrorism threats
George Foresman, Deputy State Coordinator, Department of Emergency Management, Commonwealth of Virginia	Emergency response - state
William Garrison (Major General, U.S. Army, Retired), Private Consultant, and Former Commander, U.S. Army Special Operations Command's Delta Force	Special operations
Ellen M. Gordon, Administrator, Emergency Management Division, Department of Public Defense, State of Iowa, and President, National Emergency Management Association	Emergency response - state
James Greenleaf, Independent Consultant, and Former Associate Deputy for Administration, Federal Bureau of Investigation	Law enforcement - federal
Dr. William Jenaway, Corporate Executive, and Chief of Fire and Rescue Services, King of Prussia, Pennsylvania	Emergency response - local
William Dallas Jones, Director, Office of Emergency Services, State of California	Emergency Response - State
Paul M. Maniscalco, Past President, National Association of Emergency Medical Technicians, and Deputy Chief/Paramedic, City of New York Fire Department, EMSC	Emergency response - local
John O. Marsh, Jr., Attorney at Law, former Secretary of the Army, and former Member of Congress	Interagency coordination, cyber, and legal aspects

Kathleen O'Brien, City Coordinator, City of Minneapolis, Minnesota	Local perspective
M. Patricia Quinlisk, M.D., Medical Director/State Epidemiologist, Department of Public Health, State of Iowa	Health - state
Patrick Ralston, Executive Director, Indiana State Emergency Management Agency; Executive Director, Department of Fire and Building Services; and Executive Director, Public Safety Training Institute, State of Indiana	Emergency response - state
William Reno (Lieutenant General, U.S. Army, Retired), former Senior Vice President of Operations, American Red Cross	NGOs
Joseph Samuels, Jr., Chief of Police, Richmond, California, and Third Vice President, International Association of Chief of Police	Law Enforcement - local, Terrorism
Kenneth Shine, M.D., President, Institute of Medicine, National Academy of Sciences	Health - federal
Hubert Williams, President, The Police Foundation	Law Enforcement/Civil Liberties

****

Ellen Embrey, U.S. Department of Defense Representative

APPENDIX C—RESEARCH METHODOLOGY AND STRATEGY DEVELOPMENT

This is the second annual report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (hereafter the "Advisory Panel"). The mandate to the Advisory Panel, contained in its enabling legislation,[89] requires it to:

- assess Federal agency efforts to enhance domestic preparedness for incidents involving weapons of mass destruction;
- assess the progress of Federal training programs for local emergency responses to incidents involving weapons of mass destruction;
- assess deficiencies in programs for response to incidents involving weapons of mass destruction, including a review of unfunded communications, equipment, and planning requirements, and the needs of maritime regions;
- recommend strategies for ensuring effective coordination with respect to Federal agency weapons of mass destruction response efforts, and for ensuring fully effective local response capabilities for weapons of mass destruction incidents; and
- assess the appropriate roles of State and local government in funding effective local response capabilities.

The Advisory Panel is a Federal Advisory Committee,[90] and has no directive authority over any government entity.

The enabling legislation also directed that a Federally-Funded Research and Development Center provide research, analytical, and other support to the Advisory Panel during the course of its activities and deliberations. RAND has been providing that support, under contract from the Department of Defense,[91] since the Advisory Panel's inception.

This Appendix provides a full description of the Advisory Panel's deliberative process, research methods, as well as information on the structure and foundation of this report.

Research and Analytical Methodology

This report is based on a number of research and analytical efforts, including:

[89] Section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105-261 (H.R. 3616, 105th Congress, 2nd Session) (October 17, 1998). The full text of the statutory enabling provisions is contained in Appendix A.

[90] The Advisory Panel is subject to the provisions of the Federal Advisory Committee Act, 5 U.S.C. App., Pub L. 92-463, October 6, 1972, as amended.

[91] Awarded by the Secretary of Defense, following consultation with the Attorney General, the Secretary of Energy, the Secretary of Health and Human Services, and the Director of the Federal Emergency Management Agency.

- The assessment of a variety of relevant programs of various Federal agencies through direct interviews with agency representatives and exhaustive analysis of written program and budget documents
- Interviews with numerous government officials at the local, state, and federal levels
- Consultations with subject matter experts
- Oral and written presentations and other submissions to the Advisory Panel
- Case studies addressing specific issues
- Facilitated discussions among panel members
- Other quantitative and qualitative research

Some of the research is contained, either in its entirety or in synopsis form, in other appendices to this report, including Federal agency program information, case studies, and other documentation.

The Advisory Panel has also commissioned a nation-wide survey of almost 2000 response entities at the State and local levels. The results of that survey and a comprehensive analysis of the results will be contained in the third and final Advisory Panel report to the President and the Congress. For a description of the survey and a categorization of the target audience, see Appendix K.

Advisory Panel Activities

During the period since its last report, the Advisory Panel has maintained a robust meeting schedule (as detailed in Appendix O). Members and support staff have also conducted numerous additional activities, including the presentation of Congressional testimony, attending numerous Congressional hearings and Federal interagency meetings, and participation in a variety of related conferences, symposia, and workshops, all of which have assisted in informing and guiding the deliberative process.

Scope of the Report

The conclusions of the Advisory Panel, and its related recommendations, are made in the belief that the instant report, its first report, and the final report that it will submit in December 2001, will contribute to the public debate about how the nation can most effectively combat the threat of terrorism.

This report does not contain specific budgetary recommendations. It outlines, rather, several priorities for focusing limited resources. In its third and final report, the Advisory Panel will address fiscal issues at the Federal, State, and local levels.

Except for a portion of the case study on the Los Angeles Operational Area (see Appendix G), this report also does not address comprehensively one specific legislative

mandate – the consideration of the "needs of maritime regions."[92] That issue will likewise be addressed in the final report.

Preliminary Considerations

The potential for terrorist attacks inside the borders of the United States represents is an emerging threat. Effectively preparing the United States for the consequences of such attacks will require changes in the relationships among and between all levels of government. Key to these changes will be the realization that our ability to respond cannot be dependent upon a single level or agency of government. Rather we need a national approach, one that recognizes the unique skills that a community, state and the federal government possess and that, collectively, will give us the "total package" needed to address the consequences of terrorism.

In its first report,[93] the Advisory Panel concluded that, despite a number of Federal programs and a significant increase in Federal funding over a six-year period, "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." Having recognized that such a strategy was not likely to be produced in the near term, the Advisory Panel decided in March of this year to put forward its proposals with the hope that they will serve as a basic framework for that strategy. We have noted the growing frustration of local, State and Federal officials over the absence of a clear national vision and corresponding strategies, particularly in the area of domestic response capabilities. The need is clear, it is time for action, and we intend to help to build momentum toward resolution of these issues.

This Advisory Panel is unique, if for no other reason than its composition. It reflects, through the backgrounds of its members, the larger universe of local, State and Federal response disciplines that will work together to respond to the next terrorist attack on our home soil. With the addition of other members who have policy experience at the national level, its perspectives, therefore, reflect a broad strategic vision dealing with structure, programmatic, operational and policy issues. The panel is a microcosm of the larger process ultimately needed to develop fully a viable national strategy. As previously noted, a national strategy does not equate to a Federal strategy; a Federal component is only part of a national strategy. In developing a true national strategy, the role of the Federal government should be to facilitate and participate in a strategic planning process that involves States and communities as equal partners.

The conclusions and recommendations contained in this report have been informed from a variety of sources, including the vast knowledge and experience of panel members, discussions with numerous officials at all levels of government, participation in numerous

[92] Section 1405 d. 3. of the enabling legislative.
[93] *"The First Annual Report to the President and the Congress: I. Assessing the Threat," (the "First Report") was delivered on December 15, 1999. See:* http://www.rand.org/organization/nsrd/terrpanel/ to download a complete copy of the report.

activities where the issue is discussed, and written reports from various entities, both public and private. One of the most effective processes for identifying the issues most important to State and local entities has been the joint effort of the National Governors Association (NGA) Center for Best Practices and the National Emergency Management Association (NEMA) in conducting "States' Regional Terrorism Policy Forums." Emanating from those forums is a consolidated list of fifty-four "States' Recommendations," compiled in eight functional categories, in which are reflected many of the themes contained in this report.[94]

It has been suggested that several officials documents that have been published in recent years – Presidential Decision Directives 39 and 62, the Attorney General's 1999 Five-Year Interagency Counterterrorism and Technology Crime Plan, and the most recent *Annual Report to Congress on Combating Terrorism*, Including Defense against Weapons of Mass Destruction/ Domestic Preparedness and Critical Infrastructure Protection (dated May 18, 2000) – taken as a whole, provide a national strategy. We disagree. The Presidential Decision directives, for the most part, only direct assign certain responsibilities to Federal entities. The Attorney General's "Five-Year Plan," while salutary, falls short of a fully-coordinated strategy, one that is promulgated by the President; and it does not in our view have the requisite "bottom up" approach – having as its underpinnings the needs of the local and State response entities. While that document contains many significant goals and objectives, it is not apparent that there is any enforcement or other tracking mechanism to ensure that the specific objectives are tied to milestone dates, or other measures to effect its full implementation.

These documents describe plans, the description of a compilation of various programs already under way, and some objectives; but they do not either individually or collectively constitute a national strategy.

Many of the current programs have resulted from specific Congressional earmarks in various appropriations bills and did not originate in Executive Branch budget requests: They are the initiatives of concerned and proactive Senators and Representatives.

The panel recognizes that this instant report addresses only part of a comprehensive national strategy for combating terrorism. That focus is the necessary result of the panel's legislative mandate and, consequently, the structure of the panel project being limited to the fundamental elements of a "domestic preparedness and response" portion of a much broader strategy. We must avoid placing too much emphasis on preparedness for response, if it unnecessarily detracts from other necessary efforts.

The panel is also fully aware of the interdependencies among all aspects of deterrence, prevention, and response. That point cannot be overstated. States and communities have emerged as critical partners in the formulation of polices on national security, as they may have critical roles to fill in the execution of many of those policies. This concept

[94] The entire compilation of "States' Recommendations" from the NGA/NEMA States' Regional Terrorism Policy Forums is contained in Appendix J.

will require a change of culture, a new way of thinking, and more dialogue between our three levels of government. Our approach as a nation must be one of integration, focus, flexibility, and priority allocation of limited resources. We must, therefore, do a better job as a nation of planning, coordinating, and providing resources to our domestic response capabilities. It will help us achieve a better level of preparedness not only for terrorism, but all emergencies and disasters.

International and Domestic Considerations

The national strategy should be geographically and functionally comprehensive. It should address both international and domestic terrorism. The distinction between terrorism outside the borders of the United States and domestic terrorist threats is eroding. International terrorism crosses borders easily and may directly affect the American homeland. This was evident in the New York World Trade Center bombing in 1993, and more recently in the activities around the turn of the century, especially with the arrests of Ahmed Ressam in Washington State, and Lucia Garofalo and Bouabide Chamchi in Vermont. The terrorist bombings of the U.S. garrison at Khobar Towers, Saudi Arabia, the two U.S. embassies in East Africa, and the recent USS *Cole* incident, also illustrate the reach of terrorists against U.S. interests and the profound domestic implications they pose.

A complete strategy will articulate the various policy and diplomatic reasons for a robust U.S. program to combat terrorism directed against U.S. persons and interests around the world, and the advantages to engaging our allies in mutual efforts in that regard. It will likewise include the necessary linkage between international threats and their potential for domestic incidents, as well as terrorism that may have its source inside the United States.

The Relationship of Deterrence, Prevention, and Response

"The cornerstone of our recommendations for improving our efforts
to combat terrorism is that we build on existing systems,
not create entirely new ones."

To be functionally comprehensive, the national strategy should address the full spectrum of the nation's efforts against terrorism: intelligence, deterrence, prevention, investigation, prosecution, preemption, crisis management, and consequence management. As the Advisory Panel recognized in its first report, our nation's highest goal must be the deterrence and prevention of terrorism. The United States cannot, however, prevent all terrorist attacks. When deterrence and prevention fail, the nation must respond effectively to terrorism, whether to resolve an ongoing incident, mitigate its consequences, identify the perpetrators, and prosecute or retaliate as appropriate. The national strategy should deal with all aspects of combating terrorism and must carefully weigh their relative importance for the purpose of allocating resources among them.

The timely identification of potential terrorist adversaries carries significant strategic implications for deterrence, prevention, and response considerations. Our ability to detect the potential sources of terrorist activity through a variety of sources and methods is, perhaps, the most critical element in all of the activities that we as a nation may undertake to combat terrorism.[95] While it is unlikely that we will ever be able to identify in advance *all* specific threats with certainty as to time and location of an attack, the better we perform that identification function, the more effective we will be in our total effort.

It likewise logically follows that we must maintain overwhelming capability to preempt and interdict intended terrorist activity before the act occurs, as well as the capability and national will – as noted above -- to retaliate against the actual perpetrators and their direct or indirect supporters, and to prosecute perpetrators to the full extent of the law.

In developing effective response capability, adequate advance preparations obviously are key. But the question may remain: "How much is enough?" We have been fortunate as a nation that we have suffered relatively few domestic terrorist incidents, the experience from which could help to provide answers to such a question. Notwithstanding the fact that natural disasters have proven tragic in countless ways, the nation has never been faced with the consequences of a man-made attack so devastating that it could threaten the very fabric of our society. As a consequence, the answer to that question for any actual attack may have to wait for the day-after analysis.

Historical Considerations

While history may not always be the best teacher, there are perhaps any number of historical events in the last century, including some in the last decade, that may appropriately help to shape our thinking about designing, implementing, and executing an effective system for response to domestic terrorist acts.

For example, the tragic 1918 worldwide influenza epidemic, which took the lives of at least 500,000 people in the United States, and at least 20 million world wide,[96] carries with it important lessons about the need for robust medical surveillance, rapid identification, and prompt warning capabilities that will be essential in mitigating the consequences of certain terrorist attacks, especially biological ones.

U.S. civil defense efforts during the Cold War era, regardless of how well intentioned, eventually failed because they were perceived as unlikely to accomplish their stated

[95] It is, at least, arguable that it was unlikely that any reasonable detection capability or processes in existence at the time could have recognized the motivations, intentions, and capabilities of Timothy MacVeigh before his bombing of the Alfred P. Murrah Federal Building in Oklahoma in April 1995. Nevertheless, and as described in further detail elsewhere in this report, efforts must be directed at finding ways, within our constitutional and legal framework, to discern to the extent possible such conduct before an actual terrorist attack.

[96] *Preventing Emerging Infectious Diseases: A Strategy for the 21st Century*, Centers for Disease Control and Prevention, U.S. Department of Health and Human Services, October 1998, p .

purpose. If public support is to be achieved and maintained, Americans must believe that any national program for domestic response is realistic and credible.

While there are a number of anecdotes, most Americans will likely agree with the premise that we have a reasonably effective system and robust capabilities to respond to a wide spectrum of natural disasters, as well as to criminal acts of various types and magnitude. Those capabilities have evolved and improved, and are continuing to improve, at all levels of government, including cooperation and coordination vertically and horizontally.

In those situations where wartime exigencies and internal strife have caused extraordinary steps to be taken—rationing of food and other commodities, the integration of public schools in the 1960s, and responses to riots in certain cities, as examples—the actions taken by government entities at all levels have, by and large, been measured and appropriate, when considered in the context of our Federal form of government, our Constitutional protections, and our legal systems.[97]

In those fortunately few cases where terrorism has struck us at home—most notably the New York World Trade Center bombing, the Oklahoma City Murrah Federal Building bombing, and the Atlanta bombing during the 1996 Olympics—the day-after analysis of each response undoubtedly merits relatively high marks. Lessons learned from each of those events, however, suggest that there are a number of improvements that can be made—in local capabilities, in coordination among governmental entities at various levels, in forensics, in mitigation and recovery operations, and other critical functions.

The reaction to those recent incidents, coupled with the anxiety following the Aum Shinrikyo attack in the Tokyo subway in 1995, has sparked continuing debate about the question posed earlier: "How much (preparation) is enough?" The public perceptions of terrorism in the last decade have, in large measure, been driven by entertainment and news media descriptions of the most catastrophic consequences from terrorist attacks. Some senior governments officials and terrorism "experts" have contributed to those perceptions. As a result, the evolution of terrorism domestic preparedness and response processes has, to date, been influenced by such perception.

The key point here is that both the anxiety and the level of public expectation for an effective response to a major terrorist incident may have been unrealistically heightened.

Threat Analyses

Early in our deliberations, the Panel determined that we could not adequately fulfill our legislative mandate without a current, comprehensive assessment of the potential threats

[97] Examples that could be used to challenge this thesis are relatively few, but would likely include the internment during World War II of Americans of Japanese descent, the Kent State University shootings, the treatment of certain civil rights and Vietnam War protesters, the Ruby Ridge standoff, and the Waco Branch Davidians incident.

from terrorists seeking to strike Americans where we live – inside the borders of the United States. The threat assessment commissioned by the Advisory Panel is contained in its first report.[98]

The Panel fundamentally reaffirms the threat analysis contained in the first report. In recent months, other entities have arrived at essentially the same point of departure in terms of potential terrorist threats in the near term,[99] namely that conventional weapons are more likely to continue to be the "weapon of choice;" that some terrorist may decide, for any number of reasons, to attempt to use a CBRN device, but that such an attack is likely to be lower on a relative scale of consequences; and that the catastrophic event using an unconventional device—while possible and consequential enough to merit continuing vigilance and appropriate preparations—is lower on the relative scale of probabilities. We also take note of the increasing likelihood that the use of cyber attacks, to create or compound disruption, or to interfere with our response capabilities. While not a "Weapon of Mass Destruction" in the legal or technical sense, the direct or indirect consequences of cyber terrorism are nevertheless potentially devastating. It is not implausible that nation-state adversaries may turn to terrorism or other asymmetric activity as their only means to compete effectively against the overwhelming military and economic superiority of the United States.

Without comprehensive and current threat and risk assessments, the Panel believes it unlikely that public officials—at any level of government—can make informed decisions about the allocation of resources to respond to such threats.

Basic Assumptions

The conclusions and recommendations of the Advisory Panel are based on several key assumptions.

First, the threats from terrorists, whether foreign or domestic, seeking to carry out an attack inside the borders of the United States, will continue to evolve and could expand dramatically with some unexpected advance in capability.

Second, "local" response entities—law enforcement, fire service, emergency medical technicians, hospital emergency personnel, public health officials, and emergency managers, in any of several combinations depending on the nature of the attack—will *always* be the "first "—and conceivably only—response. "Local" entities in this context

[98] First Report, chapter 2.

[99] See, for examples, the report from the National Commission on Terrorism, "Countering The Changing Threat of International Terrorism," June 5, 2000, which is available on the World Wide Web at several sites, including our home page*:* http://www.rand.org/organization/nsrd/terrpanel/; and several reports and testimony of the General Accounting Office, including "Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks" (GAO/NSIAD-99-163), September 7, 1999, and "Combating Terrorism: Issues in Managing Counterterrorism Programs (GAO/T-NSIAD-00-145), April 6, 2000. The entire series of the comprehensive GAO Combating Terrorism reports and testimony can be accessed at: http://www.gao/gov.

can include elements of incorporated and unincorporated municipalities, counties, and State organizations. In every case, some combination of those entities will inevitably be involved.

Third, in the event of a *major* terrorist attack, however defined—number of fatalities or total casualties, the point at which local and State capabilities are overwhelmed, or some other measure—no single jurisdiction is likely to be capable of responding to such an attack without outside assistance. This assumption is critical to understanding the need for mutual aid agreements and coordinated operations.

Fourth—and perhaps most important—there are existing emergency response and management capabilities, developed over many years, for responses to natural disasters, disease outbreaks, and accidents. Those capabilities can and should be used as a base for enhancing our domestic capability for response to a terrorist attack. We are not, as some have asserted, "totally unprepared" for a major terrorist attack, even with a biological weapon. We can strengthen existing capabilities, without buying duplicative, cost-prohibitive capabilities exclusively dedicated to terrorism. Similarly, our capabilities to deter, prevent, or respond to a terrorist attack correspondingly enhance capabilities against similar attacks from nation-states.

The Cyber Dimension

The focus in our *First Report* was on the more unconventional weapons that terrorist might choose to employ – chemical, biological, radiological, and nuclear (CBRN). Nevertheless, we acknowledged "that the issues of cyber terrorism and the (CBRN) forms of terrorist activities . . . .are so inter-related that the Panel cannot ignore"[100] the potentially significant consequences of cyber terrorism. For that reason, we have included in Chapter Three issues related to cyber-terrorism currently under consideration by the Advisory Panel

Societal Implications

We have been fortunate as a nation. The terrorist incidents in this country—however tragic—have occurred so rarely that the foundations of our society or our form of government have not been threatened. Nevertheless, the potential for terrorist attacks inside the borders of the United States is a serious emerging threat. There is no guarantee that our comparatively secure domestic sanctuary will always remain so. Because the stakes are so high, our nation's leaders must take seriously the possibility of an escalation of terrorist violence against the homeland.

Some have suggested that a truly catastrophic event may sorely test us in that arena – that public panic, government over-reaction, the use of the U.S. Armed Forces to conduct major military activities on American soil,[101] or other factors may do long-term damage

[100] First Report, p. 67.
[101] See further discussion on this topic in Chapter 3.

or change the unique nature of American society. Such an unfortunate outcome will be much less likely if we conduct more thoughtful advance planning, coordination, and cooperation. In that vein, there are several factors that must be taken into consideration to prepare for an effective response capability.

Others have postulated that a major attack will prompt a loss, at least temporarily, of certain civil rights or liberties. We take the view that addressing such hard issues in advance, and head on, will lessen—perhaps negate—any such outcome. For that reason, the members of this panel have kept the issue of the protection of civil rights and liberties squarely in the forefront of all their deliberations.

Panel members also believe that our leadership can and must do a better job of raising the level of public awareness on this issue. In recent years, as we have noted previously, the public has for the most part been informed by depictions in the entertainment and news media, and from some others with public platforms, of mostly catastrophic terrorists attacks, leading one to the conclusion that such attacks are the most likely. American citizens can and should be given better information about the potential for terrorist attacks without heightening—perhaps even lessening—public fear.

Without better public awareness, it is less likely that government officials at all levels will be able to make fully-informed decisions about the appropriate levels of public expenditure to address domestic preparedness before the next attack. Moreover, public support in the aftermath of an actual attack will be critical. The more that American citizens can be educated about what may happen and what will be expected of them, the less likely that an incident will be exacerbated by uninformed public reaction.

Roles of Government

Fundamental to a good understanding of the Advisory Panel's approach to strategy development is an insight into the Panel's view of the appropriate role of each level of government, especially the Federal role.

Prior to an attack, the Federal government must provide national leadership, guidance, and assistance to response entities at all levels. Federal entities can facilitate nationwide preparedness by helping to develop national standards for training, exercising, and equipment programs. The Federal role is preeminent, perhaps exclusive, in the areas of research, development, test, and evaluation. Moreover, the Federal government must have the lead in collecting and analyzing intelligence and in fostering sharing intelligence and information.

When a terrorist attack is threatened or occurs, the Federal role for criminal investigation and prosecution is already very specific. The FBI has responsibility for investigations of terrorist threats and attacks. The U.S. Department of Justice then has responsibility for prosecution under various Federal criminal statutes on terrorism. Terrorist threats or attacks may also be violations of State or local law, so jurisdiction over investigations and prosecutions can be concurrent. It is, nevertheless, widely recognized at State and

local levels that the FBI and DOJ have "paramount" though not exclusive jurisdiction in both terrorism investigation and prosecution.

Otherwise, the Federal role in a response to an actual attack should be limited to assistance when requested and to meeting response requirements that exceed local and State capabilities. Response to an attack must be layered and sequential: Local entities will respond first, supplemented as necessary by State capabilities. When local capabilities are limited or exhausted, the response shifts to the State (perhaps multi-state) level. The Federal response should come only after local and State elements are so taxed that such assistance is requested or required. The Federal response should not be a major response—with the Federal response entities "in charge" of operations—except in the most extreme, the most catastrophic, situation. For such cases, detailed planning and close coordination will lessen the prospect for overreaction that could infringe civil liberties. Moreover, there are inherent problems in relying on assets at the Federal level that are many hours—perhaps days—from deployment in an actual response.

Strategic Objectives

The Advisory Panel was constrained in the development of a complete strategy for combating terrorism—one that would address all aspects of foreign and domestic issues, all elements of deterrence and prevention, and all dimensions of preparedness and response capabilities for attacks outside the United States. First, as noted previously, its enabling legislation restricts the panel's scope of consideration to domestic response capabilities, and in that context, to Federal programs. Second, the panel members are part-time "volunteers" who have other obligations. Finally, the fiscal resources allocated to the project are insufficient to do full justice to such a comprehensive strategy.

It is our intent that the strategic recommendations contained in this report be goal oriented. Only through the expression of some strategic goals can a sense of direction be given that will shape the development of priorities (especially for resource allocation) and indicate the types and level of activities that need to be undertaken. We seek to contribute to the development of well-reasoned plans before an attack, not reaction after one occurs.

The domestic preparedness strategy contained in this report is predicated on a "bottom-up" approach. The Panel has been careful to consider the needs of local response entities as the cornerstone for its recommendations. It has sought and obtained that "local stakeholder" input from a variety of sources. Nevertheless, the Advisory Panel recognizes the substantial role that the Federal government can and must play in the implementation of a complete national strategy.

States and localities are not looking to the Federal government as the panacea for all aspects of domestic terrorism response. The Federal government does, however, have several important responsibilities that it must discharge.

The Panel emphasizes building on existing response capabilities, structures, and systems. The nation has developed a reasonably effective system for responses to natural disasters, naturally occurring disease outbreaks, accidents, and for most criminal acts. It is not necessary, in our view, to create a completely separate set of capabilities for responses to terrorist attacks. Under that same philosophy, many recommendations in this report are based on the advantages that accrue in the development of new or enhancement of existing capabilities that can have dual-, even multi-purpose applications.

Timing of the Submission of this Report

This panel has been critical of certain policies and programs of the current Executive and Legislative Branches of the Federal Government. The date of the submission of this report, although coincidental, is fortuitous. The report has, therefore, been designed to provide a set of recommendations to be considered by the new Administration and the 107th Congress. This document does not purport to provide all the answers. The Panel hopes that it will contribute to public debate and stimulate action.

APPENDIX D—PERSONS INTERVIEWED*

Cheri Abdelnour
Defense Threat Reduction Agency

Lawrence Adams, Critical Incident Analysis Group
University of Virginia

Graham Allison, Ph.D.
John F. Kennedy School of Government, Harvard University

Alane Andreozzi-Beckman,
Defense Threat Reduction Agency

Anne A. Armstrong
Virginia's Center for Innovative Technology

Charles R. Bell
Marine Corps Systems Command

Timothy Beres
Office for State and Local Domestic Preparedness Support
Department of Justice

Richard Andrews
EQE International

Dr. Rick Babarsky
National Ground Intelligence Center

Ann Beauchesne
National Governors Association

Richard Behrenhausen
McCormick Tribune Foundation

Anthony S. Beverina
Digital Sandbox

Pamela Berkowsky
Assistant to the Secretary of Defense-Civil Support

D. Douglas Bodrero
Institute for Intergovernmental Research

Major Adrian Bogart
InterAgency Board for Equipment Standardization and Interoperability

Sam Brinkley,
Department of State

Aaron B. Budgor
SAIC

Michael L. Brown
Office of Emergency Preparedness
State of Louisiana

Brigadier General Eddie Cain
Joint Program Office for Biological Defense,
Department of Defense

Stephen L. Caldwell
General Accounting Office

Kwai-Cheung Chan
General Accounting Office

Lewis M. Chapman
Federal Bureau of Investigation

Jayanto N. Choudhury
Embassy of India

John Cellantano, M.D.
Office of Emergency Services
City of Los Angeles

Frank Cilluffo
Center for Strategic and International Studies

Richard Clarke
National Security Council

Jim Cline, PH.D
SAIC

Deborah Colantonio
General Accounting Office

Joseph J. Collins, Ph.D.
Center for Strategic and International Studies

Robert J. Coullahan
SAIC

Martha Crenshaw, Ph.D.
Wesleyan University

Cabell Cropper
National Criminal Justice Association

David Cullin, Ph.D.
Joint Program Office for Biological Defense,
Department of Defense

Michael Dalich
Department of Justice

Brian David,
Joint Program Office for Biological Defense,
Department of Defense

Ruth David, Ph.D.
ANSER Corporation

Frederick S. Davidson
Critical Infrastructure Assurance Office

Armand DeKeyser
Office of Senator Jeff Sessions

Mark DeMier
ANSER Corporation

Rick DeWater
U.S. Department of Agriculture

Edward P. Djerejian
James A. Baker III Institute for Public Policy
Rice University

Dan Donohue
National Guard Bureau

Stephen M. Duncan
Southeastern Computer Consultants, Inc.

N. Dale Dunham
San Francisco International Airport

Edward Edens
Committee on Armed Services
United States Senate

William W. Ellis
Congressional Research Service

Thomas Emsley
Joint Program Office for Biological Defense,
Department of Defense

Gerald Epstein
Office of Science and Technology Policy
The White House

Glenn Fiedelholtz
Federal Emergency Management Agency

Richard Fieldhouse
Armed Services Committee
United States Senate

Jonathan Fielding
University of California at Los Angeles

Woodbury P. Fogg
New Hampshire Office of Emergency
Management

John M. Fowler, Jr.
Gold Creek Technology, LLC

John Frank
InterAgency Board for Equipment
Standardization and Interoperability

Robert R. Friedman, Ph.D.
Georgia State University

Neal Fudge
Office of Emergency Preparedness
State of Louisiana

Archie Galloway
Office of Senator Jeff Sessions

Jorge Garcia
Federal Bureau of Investigation

Benjamin Garrett
Battelle

Michael J. Gilbreath, Ph.D.
Joint Program Office for Biological Defense,
Department of Defense

George Goodwin,
National Ground Intelligence Center

Lisa Gordon-Hagerty
National Security Council

John Hamre
Center for Strategic and International Studies

Daniel I. Gluckman
ISEA Safety Equipment Association

Michael Guerin
California Office of Emergency Services

John E. Guido
Texas A&M University

Don Hamilton
National Commission on Terrorism

William L. Hamilton, III
Research Planning, Inc.

Jerome Hauer
SAIC

Jane Hindmarsh
California Office of Emergency Services

Frank Hoffman
National Security Study Group

Robert V. Homsy, Ph.D.
Lawrence Livermore National Laboratories

Jeffrey Hunker
National Security Council

Kenneth H. Huffer
United States Secret Service

Christopher Jehn
Congressional Budget Office

Lieutenant Colonel William Johnson
7th Civil Support Team

Vernon M. Keenan
Georgia Bureau of Investigation

Barry Kellman, J.D.
DePaul University

Terrence K. Kelly, Ph.D.
Critical Infrastructure Assurance Office

W.O. King
James A. Baker III Institute for Public Policy
Rice University

Stephanie Kopelousos
Office of Congresswoman Tillie K. Fowler

Phil Kosnett
National Commission on Terrorism

Robert T. Kroutil, Ph.D.
U.S. Army Edgewood Research Development and Engineering Center

Thomas Kuker
National Domestic Preparedness Office

Paul B. Kurtz
National Security Council

Phil Lacombe
VERIDIAN

John Landry
National Intelligence Council

Colonel Timothy Lampe
Defense Threat Reduction Agency

Peter LaPorte
Emergency Management Agency
District of Columbia

Randall Larsen
ANSER Corporation

Major General Bruce M. Lawlor
Joint Task Force-Civil Support

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

Mary Lou Leary
Department of Justice

Howard Levitin, M.D.

Ted Macklin
Office for State and Local Domestic Preparedness Support
Department of Justice

Anne Martin
Federal Emergency Management Agency

John A. McCarthy
Critical Infrastructure Assurance Office

Alan McCurry
Office of Senator Pat Roberts

Craig A. McDowell
City of Houston

Leeanne McInnis
University of Texas

Gary McConnell
Emergency Management Agency
State of Georgia

Stanley M. McKinney
Emergency Preparedness Division
State of South Carolina

Barbara Martinez
Federal Bureau of Investigation

Timothy Miles
California Office of Emergency Services

Andy Mitchell
Office for State and Local Domestic Preparedness Support
Department of Justice

V. Alan Mode, Ph.D.
Lawrence Livermore National Laboratory

Lisa Moreno-Hix
Oklahoma City National Memorial Institute for the Prevention of Terrorism

Richard J. Morgan
Consolidated Edison

James Morhard
Subcommittee on Commerce, Justice, State, and the Judiciary Appropriations
United States Senate

Joe Muckerman
Association of National Defense Emergency Resources

Randall Murch,
Defense Threat Reduction Agency

J. Howard Murphy,
SAIC

William Navas

John T. Neuhaus
Confidential Advisory Services, Inc.

Robert Newberry
Office of the Secretary of Defense

Commander Mark E. Newcomb
United States Navy

Kyle Olsen
Research Planning, Inc.

Gerould W. Pangburn
James Madison University

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

John V. Parachini,
Center for Nonproliferation Studies
Monterey Institute of International Studies

Marcus Peacock, P.E.
Subcommittee on Oversight, Investigations and Emergency Management
U.S. House of Representatives

Tony D. Perez,
Centers for Disease Control and Prevention

Raphael F. Perl
Congressional Research Service

Ann Petersen, J.D.

Joseph Pilat
Los Alamos National Laboratory

Ed Plaugher
Arlington County Fire Department

William Pollack
Department of Energy

Peter S. Probst
Office of the Secretary of Defense

Lieutenant Colonel Bob Ranhofer
Joint Program Office for Biological Defense,
Department of Defense

Dennis Reimer
Oklahoma City National Memorial Institute for the Prevention of Terrorism

Sue Reingold
Center for Strategic and International Studies

Gary Richter
Sandia National Laboratory

David J. Rigby
Defense Threat Reduction Agency

The Honorable Laurie Robinson
Department of Justice

Gary Rowen
National Domestic Preparedness Office

Dwight D. Rowland
General Accounting Office

Richard L. Rumpf
Rumpf Associates International

Richard Scribner,
Institute for Security Technology Studies
Dartmouth College

The Honorable Jeff Session
United States Senate

John A. Shannon
SAIC

The Honorable Michael Sheehan,
Department of State

Brendan Shields
Office of Congressman J.C. Watts

Henry J. Siegelson, MD, FACEP
Emory University School of Medicine

Roman W. Sloniewsky
Critical Infrastructure Assurance Office

Suzanne Spaulding, J.D.
National Commission on Terrorism

Ellis Stanley
Office of Emergency Services
City of Los Angeles

James R. Stanton, M.S.W.
Maryland Institute for Emergency Medical Services Systems
University of Maryland

Leslee Stein-Spencer
Illinois Department of Public Health

C.H. Straub II
Office for State and Local Domestic Preparedness Support
Department of Justice

John Sullivan
Los Angeles Sheriff's Department

Patrick J. Sullivan
Arapahoe County (CO) Sheriff's Department

Chuck Swan
Joint Program Office for Biological Defense,
Department of Defense

Thomas W. Taylor, J.D.
Department of the Army

James W. Tape
Los Alamos National Laboratory

David Trachtenberg
Committee on Armed Service
U.S. House of Representatives

John Tritak
Critical Infrastructure Assurance Office

Joel Tsiumis
National Domestic Preparedness Office

Barry Turner
Australian Federal Police

Victor Utgoff
Institute for Defense Analysis

Michelle Van Cleave
National Security Concepts, Inc.

Eileen S. Vergino
Lawrence Livermore National Laboratory

A.D. Vickery
Seattle Fire Department

Charles Ward, Ph.D.
National Ground Intelligence Center

Bryan S. Ware
Digital Sandbox

Ron Watson
Los Angeles County Fire Department

Sam Watson
BioMedical Security Institute
University of Pittsburgh

William H. Webster
Attorney at Law

Captain Robert West, USN
Joint Task Force-Computer Network Defense

Shaundra Westley
California Firefighters Association

Richard M. Wheeler, Ph.D.
Department of Energy

Michelle E. White
Subcommittee on Oversight, Investigations and Emergency Management
U.S. House of Representatives

John Allen Williams, Ph.D.
Loyola University Chicago

Michael A. Williams
Department of State

Leslie Wiser
National Infrastructure Protection Center

Lee Zeichner
LegalNetWorks

---

* An "interview," for the purpose of this list, includes a formal presentation to members of the Advisory Panel, a formal interview by a panel member or support staff, the written submission or exchange of information, or informal discussions about the issues addressed in this report with panel members or support staff.

APPENDIX E—ALTERNATIVE STRUCTURES CONSIDERED

During the course of our deliberations on the issue improving Federal Executive Branch coordination for combating terrorism, the Advisory Panel considered and rejected other alternatives to the creation of an entity in the Executive Office of the President.[102] We set forth those various alternatives below, and explain the reasons why each was rejected.

Status Quo. We discussed extensively the current structure for coordination of Federal programs and activities for combating terrorism, including modification of the current processes to make them more effective. We acknowledge the improvements that have been made in Federal Interagency coordination but we adjudged the current structure and processes inadequate, for the following reasons.

- Lack of Political Accountability—The senior person with day-to-day responsibility for Federal programs for combating terrorism—the National Coordinator for Security, Counter-terrorism, and Infrastructure Protection—is not Presidentially-appointed and Senate-confirmed. A career employee of the Executive Branch holds the position. It is essential that the person responsible for these processes must be a senior-level Presidential appointee, confirmed by the Senate.
- Insufficient Program and Budget Authority—The current structure relies on a very involved process of interagency "coordinating groups" which depends heavily on meetings to get things done. While there is opportunity for discussion and for suggestions to improve programs, there is no real authority to enforce program or budget changes. Moreover, that the current format for budget submissions is insufficient in detail to prove useful in the budget deliberative process.
- Lack of Adequate Resources—The current NSC structure lacks sufficient staff even to oversee the Federal coordination structure—there is no inherent directive authority to require Federal agencies to detail support personnel—much less to engage State and local entities in the process of developing national strategies and implementation plans.
- Lack of State and Local Expertise—The current structure lacks the resources to accommodate the resident State and local staff expertise that is required to build strategies and plans with a true "bottom up" approach.

"Enhanced" FEMA. We considered the prospect of providing additional authority and responsibility to the Federal Emergency Management Agency. The "FEMA Option" was appealing because of its designation as the Lead Federal Agency for "consequence management," and its existing statutory and regulatory authority for disaster response.[103] But we likewise discounted that option for three reasons:

---

[102] See Chapter Two.

[103] Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended. 42 U.S. Code, Chapter 68 (42 U.S. Code, Sections 5121–5204).

- Domestic Only Responsibility—FEMA has a domestic-only focus. Once we made the determination that the Federal coordinating entity should have both foreign and domestic responsibility, this is not a viable option.
- Autonomy and Neutrality Issues—Even if FEMA were given additional authority to oversee the programs and budgets of other Federal agencies for combating terrorism (including the authority to direct other agencies to detail personnel to FEMA), it is likely be the case that the exercise of that authority would be viewed by other agencies as parochial, creating the type of interagency "turf" issues that have arisen in other contexts. By the same token, the person in FEMA with the responsibility for this coordination[104] would be answerable to an internal hierarchy and not likely, therefore, to have the requisite autonomy.
- Lack of Visibility and Access. Injecting the responsibility for coordinating programs to combat terrorism into an existing agency with other programs was an issue. FEMA's responsibilities are much broader than simply consequence management for domestic terrorist attacks. Terrorism issues might be subordinated to FEMA's other programs. Moreover, the "director" of this activity in FEMA would not have the same measure of direct access to the President, as would the director of an entity in the Executive Office.

Department of Justice (DOJ). There has been at least one proposal[105] for the creation of a new senior official in DOJ. We considered that option, but discarded it for many of the same flaws that we found in an "enhanced FEMA."

- Domestic Only Responsibility—It is unlikely that any entity in the Department of Justice could be configured to transcend a domestic-only focus. Once we made the determination that the Federal coordinating entity should have both foreign and domestic responsibility, this would not be a viable option.
- Law Enforcement/Prosecutorial Focus—The DOJ generally, and the FBI in its "Lead Agency" role for "crisis management" specifically,[106] have often been criticized for having too much of a law enforcement and prosecutorial focus in their approach to combating terrorism, which detracts from their ability to coordinate non-law enforcement activites. That same criticism applies to the decision to place the National Domestic Preparedness Office inside the FBI, and to have it headed by an FBI Special Agent. Even with a structure organized around a Deputy Attorney General, perhaps even with personnel detailed from other Federal agencies, it is difficult to envision a DOJ structure that could overcome this perception.

[104] It is unlikely that the Director of FEMA could have this responsibility personally and directly, because of the other significant requirements that FEMA has by statute and regulation

[105] Contained in the U.S. Senate version of the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act for Fiscal Year 2001 (H.R. 4690). The provision was not contained in the version that emerged from the conference between the House and Senate. H. Rept. 106-1005. That version, which has now passed both houses, is awaiting Presidential signature or a threatened veto for other reasons.

[106] Pursuant to Presidential Decision Directive 39.

- Autonomy and Neutrality Issues—For the same reasons that we stated for FEMA, a DOJ entity would likely be viewed as parochial. Although DOJ has a number of Federal programs designed to assist in the efforts to improve domestic response capabilities for terrorism,[107] that may be more of a negative than a positive consideration. Any modification to those programs, approved by a Deputy AG, would likely be interpreted as the "Department taking care of its own." By the same token, even a Deputy AG, vested with the responsibility for coordinating programs for combating terrorism, would be answerable to the Attorney General, and not likely, therefore, to be viewed as having the requisite autonomy.

- Lack of Visibility and Access. Having the responsibility for coordinating programs to combat terrorism inserted into an existing agency with other programs was also an issue that we considered for the "DOJ option." DOJ's responsibilities cover everything from the responsibility for overseeing the entire Federal criminal prosecutorial system, to major civil litigation, to immigration and naturalization, to running Federal prisons. It is not likely that combating terrorism would be high on the Department's priority list. Moreover, a Deputy AG would not have the same measure of direct access to the President, as would the director of an entity in the Executive Office.

Other Federal Departments. Other cabinet-level departments, most notably the Department of Health and Human Services and the Department of Defense, were considered but discounted for many of the same reasons cited for other agencies. In addition, the Department of Defense would not be appropriate, politically palatable, or publicly acceptable to assume the role of "lead agency."

Stand-Alone Presidential Advisory Council. We considered the merits and demerits of having a council or commission to advise the President on national strategy and policy for combating terrorism. There is much day-to-day work to be done in the coordination of programs that span many Federal agencies, and that requires regular coordination with State and local response entities. There are, nevertheless, considerable advantages to the concept of having knowledgeable individuals providing such advice and assistance. For that reason, we have included such a structure in our proposal for the National Office for Combating Terrorism, through our recommendation for the establishment of a national "Advisory Board for Domestic Programs."

[107] Major combating terrorism programs are resident in the Office of Justice Programs, especially in the National Institute of Justice and the Office for State and Local Domestic Preparedness Support.

APPENDIX F—ISRAEL CASE STUDY

The author of this report visited Israel in August-September 1999, to study that country's understanding of the CBRN terrorism threat and the measures that have been taken there for both prevention and preparation.

Introduction

Two major factors color the potential for learning from Israeli counter-terrorism (CT) experience. On the one hand, Israel has an unfortunately rich history of dealing with terrorism, and has accumulated more than fifty years of strategic, tactical and technical CT experience. On the other, Israel is an extremely small country, many of its CT institutions are national and unified (as opposed to local and independent), and thus relatively easy to manage, and its legal system is far more permissive towards law enforcement vis-à-vis the country's citizens than is its American counterpart. While these latter must give American policymakers pause when considering implementation of Israeli CT lessons in the United States, the fact remains that Israel has a wealth of technological and practical experience that is currently lacking in the United States, and there is much to be learned from its institutions and individuals.

Israel's concerns with CBRN weapons date to the mid-1960s, when Egypt used chemical weapons during its involvement in the Yemeni civil war. At that time, Israel's parliament, the Knesset, passed a law mandating the procurement of protective gear (masks and atropine injectors) for each and every Israeli citizen. Until the run-up to the Gulf War, the protective gear was stored in warehouses. Since then, civilians have kept their individual protective kits in their homes. What is important to note here is that Israel has amassed more than 30 years' worth of experience in developing the means to protect *civilians* from the threat of chemical and biological weapons (CBW). This experience has manifested itself in the development of several generations of personal protective equipment (PPE) as well as strategy.

While the main CBRN threat is still seen to come from neighboring states at wartime (indeed, it is now assumed that CBW will be used against both soldiers and civilians in any future war),[108] it is has been suggested that Palestinian terrorists may seek employ chemical agents against Israeli civilian and military targets.[109] That said, a number of experts suggest that the massive and often alarmist attention given to the CBRN terrorism issue by American officials and the American media in recent years in fact helps to build the atmosphere of fear that terrorists seek to create. Further, they posit that continued widespread, overt discussion of the issue in these terms might make CBRN terrorism a self-fulfilling prophecy. One Israeli professor has even begun to include Secretary of

[108] Amos Harel, "Non-Conventional Warfare Becomes Conventional," *Ha'aretz*, July 20, 1999.

[109] While impossible to verify using open-source materials, one of the leaders of the Egyptian terrorist group, "Gama'at al-Jihad," told the London daily, *al-Hayat*, that his group and Osama bin Laden's "al-Qa'idah" had biological and chemical weapons and had plans for 100 attacks against American and Israeli targets around the world. Salah, Muhammad, "*Musa'id al-Zuahari l-"al-Hayat": lidayna aslahah biolojiya wakimawiya* (Assistant to al-Zuahari to "al-Hayat": We Have Biological and Chemical Weapons)," *Al-Hayat*, Monday, April 19, 1999.

Defense Cohen's July 1999 *Washington Post* op-ed piece, "Preparing for a Grave New World" in his terrorism courses' reading lists as an example of what he sees as counterproductive hysteria. This is not to say that these officials and experts want to hush all discussion of the subject. Rather, they prefer a more organized and deliberate information campaign that would inform the public about ongoing mitigation and prevention efforts (e.g., telling the public that anthrax is treatable). Israeli officials believe that terrorists would find CBRN weapons less attractive if the government took measures to reduce public panic and by making it known that the country is prepared to deal with the CBRN threat.

American-Israeli CT cooperation in general, and CBRN CT cooperation in particular, is not new. A number of Memoranda of Understanding (MOUs) govern an already prosperous relationship between the two countries' defense establishments. The Ministry of Defense (MOD) on the Israeli side and the Office of the Secretary of Defense (OSD) (defense issues) and National Security Council (NSC) (CT issues) in the United States manage the coordination of this relationship, which includes joint research and development (R&D), operations and development of doctrine. Following their July 1998 meeting in Washington, DC, President Clinton and Prime Minister Barak indicated that a new MOU would be signed to widen cooperation in the field of CBRN CT.

Another area of mutual concern that was discussed between the two leaders was the growing threat of WMD [weapons of mass destruction] terrorism. This was acknowledged to be an area in which both countries stood much to gain from each other's knowledge and experience. In order to enhance their capability to deal effectively with this threat, it was agreed to sign a new MOU between their respective national security institutions. It would facilitate broad cooperation between the various government agencies in both countries in all areas associated with preparing and responding to WMD terrorism.[110]

A senior Israeli defense official pointed out, however, that this new MOU would, in fact, only be formalizing a relationship that has already been functioning for some time.

This essay, the fruit of an August-September 1999 fact-finding trip to Israel, presents some of the fields in which the United States can benefit from Israeli know-how and/or in which future cooperation can benefit both countries' efforts to combat CBRN terrorism.

Ministry of Defense NBC Protection Division

A 1995 MOU has fostered a technical R&D relationship between the United States and Israel. A bilateral steering committee meets every six months to discuss current and planned projects. Representing the United States is the Office of the Assistant Secretary of Defense for Special Operations & Low-Intensity Conflict (OASD [SO/LIC]). Representing Israel is the Ministry of Defense NBC (Nuclear, Biological and Chemical) Protection Division.

[110] The White House, Office of the Press Secretary, "Joint Statement by President Clinton and Prime Minister Ehud Barak July 19, 1999," Washington, DC, July 19, 1999.

- **Mission of the NBC Protection Division**

The NBC Protection Division was established following the Gulf War of 1991 and is the organization responsible for R&D in the field of chemical and biological (CB) defense for all branches of the armed forces and the Home Front Command (HFC).[111]

The NBC Protection Division has numerous responsibilities, ranging from directing basic research and managing the infrastructure in CB defense, to developing and maintaining laboratories, research centers, and installations for analysis, initiating research and feasibility studies, through the full scale development of protective equipment.

The NBC Protection Division covers all aspects of CB protection, including individual and collective protection, the development of tools and methods for detection and identification, decontamination and medical treatment, as well as threat analysis, risk assessment, and modeling the behavior and dispersion of pollutants.

Finally, the NBC Protection Division acts as a senior advisory body to the MOD and the Israel Defense Forces (IDF) General Staff for issues of CBRN doctrine and threat analysis. The broad nature of the division's many activities means that its staff deals with everything from respirator system batteries to policy decisions regarding the stockpiling of medication, and was reflected in the number of topics raised by division staff.

The main focus of the NBC Protection Division's activities is the wartime CBRN threat. While there are important, recognized differences between the preparations needed for wartime CBRN attack and a terrorist CBRN attack, the former are seen as a base for the latter.

- **Research and Development**

In the late 1970s, the MOD began to study how the Israeli public reacted to the gas masks that the government was then stockpiling. The results of this research led to domestic development of protective kits for children, for whom standard gas masks were found to be inappropriate for a variety of reasons (e.g., the varied sizes and shapes of children's heads and their impatience for wearing uncomfortable masks). Further experience was gained during the Gulf War, when 300-400 thousand children used domestically produced protective equipment. Recently, the U.S. Army bought approximately 3,500 Israeli kits for dependent women and children of personnel in South Korea.

Further R&D is ongoing for adult civilian as well as first responder PPE. Israeli experience has demonstrated that hood-based systems are more comfortable, easier to don and allow for greater user activity (e.g., search and rescue operations under CBW conditions) than traditional mask systems. A new hood-based system, known as the First Responders Mask (FIRM) has been developed as part of the technical cooperation program with OSD, and according to the specifications of a number of American

[111] Descriptive information taken from the NBC Protection Division's information packet.

agencies. The system has undergone physiological testing in cooperation with the Army Research Lab at Edgewood Area, Aberdeen Proving Ground, Maryland.

FIRM has run into a problem that is frequently mentioned by American officials dealing with CBRN terrorism – the lack of clear standards for non-military CBRN PPE. According to National Institute for Occupational Safety and Health (NIOSH) rules, products such as FIRM must be approved before their employment by first responders. At the time of this writing (late 1998), FIRM had been held up in the NIOSH review process for more than six months.

The NBC Protection Division has also made progress in the development of computer-based, real time models that use current meteorological data to simulate the dispersion of biological and chemical agents.[112] Such models for battlefield dispersion are not new. However, in response to the terrorist threat, the NBC Protection Division has expanded these models to include chemical and biological agent behavior in urban areas as well as in enclosed spaces (e.g., malls, tunnels, etc.). The Division is also developing a number of CBW detectors.

- **Response to the Biological Threat**

Historically, most Israeli efforts for protecting the population from CBRN weapons have focused on chemical weapons. However, following the Iraq crisis of January/February 1998, at which time Scott Butler told the New York Times that Iraq had enough biological weapons to "blow away Tel-Aviv,"[113] Israel began to direct significantly more attention to the biological threat. Israel now stockpiles anthrax vaccine, in addition to the stocks of atropine and antibiotics already in place.[114] Currently there are enough doses of antibiotics in storage to supply the entire country.

Ministry of Defense, Office of Strategic Dialogue and Cooperation, Directorate for Foreign Affairs, Arms Control & Regional Security

This office is the main point of contact for cooperation between the MOD and both OSD and NSC.

- **General**

The office's representative reiterates that both states and terrorist groups threaten Israel with CBRN weapons. He contrasts these threats with those of the United States, where there is no threat to the home front from foreign states (except for that of strategic nuclear weapons), but the terrorist threat may come from *individuals* as well as groups. He

[112] Ahi Raz, "*Tokhnat mahshev tahazeh kivun hitpashtut halakh ba'avir*" (Computer Program Will Predict the Direction of Chemical Agent Dispersal in the Air), *Bamahaneh*, October 23, 1998.
[113] "Security Council Members Criticize Butler for Comments," Associated Press, February 5, 1998, Internet: http://cnn.com/WORLD/9802/05/iraq.butler.ap/index.html .
[114] According to media reports, a locally developed anthrax vaccine is currently being tested on an unspecified number of Israeli soldiers. "Report: Israeli Army Conducting Trials with Anthrax Vaccine," Associated Press, September 26, 1999.

accepts the "when, not if" premise of CBRN terrorism. He also points out that unlike traditional counter-terrorism measures, which have come in response to attacks (e.g., the increased security measures employed by El Al after the 1968 hijacking of an aircraft from Rome to Algeria), measures to counter CBRN terrorism must be researched, developed and deployed in advance of such an attack.

- **The Biological Threat**

A medical surveillance system is being developed featuring mapping software for determining geographic morbidity patterns. As mentioned above, Israeli equipment and doctrine are being developed in large part in conjunction with OSD.

- **Refining the Response to CBW Terrorism**

Since its founding in 1992, the HFC has been training to deal with chemical and biological attacks in Israel's towns and cities, and it was considered the most natural force of first responders to CBW terrorist attacks as well. However, the HFC is made up primarily of reservists who typically would be mobilized in advance of Israel being attacked. Mobilization takes time (up to 48 hours for full national mobilization). By its very nature, terrorism often comes as a surprise and is likely at peacetime as well as during war. It has become clear that a more appropriate role for HFC responders is to support and supplement the true first responders to any security incident – the national Israel Police, the Fire Service, Israel's emergency medical service, *Magen David Adom* (MDA), and the Ministry of the Environment (MOE).

The Israel Police is in command of emergency services at peacetime, and has formulated its CBRN terrorism response doctrine for all relevant bodies with the assistance of the HFC.

- **Treatment of Victims**

Israeli treatment doctrine has responders bring victims to the hospital as soon as possible (i.e., before being decontaminated), while in the United States, decontamination typically takes place near the scene of the incident. The reasoning behind the Israeli doctrine has two elements. First, it will be difficult to control the population following a CBRN incident and many ambulatory victims will arrive at the hospital on their own before being decontaminated. Second, the Israelis do not share the apparent American concern for contaminating rescue vehicles. A study by the IDF Medical Corps indicates that victims with light and moderate chemical exposure are likely to have low concentrations of CW material in their clothing. Stripping, covering and transporting the victim in a vehicle with its windows open is believed to be safe and effective. For more heavily exposed victims, special vehicles probably will be required. This system is in the process of being examined, and it is likely that experiments using chemical and biological simulants will be performed.

- **Exercises**

Israel runs periodic large-scale disaster exercises, including simulated CBW missile and terrorist attacks. One unique feature of the Israeli exercises that is often impossible to implement in the United States for various legal and other considerations, is the use of chemical and biological simulants to gain experience with and measure the effectiveness of protective gear (both in terms of design and employment) and modeling software. American officials have shown particular interest in this aspect of Israeli exercises. A number of American officials from the military and the first responder communities have observed Israeli exercises in the past and have been invited to future exercises as well.

Brigadier General (Res.) Yehiam Sasson, Office of the Prime Minister, Counter-Terrorism Bureau

- **Threat**

General Sasson emphasizes the psychological impact of the CBRN terrorism threat, pointing to the panic among the Israeli population before and during the Gulf War and during the above-mentioned 1998 Iraq crisis. He points out that a large-scale attack is not necessary in order to achieve the psychological effects desired by terrorist groups, which already have crude CBW at their disposal (e.g., off-the-shelf chemicals, insecticides). Further, the acquisition of materials (as opposed to their production), whether by purchase or theft, or the blowing up of a production facility would give terrorist groups CBRN capabilities while demanding no special technical expertise. Moreover, without strict global supervision of military CBW, the general believes that these weapons will eventually fall into the hands of terrorist groups.

Despite all of this, General Sasson points out that most terrorist groups are rational actors, and as such are concerned about such things as public opinion, possible exposure of nearby non-target populations and Israeli retaliation. He believes this latter largely explains why CBRN weapons have not been used on a large scale to date.

- **Preparation**

According to General Sasson, the CBRN terrorism threat makes worst-case analysis impossible. The magnitude of worst-case scenarios is so large that policymakers are virtually paralyzed into inaction and do not know how to properly evaluate the true extortive capability of the terrorists. This puts a premium on preparation, which improves the authorities' abilities to cope and make sound decisions during crises, and on prevention, which will require worldwide cooperation.

- **United States-Israel Cooperation**

General Sasson points to a number of fields where American-Israeli cooperation would be most productive, including intelligence (to include technical intelligence), detection

and identification equipment development for before, during and after CBRN weapon use and continued R&D in first responder PPE.

- **Public Awareness**

(This topic will be addressed at greater length in the HFC section below.)

The CT Bureau supports limited public discussion of the CBRN terrorism issue for two main reasons. First, if done wisely, prior familiarity with the issue and the government's preparations will mitigate panic. Second, not only does the public want to be told what to do in times of crisis, doing so will make the job of responders far easier as well.

Major General Gabi Ofir, Commanding Officer, IDF Home Front Command (HFC)

The HFC was established on February 17, 1992 in the wake of the Gulf War, the first war in which the Israeli home front was the main theater of operations for the IDF. At wartime, the HFC is in command of all emergency services in the country. The HFC is responsible for providing Israel's citizens with a complete protection package. The responsibilities that go along with providing this package include the setting of building standards to withstand conventional and unconventional attacks, the distribution and maintenance of personal protective kits (the main components of which are a mask and an atropine injector), the administration of vaccines and other large-scale medical services, the operation of the national early warning alert/siren system and a "lookout" system to quickly identify bomb and missile strike sites, and the decontamination of areas hit with CBW.

The HFC has devoted considerable efforts into developing a reliable and efficient public information system, which is used during war- and peacetime. This system will be reviewed in greater detail below.

While the HFC is, by design, geared toward wartime response to foreign missile and bombing threats, the terrorism issue has been receiving attention for about one year. The HFC has been working continuously with the Israel Police to develop the latter's response doctrine for CBRN terrorism.

Colonel Avi,[115] Head, Doctrine, Development & Rescue Department, HFC

One of the main ideas guiding Colonel Avi's work is the importance of speed. Responders to a CBW incident must understand exactly what has happened as quickly as possible. This information must then be passed on to decision makers and other responders so that appropriate policy and emergency decisions can be made in a timely fashion.

[115] In accordance with standard practice, IDF officers who are not public figures are identified here only by first name.

In addition to the development of HFC response doctrine, Colonel Avi has been involved in the preparation of other bodies for CBRN response. Some points on preparation:

- As part of the Israel Police's preparations for CBW attack, police mobile units have been equipped with PPE.
- In line with the Israeli approach that has patients decontaminated at hospitals rather than in the field, MDA's job in the field is almost purely for transportation.
- The HFC, though primarily based on reservists, is ready to support the civilian rescue services as needed. The HFC maintains active duty, rapid response medical teams throughout the country. Additionally, there are rescue teams and an NBC team that can quickly respond anywhere in the country.[116]

- **Information**

Colonel Avi reiterates that information forms a critical part of HFC response doctrine. In the meantime, however, a political decision has been taken not to discuss the CBRN terror issue publicly at great length, so as "not to make it stand out too much." In any case, the threat is not seen to be as great as is, for example, the Iraqi surface-to-surface missile threat.

The focus on information is part-and-parcel of the importance that the HFC attributes to psychological issues. This is also reflected in the fact that every HFC rescue battalion includes a Civilian Behavior Officer (CBO). The CBO acts as a population barometer, finding out what people know and feel, and what they don't. They provide immediate, on-site psychological support services to the traumatized population and policy advice to commanders and officials dealing with that population. The CBO also provides psychological support to the rescuers themselves, who are typically exhausted and worried about their loved ones at home, in addition to the fact that they have been exposed to the victims of a disaster in their most grotesque states.

Lieutenant Colonel Revital, Head, Civilian Information and Training Branch, HFC

The Gulf War demonstrated the intense psychological forces at work among a population under the threat of both conventional and unconventional weapons. The HFC has devoted a great deal of effort to familiarizing the public with various civil defense topics in the belief that these efforts will lead to 1) greater public cooperation in times of emergency; 2) a reduced level of panic; 3) improved ability of a traumatized public to return to life as usual after danger passes; and 4) a reduction in the attractiveness of CBRN weapons in the eyes of the enemy due to well publicized, effective Israeli consequence management. The goal is to have a calm yet alert public.

Israel, like the United States, has a large number of foreign language-speaking immigrants among the population. As such, the HFC's public information materials are produced in Hebrew, Arabic, English, Russian, Amharic (an Ethiopian dialect), and in sign language.

[116] See also Harel, "Non-Conventional Warfare Becomes Conventional."

There are five primary topics covered by HFC information campaigns: 1) preparedness; 2) behavior during times of crisis; 3) personal protection kits; 4) sealed/security rooms in the home; and 5) evacuation.

The Civilian Information and Training Branch, in conjunction with the IDF Spokesperson's Unit, annually briefs the nation's broadcasters on relevant civil defense topics as well as on how they should behave during times of emergency. Television and radio stations are provided with pre-recorded HFC informational video- and audiotapes for use during specific crises (e.g., chemical weapons attack) as well as a file of pre-written official announcements. The Civilian Information and Training Branch with the help of psychologists from the Civilian Behavior Branch write these announcements, which also address specific civil defense issues. The motivation behind these briefings and prepared statements is the perceived importance of uniformity in information coming from official channels in order to reinforce the authority and reliability of such information.

The HFC has soldier-instructors (all females) who provide instruction to fifth- and sixth-graders across the country on civil defense matters. Thus, by age 11 all Israeli students have been introduced to the threats that the Israeli home front faces, what is being done to deal with these threats and what their responsibilities are as civilians.

The HFC also runs a national information center. The center has a limited staff at peacetime, but in times of crisis the staff can be augmented to meet increased demand for services. Here, too, language issues are important and are addressed by multilingual operators. Fax service is available for hearing impaired citizens.

During peacetime, the Civilian Information and Training Branch takes advantage of and creates opportunities to reach the public. The Branch places notices in newspapers (again, in various languages), publishes a special section in the telephone directory and has informational brochures available at municipalities around the country. These notices and publications deal with a variety of civil defense topics, including proper techniques for preparing a sealed room or shelter, how to wear a mask, how to behave when a siren is heard, earthquakes, fires, hazardous materials and important telephone numbers. Newspaper notices often have to do with the opening and closing of protective kit distribution centers.

The HFC has a number of other methods for reaching the public. Media coverage of HFC exercises is invited, including an annual CBW drill in educational institutions. The IDF Internet site (http://www.idf.il/ – Hebrew/English), features an HFC section that provides information answers to frequently asked questions, in addition to covering most of the topics addressed in the telephone directory pages. The soldier-instructors visit companies and other organizations, in addition to the above-mentioned schools. Finally, there is an annual "Home Front Week" – in fact, an intensive awareness campaign.

During wartime, the HFC will run a "telemesser," which is a dial-up automated information system. The manned national information center will shift to 24-hour/seven-

day staffing and regional centers will be opened as well. HFC representatives will be assigned to municipal hotline centers around the country. IDF Radio will have a mobile team broadcast from the center so that frequently asked questions can reach as broad an audience as possible. Prepared HFC circulars will be carried by the newspapers and topic-specific brochures will be distributed locally. The HFC will provide officials to be interviewed by the media. Additionally, the HFC maintains a list of specialists who can address relevant issues in times of crisis. These specialists receive briefings from the HFC about how to work with the various media outlets. The number of operating distribution stations for protective kits and information can jump from 16 (normally operating) up to over 100. Finally, the HFC Behavior Branch will operate its "Population Center," a kind of war room for dealing with civilian issues before and as they arise. The HFC has trained a cadre of Emergency Population Instructors (again, all females) for assisting in local crisis management.

The Civilian Information and Instruction Branch is currently working with the Israel Police to address the latter's information needs for dealing with CBRN terrorism.

Yitzhak Goren, Deputy Director General, Ministry of the Environment (MOE)

The Ministry of the Environment is responsible for dealing with all types of chemical dangers in Israel, including CW terrorism. The CW terrorism threat has been included in ministry procedures and exercises since about 1994. From the standpoint of the MOE, the only differences between an accidental spill and a terrorist attack are the probable location (i.e., in an urban area as opposed to an industrial zone) and, thus, the number of victims. These differences make response time more important.

The MOE has been working with the Israel Police and the Fire Service to help them prepare for the possibility of CW terrorism. To date, thousands of police officers have already taken courses dealing with event identification, management and assessment.

The MOE's Chemical Materials Treatment School runs a number of incident management courses annually for local authorities, Fire Service and IDF personnel, and additional courses for emergency dispatchers.

The MOE runs a national HAZMAT information center 24 hours a day, seven days a week in cooperation with the HFC. The information center is notified by the Israel Police and Fire Service in the event of a chemical incident, collects information and guides those in the field. Further, the center has a detailed, continuously updated record, including mapping software, of the location of all concentrations of hazardous materials in the country.

There are MOE HAZMAT treatment units throughout Israel, in addition to units run by local authorities (in full accordance with MOE standards). The units can rapidly respond anywhere in the country and are staffed by trained chemists. The units are now trained and equipped to detect and neutralize commercial as well as military chemical agents.

Mr. Goren and other officials from Israel attended an exercise in Wichita, Kansas in August 1998, and expressed interest in continued and expanded information and training cooperation with relevant American agencies.

Lieutenant Colonel Boaz, MD, Head, NBC Branch, IDF Medical Corps
Major Amnon, MD, NBC Branch, IDF Medical Corps
Boaz I. Lev, MD, Associate Director General, Ministry of Health (MOH)

These health professionals are working together to prepare the nation's medical system to deal with various CBRN threats, both from terrorism and warfare.

The medical surveillance system described above is being developed by the MOH with the IDF Medical Corps acting as a "professional advisor."

IDF Medical Corps and MOH personnel have given lectures at each of Israel's 24 hospitals. All doctors at these hospitals have received training for dealing with CBW victims. Hospitals have the necessary procedures, equipment and supplies in place to rapidly set up decontamination lines. These procedures are regularly drilled by hospital personnel in conjunction with other responder agencies, often as part of a larger regional disaster exercise.

Since the Iraq crisis, Drs. Boaz and Lev have been in constant contact with a number of American bodies, including the Department of Health and Human Services (DHHS), the Centers for Disease Control and Prevention (CDC), the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) and other DoD and local agencies.

Professor Ehud Sprinzak, The Hebrew University of Jerusalem

Professor Sprinzak, perhaps Israel's most prominent academic expert on terrorism, wrote an article, "The Great Superterrorism Scare," in the Fall 1998 edition of *Foreign Policy*. Sprinzak defines superterrorism as "the strategic use of chemical or biological agents to bring about a major disaster with death tolls ranging in the tens or hundreds of thousands."[117] In that article, Sprinzak, posits that "…as horrifying as [CBW terrorism] may be, the relatively low risks of such an event do not justify the high costs now being contemplated to defend against it,"[118] a position he still maintains.

An important point made by Sprinzak and others is that because of the political nature of terrorism, and the poor political returns that would likely result from a CBRN terrorist attack for most political movements, CBRN attacks may be more likely to be attempted by groups that are on the verge of extinction (e.g., groups that have suffered major leadership blows due to arrest or death). With little to gain or lose, such groups may want to "go out with a bang."

[117] Ehud Sprinzak, "The Great Superterrorism Scare," *Foreign Policy* 112 (1998): 116.
[118] Sprinzak, 111.

Sprinzak explains the widespread worry in the United States as being the result of three major factors: 1) sloppy thinking (i.e., the failure of most "to distinguish among the four different types of terrorism: mass-casualty terrorism, state-sponsored chemical- or biological-weapons (CBW) terrorism, small-scale chemical or biological terrorist attacks, and superterrorism."); [119] 2) vested interests (i.e., by those who make PPE, detection equipment, etc.); and 3) morbid fascination ("People love to be horrified."). [120] While believing that there are relatively few prospects for superterrorism in the near future, Sprinzak does agree that on the small-scale, tactical level, "there will be an increase in CBW use – if only because it stirs the imagination."

In policy terms, Sprinzak recommends a low-cost (i.e., in proportion to his understanding of the threat) package that includes improved international and domestic deterrence, better intelligence,[121] "smart and compact consequence management teams," psychopolitical research to gain better insight into the "psychological mechanisms that may compel terrorists to contemplate seriously the use of weapons of mass destruction,"[122] and finally, reduction of unnecessary superterrorism rhetoric.[123]

Colonel (Res.) Dr. Dany Shoham, Bar-Ilan University, Begin-Sadat (BESA) Center for Strategic Studies

Dr. Shoham is a medical microbiologist, and served as a senior analyst in the IDF's Intelligence Corps, specializing in chemical and biological warfare. In 1998, Dr. Shoham published *Chemical and Biological Terrorism: An Intensifying Profile of a Non-Conventional Threat* through the Ariel Center for Policy Research, in which he provides a detailed and well-documented chronology of Middle East and global CBW terrorism-related events, the former dating to 1964 and the latter to 1978.[124]

Dr. Shoham believes that bioterrorism is likely to be the preferred mode of CBRN terrorism due to its potential efficiency, it being indistinguishable (at least at first) from a natural event[125] and the difficulties involved in tracing its source. That said, he estimates that it is about 1½ times more difficult to acquire a BW capability than a CW capability. He makes it clear that acquiring capability does not necessarily mean that terrorists will be able to produce chemical and biological agents. Rather, these agents could be bought, stolen or transferred from a CBW-producing state. This latter is interesting in that while most analysts believe that the fear of such weapons being turned on the donor states make

[119] Sprinzak, 116.
[120] Sprinzak, 118.
[121] Perhaps indicative of the less restrictive environment in which Israeli law enforcement officials operate, Sprinzak asserts that "[p]roper CBW intelligence must be freed from the burden of proving criminal intent." Sprinzak, 121. While this would certainly make preemptive intelligence work easier, it is not clear that such an idea would fly in the United States among legislators and civil rights advocates.
[122] This call for more psychological research is echoed in Jerrold Post, M.D. and Dr. Ehud Sprinzak, "Searching for Answers: Why Haven't Terrorists Used Weapons of Mass Destruction?" *Armed Forces Journal International* 135.9 (April 1998): 16-7.
[123] Sprinzak, 118-22.
[124] Dany Shoham, *Chemical and Biological Terrorism: An Intensifying Profile of a Non-Conventional Threat* (Tel-Aviv: Ariel Center for Policy Research (ACPR), 1998), 17-28.
[125] Shoham, 10.

their transfer unlikely, Dr. Shoham suggests that terrorists could provide "a state with a cheap way to test the effectiveness and dispersal techniques of such products…" and thus, "cannot be wholly ruled out."[126]

Dr. Shoham divides the CBRN terrorism threat into three elements: 1) technical feasibility, 2) probability and 3) impact. He believes that CBRN terrorism is highly feasible (8 on a scale of 10) and would have a great impact (9/10). He believes that such an attack today is rather unlikely (3/10), though this probability is slowly "crawling" upwards. He goes beyond General Sasson's assessment regarding impact, saying that there is no correlation between dispersability/effectiveness and [psychological] impact. As for public information, he suggests finding an "information balance" that will moderate or prevent public panic.

Conclusion

The Israelis have clearly dedicated a great deal of time, thought and resources to preparing for both general and specific CBRN threats.

Israeli responders will continue to engage in large-scale, complex exercises involving CBW simulants and new PPE and detection equipment in a variety of urban and rural settings. American officials from all levels of government have taken advantage of these exercise opportunities to learn from Israeli experience and should continue to do so. It should be pointed out, however, that perhaps the most important lesson to be learned from Israeli exercises is that the exercises themselves are a vital part of the Israeli response plan. The Israelis can provide valuable assistance in the formulation and execution of a broad spectrum of exercises in the United States. The Israelis consulted for this study without exception welcomed the prospect of enhanced bilateral cooperation.

American mental health and consequence management professionals stand to benefit from the extensive work done to date by HFC psychologists, the HFC Civilian Information and Training Branch and the IDF Spokesperson's Unit. To be sure, each society's psychological needs are different, however the Israeli work in message formulation for a diverse, multilingual population, development of relationships with the mass media and integration of mental health specialists in the disaster management process is worthy of future study.

In terms of CBRN CT technology, the Israelis have much to gain from American know-how and economies of scale. The small Israeli market makes it relatively easy to stockpile antibiotics and manage crises, but it also makes R&D costs per capita quite expensive. Producing for the 270 million people that make up the U.S. market certainly holds economic advantages when compared to doing so for the six million people in Israel alone. The United States, for its part, stands to benefit from 30 years of Israeli technical and operational experience and the lessons learned from Israeli studies that are not likely to be feasible in the United States. It appears that both sides stand to gain from continued and enhanced cooperation in the CBRN CT field.

[126] Shoham, 7-8.

Abbreviations

BSD	*Biosensor Systems Design, Inc.*
BW	*Biological Weapons*
CB	*Chemical and Biological*
CBO	*Civilian Behavior Officer*
CBRN	*Chemical, Biological, Radiological and Nuclear*
CBW	*Chemical and Biological Weapons*
CDC	*Centers for Disease Control and Prevention*
CT	*Counter-Terrorism*
CW	*Chemical Weapons*
DHHS	*U.S. Department of Health and Human Services*
DoD	*United States Department of Defense*
EMS	*Emergency Medical Services*
FIRM	*First Responders Mask*
HAZMAT	*Hazardous Materials*
HFC	*IDF Home Front Command*
ICT	*International Policy Institute for Counter-Terrorism*
IDF	*Israel Defense Forces*
MDA	Magen David Adom *(Red Star of David); Israeli national emergency medical service*
MOD	*Israel Ministry of Defense*
MOE	*Israel Ministry of the Environment*
MOH	*Israel Ministry of Health*
MOU	*Memorandum of Understanding*
NBC	*Nuclear, Biological and Chemical*
NIOSH	*National Institute for Occupational Safety and Health*
OSD	*Office of the Secretary of Defense*
PPE	*Personal Protective Equipment*
R&D	*Research and Development*
USAMRIID	*U.S. Army Medical Research Institute of Infectious Diseases*
WMD	*Weapons of Mass Destruction*

Bibliography

Cohen, William S. "Preparing for a Grave New World." *Washington Post*, July 26, 1999: A19.

DeGiovanni, Cleto, Jr. "Domestic Terrorism With Chemical or Biological Agents: Psychiatric Aspects." *American Journal of Psychiatry* 156 (1999): 1500-5.

Ganor, Boaz. "Nonconventional Terrorism: Nuclear-Chemical-Biological." *Survey of Arab Affairs*, 15 August 1995.

Harel, Amos. "Non-conventional Warfare Becomes Conventional" (English). Also published as "*Hakhanah l'khimiah v'biologiah*" (Hebrew). *Ha'aretz*, July 20, 1999: 43.

Israel Defense Forces. *IDF Official Web Site*. Internet: http://www.idf.il/ .

Israel Defense Forces, Home Front Command. "*Meida' shehashuv l'da'at b'nosei hitgonenut ezrahit* (Important Information to Know about Civil Defense Matters)." *Dapei Zahav* (Golden Pages) North 06. Ramat Gan: Dapei Zahav Publishers, 1998: 56-9.

Israel Ministry of Defense NBC Protection Division. *Israel CB Defense Equipment*. Tel-Aviv: Israel Ministry of Defense, n.d.

"Israel Tries to Calm Nervous Public over Attack Threat." *CNN Interactive*, February 3, 1998. Internet: http://cnn.com/WORLD/9802/03/israel.iraq/index.html .

Krasner, LTC Esther. *Analysis of the Failure Mechanisms as Criterion for Development of Respiratory Protective Systems*. Tel-Aviv: Israel Ministry of Defense, n.d.

Post, Jerrold, M.D. and Dr. Ehud Sprinzak. "Searching for Answers: Why Haven't Terrorists Used Weapons of Mass Destruction?" *Armed Forces Journal International* 135.9 (April 1998): 16-7.

Raz, Ahi. "*Tokhnat mahshev tahazeh kivun hitpashtut halakh ba'avir* (Computer Program Will Predict the Direction of Chemical Agent Dispersal in the Air)." *Bamahaneh*, October 23, 1998.

"Report: Israeli Army Conducting Trials with Anthrax Vaccine." Associated Press, September 26, 1999.

Salah, Muhammad. "*Musa'id al-Zuahari l-"al-Hayat": lidayna aslahah biolojiya wakimawiya* (Assistant to al-Zuahari to "al-Hayat": We Have Biological and Chemical Weapons)." *Al-Hayat*, Monday, April 19, 1999.

"Security Council Members Criticize Butler for Comments." Associated Press, February 5, 1998. Internet: http://cnn.com/WORLD/9802/05/iraq.butler.ap/index.html .

Shoham, Dany. *Chemical and Biological Terrorism: An Intensifying Profile of a Non-Conventional Threat*. Tel Aviv: Ariel Center for Policy Research (ACPR), 1998.

Sprinzak, Ehud. "The Great Superterrorism Scare." *Foreign Policy* 112 (1998). Fall 1998: 110-24.

Steinberg, Gerald M. "Israeli Responses to the Threat of Chemical Warfare." *Armed Forces and Society* 20.1 (1993). Fall, 1993: 85-101.

Susser, Leslie and Yael Haran. "A Silent Terror." *Jerusalem Report*, March 29, 1999: 20-2.

"Weapons Officials Arrive in Baghdad for Fresh Round of Talks." *CNN Interactive*, January 31, 1998. Internet: http://cnn.com/WORLD/9801/31/iraq.mood/index.html .

The White House, Office of the Press Secretary. "Joint Statement by President Clinton and Prime Minister Ehud Barak July 19, 1999." Washington, DC, July 19, 1999.

Acknowledgements

The author is grateful to Mr. Moshe Fox, director of the North American Division of the Israel Ministry of Foreign Affairs and to Major General Zeev Livne (Israel Defense Forces), currently the Israeli Defense and Armed Forces Attaché to the United States, for their generous assistance, without which this study would not have been possible.

APPENDIX G—LOS ANGELES AREA CASE STUDY

This case study, conducted in Los Angeles in early 2000 by RAND at the request of the "Gilmore Commission," examines CBRN counter-terrorism policies and organization, the state of responder training, the status of federal assistance and other relevant factors in Los Angeles. The study also details the rash of anthrax hoaxes that occurred in Los Angeles starting in December 1998, and the local response to them. The Gilmore Commission believes that the lessons learned in Los Angeles are relevant to jurisdictions nationwide and that the federal government can 1) aid in the dissemination of the lessons learned in Los Angeles in the course of developing its CBRN preparedness program; and 2) participate in educating agencies at all levels of government in the effective use of the methodologies employed in Los Angeles to draw relevant conclusions from experience and turn them into practice.

While Los Angeles is unique among large metropolitan areas in the United States in terms of population, area, jurisdictional structure and other factors, there is much to be learned from the experience of Los Angeles's local responders in preparing for terrorism. This case study, requested by the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (hereafter the "Gilmore Commission"), and conducted in Los Angeles in early 2000, examines the response structure, policies, state of responder training and other relevant aspects of, as well as the role the federal government has played in, terrorism preparation in Los Angeles.[127] The Gilmore Commission, having examined the state of preparedness in cities across the United States, observed that Los Angeles responders were further along in the planning and training than most other metropolitan areas. Further, the Commission believes that the lessons learned in Los Angeles are relevant to jurisdictions nationwide and that the federal government can 1) aid in the dissemination of the lessons learned in Los Angeles; and 2) participate in educating agencies at all levels of government in the effective use of the methodologies employed in Los Angeles to draw relevant conclusions and turn them into practice.

Specifically, this case study focuses on two elements of Los Angeles County terrorism preparation that are of particular interest to jurisdictions nationwide. First of these is the Los Angeles County Terrorism Early Warning Group (TEW), a collaborative, coordinating mechanism by and for local responders in the county. Second are the lessons learned from the rich experience gained in dealing with a rash of anthrax hoaxes since late 1998. Before presenting these two elements, the case study provides the reader with further background on the state and structure of terrorism preparedness as well as on local responder training in Los Angeles. Responder observations on preparing for terrorism response and a section detailing policy recommendations conclude the study.

BACKGROUND

Los Angeles County is a particularly complex operational area, with 88 different cities and 42 separate law enforcement agencies. The county has its own fire department, as do

[127] Throughout this study, "Los Angeles" refers generally to the greater Los Angeles metropolitan area.

many of the individual cities. This structure necessitates frequent and complex multi-jurisdictional emergency responses. By state law, California emergency responders follow the State Emergency Management System (SEMS), a state-specific version of the Incident Command System (ICS).[128]

In the event of a chemical, biological, radiological or nuclear (CBRN) terrorist attack, some or all of the following agencies could be expected to respond (ordered alphabetically):[129]

- Federal Bureau of Investigation (FBI), Los Angeles Field Office
- Los Angeles City Fire Department (LAFD)[130]
- Los Angeles County Department of Health Services (DHS)
- Los Angeles County Fire Department (LACoFD)[131]
- Los Angeles County Sheriff's Department (LASD)
- Los Angeles Police Department (LAPD)

LOCAL RESPONDING AGENCIES: A SNAPSHOT OF ROLES AND PROGRESS TO DATE

LASD Emergency Operations Bureau (EOB)

The EOB has a full-time Terrorism Sergeant who is responsible for coordinating the Terrorism Early Warning Group (TEW, discussed below), co-developing inter-agency terrorism response and administering a counter-terrorism technology test bed. The Sergeant provides counter-terrorism analysis for the LASD.

The EOB has headed the development of standardized training for local responders in the county. It was felt that federal training materials did not sufficiently address the specific structural and training needs of Los Angeles County. As a result, the EOB applied for, and received a $250,000 grant from the U.S. Department of Justice (DOJ) for the development of the courses and the suite of training videos mentioned above.

---

[128] The Incident Command System (ICS) is a standard management system for command, control and coordination of emergency responders used nationwide. For more information on ICS, see Federal Emergency Management Agency, Emergency Management Institute, *Basic Incident Command System (ICS) Independent Study* IS-195, January 1998. For more information on SEMS, see http://www.fema.gov/pte/exp_06.htm .

[129] This list is not intended to be exhaustive. Depending on the nature, scale and location of the incident, various local responding agencies might be involved (e.g., Los Angeles World Airports have their own, separate police force).

[130] Including the department's Hazardous Materials Unit (HAZMAT).

[131] This includes HAZMAT and Health/HAZMAT. The Health/HAZMAT Division of the Los Angeles County Fire Department oversees HAZMAT units and is the county authority for determining when a contaminated area is sufficiently clear of contaminants.

LAPD

The LAPD Emergency Operations Section is responsible for the development of policies and procedures relating to LAPD response to "unusual events." In this capacity, the EOS authors and distributes the LAPD *Emergency Operations Guide* and the *Supervisor's Field Operations Guide*, which feature sections on terrorism awareness and response. Since 1998, these sections have addressed the possibility of CBRN as well as conventional attacks.

The LAPD Anti-Terrorist Division's primary objective is "the prevention of significant disruptions of public order in the City of Los Angeles." The ATD investigates individuals or groups that "plan, threaten, finance, aid, abet, attempt or perform unlawful acts that threaten public safety."[132] Both the EOS and ATD are represented in the TEW.

Fire Departments—Los Angeles County Fire Department (LACoFD) & Los Angeles City Fire Department (LAFD)

As there are many law enforcement agencies in the Los Angeles area, so too for fire departments. LACoFD and LAFD each maintain a three-unit HAZMAT task force and has a terrorism coordinator. Battalion Chiefs from both LACoFD and LAFD co-chair the Inter-Agency Board's (IAB) Subgroup on Personal Protective Equipment (PPE).[133] The equipment list used by the National Domestic Preparedness Office (NDPO) and later adopted by the IAB was largely formulated in Los Angeles. LAFD played a dominant role in the anthrax hoaxes that took place in the city in late 1998. As of August 2000 all LAFD and LACoFD personnel have been trained to conduct mass casualty decontamination and are equipped to do so as well.

LACoFD Health/HAZMAT Division

The Health/HAZMAT Division is responsible for the enforcement of HAZMAT-related federal, state and local environmental laws in Los Angeles County. In the event of a HAZMAT incident, CBRN or otherwise, this office is the only authority in the county that can certify a contaminated area as clean. As such, Health/HAZMAT technicians fill a supervisory role over the HAZMAT units within the county that are charged with the actual cleanup of contaminants. This function puts a premium on identification of hazardous material. Thus, Health/HAZMAT plays a lead role in the early identification of CBRN agents.

Los Angeles County Department of Health Services (DHS)

---

[132] *Official Website of the Los Angeles Police Department*, http://www.lapdonline.org/ .

[133] The IAB consists of leading subject matter experts from local, state and national response organizations and is co-chaired by DoD and DOJ. The IAB has developed a standardized equipment list for WMD response operations, which ensures equipment standardization and interoperability at the local, state and federal levels. See *Combined Statement of Department of Defense Witnesses: Preparedness for a Biological Weapons Attack*, http://www.nbcindustrygroup.com/document1.htm .

DHS is actively involved in a number of aspects of CBRN terrorism preparation. Among these are TEW participation, the expansion of the disease surveillance system to include symptoms caused by potential biological agents, the establishment of the Metropolitan Medical Response System,[134] the stockpiling of CBRN treatments and the training of medical and paramedical personnel.

Caches of medical supplies are maintained at several sites throughout the county, and can be transported by ground or air.

All paramedics in Los Angeles County – public and private – receive their training through DHS. The five-month course now includes three hours of CBRN response training. DHS has trained personnel at over 50 county hospitals in CBRN treatment. Notably, this latter training has come completely from the DHS budget, with no financial assistance from any federal programs.

Los Angeles World Airports (LAWA)

Los Angeles World Airports is the one of two financially self-sufficient departments in the city, funded entirely from takeoff, landing, and other airport fees. The department operates its own police force, which is separate from LAPD. By virtue of the size and importance of Los Angeles International Airport (LAX), it was felt that the airport was a particularly attractive target for terrorists. LAWA owns several mobile mass decontamination units, which it operates in cooperation with LAFD. Via mutual aid agreements, these units contribute to the overall preparedness of the Los Angeles area, a fact demonstrated during the DNC when they were pre-positioned for use.

COORDINATING TERRORISM RESPONSE

In 1996, in an effort to coordinate the terrorism response efforts of the various relevant agencies operating there, Los Angeles County formulated its first terrorism response plan. As a result of this effort, two coordinating bodies emerged (see Figure 1). First is the Terrorism Working Group. In 1996, the Los Angeles operational area established the TWG, to be chaired by the inter-agency Los Angeles County Office of Emergency Management (OEM). The key members are the FBI, the LASD, the city and county fire departments, DHS, as well as the California Office of Emergency Services. The TWG guides broad policy and facilitates most of the county's counter-terrorism planning, training and grant application efforts. The TWG convenes regularly, and has no operational role during a terrorist event. It is overseen by the county's Emergency Management Council, which is comprised of the county's Chief Administrative Officer, Sheriff, Fire Chief and the heads of other key county departments. The TWG tasks some specific policy-related oversight to three subcommittees: the Bioterrorism Working Group, the Metropolitan Medical Response System (MMRS) Management Committee, and the Grant Steering Committee.

[134] Los Angeles is also the home of the Western National Medical Response Team.

The second terrorism response coordinating body in Los Angeles County, which does have an operational role, and informs the policy decisions of the TWG, is the Terrorism Early Warning Group. Because of this operational role in coordinating the county's response to a terrorist event, it is of particular interest to this analysis.

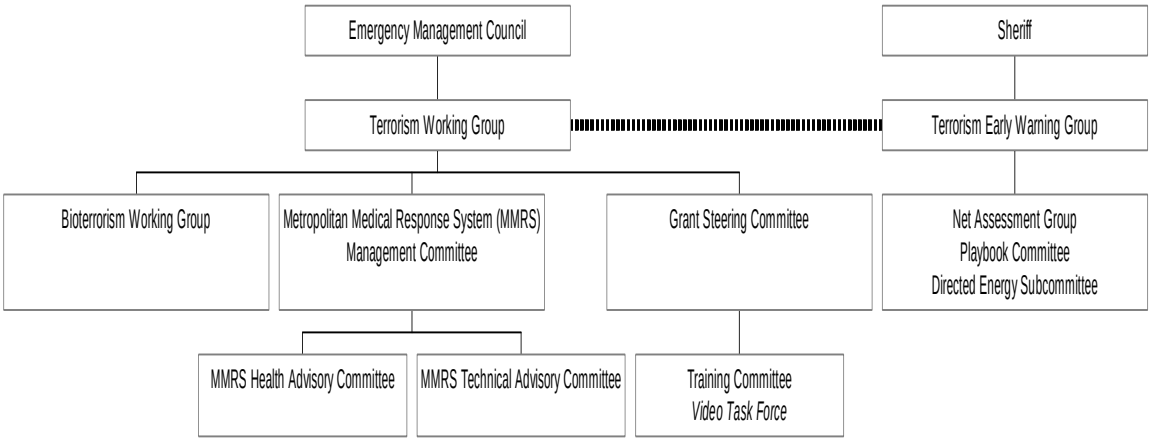


Figure 1. TWG Organizational Structure. Courtesy of Los Angeles County Sheriff's Department Emergency Operations Bureau (EOB).

TERRORISM EARLY WARNING GROUP (TEW)

TEW Mission

The role of the TEW is to monitor trends and potentialities that may result in terrorist threats or attack within Los Angeles County. Because of poor information flow between the national intelligence community and local responding agencies,[135] the TEW was founded as an indications and warning/net assessment element to evaluate open source data and research threat information in order to inform incident commanders and guide TWG training and planning efforts. The TEW works to identify precursor events when assessing trends and potential threats with an eye toward prevention and mitigation.

TEW Participants

TEW participants include core and cooperating agencies. The core agencies are the LASD, LAPD, LAFD, LACoFD, DHS and the FBI. Cooperating agencies include: California Office of Emergency Services Law Enforcement Branch, Federal Aviation Administration Security, Long Beach Emergency Management, Long Beach Fire Department, Long Beach Health Department, Long Beach Police Department, Los Angeles County District Attorney's Office, Los Angeles World Airports (Los Angeles International and Ontario Airports), Metropolitan Transportation Authority, the National

[135] There are numerous problems in the dissemination of intelligence from federal to local agencies. Aside from classic agency-proprietary "hoarding" of information, the free flow of potentially relevant information to local responders is hindered by the sensitivity of the information, much of which is classified for reasons of national security.

Security Studies Program at California State University, San Bernardino, RAND, the California Highway Patrol, the United States Secret Service, United States Customs and others.

The TEW is constituted as a committee, with its work facilitated by a Sergeant from the LASD Emergency Operations Bureau (EOB) who serves as the group's coordinator. The EOB disaster intelligence and threat assessment staff serves as group secretariat and designated interagency point of contact.

Additional members are drawn from the law enforcement, fire, and medical communities. Researchers working in national security participate to strengthen the group's ability to assess future threats. Various federal agencies also participate as *ex officio* observers.

TEW MEMBERSHIP

Public sector representatives	***Roles***
LASD Emergency Operations Bureau (EOB)	*TEW Coordinator and Secretariat*
LASD Special Investigations Section (SIS)	*LASD Crisis Management Liaison*
LAPD Emergency Operations Section (EOS)	*LAPD Crisis and Consequence Management Liaison*
LAPD Anti-Terrorist Division (ATD)	*LAPD Crisis Management Liaison*
L.A. City Fire Department (LAFD)	*Fire Service Liaison*
L.A. County Fire Department (LACoFD)	*Fire Service Liaison*
L.A. County Department of Health Services (DHS)	*Disease Surveillance/Medical Liaison*
California Office of Emergency Services—Law	*State/Law Enforcement Liaison*
California Office of Emergency Services—Fire	*State/Fire-Rescue Liaison*
Los Angeles Airport Police Bureau	*LAX Police Liaison*
Federal Bureau of Investigation	*L.A. Division Liaison*
Non-governmental representatives	
RAND representatives	*Policy Studies & Trends Identification*
National Security Studies Program, CSUSB	*Policy Studies & Trends Identification*
National Law Enforcement and Corrections Technology Center – West	*Technology Integration*
Primary "As-Needed" Members	
United States Coast Guard	*Maritime Liaison*
L. A. County Office of Emergency Management	*County Agency Liaison*
Bureau of Alcohol, Tobacco and Firearms	*ATF/ Bombing Liaison*
Immigration and Naturalization Service	*Immigration Liaison*
U.S. Customs Service (Criminal)	*High-tech (WMD) Proliferation Liaison*
LASD Arson/Explosives	*Bomb Squad*
LAPD Bomb Squad	*Bomb Squad*
LASD Computer Crimes	*Information Warfare Issues*
Metropolitan Transportation Authority	*Transit System Liaison*
Long Beach Police Department	*Crisis Management Liaison*

Table 1. TEW Membership (Courtesy of EOB)

A listing of member agencies and their roles is provided in Table 1, above. Additional agencies are incorporated into the TEW on an as-needed basis, depending upon the particular threat faced and its probable venue.

TEW secretariat personnel also act as liaison to the Sheriff's Special Investigations Section (SIS) and the LAPD's Anti-Terrorist Division (ATD). When an incident occurs, members of the TEW may augment the Plans/Intelligence Section of the County Emergency Operations Center (CEOC) or the incident's Unified Command Structure (UCS).

Monitoring Trends and Potential Threats

Since its inaugural meeting in April 1996, the TEW has been a focal point for analyzing the strategic and operational information needed to respond to and prevent terrorism and protect critical infrastructure. Special emphasis is placed on the early detection of emerging threats, including acts employing CBRN weapons and information warfare (IW or cyber-terrorism). The TEW supports the CEOC, the TWG and the Los Angeles County Metropolitan Medical Response System (MMRS). The TEW cooperates with criminal intelligence groups (such as the FBI-headed Los Angeles Task Force on Terrorism) to provide the Unified Command at a terrorist incident with a net assessment of response capabilities and the projected event horizon. To develop the analytic skills necessary to assess trends and potentials and conduct a net assessment, the group conducts regular briefings and training exercises.

TEW Monthly Meetings

Monthly TEW meetings typically start with the introduction of all participants and a brief review of the minutes from the previous month's meeting. A guest speaker, or a regular TEW participant with special knowledge then presents a briefing on a specific, relevant topic. The goal of the briefings is to educate TEW participants on emerging or changing terrorism-related issues. Recent TEW briefings have included topics as diverse as CBRN Terrorism, Advanced Terrorism Concepts and the Non-State Soldier, Future War and Terrorism (Terrorism in Strategic Context), Recent Trends: Gangs, Mercenaries and Drugs, Critical Infrastructure Protection, Preparing for Information Age Conflict, and Technology for Cyber-terrorism.

The EOB staff then gives a review of open source intelligence (OSINT). This includes local, national and international media reports and trends and milestones that have a potential local impact. Finally, each of the participants is given an opportunity to raise relevant issues that have come up or are foreseen in the coming months. The TEW meetings are beginning to include short group exercises based on hypothetical terrorism scenarios.

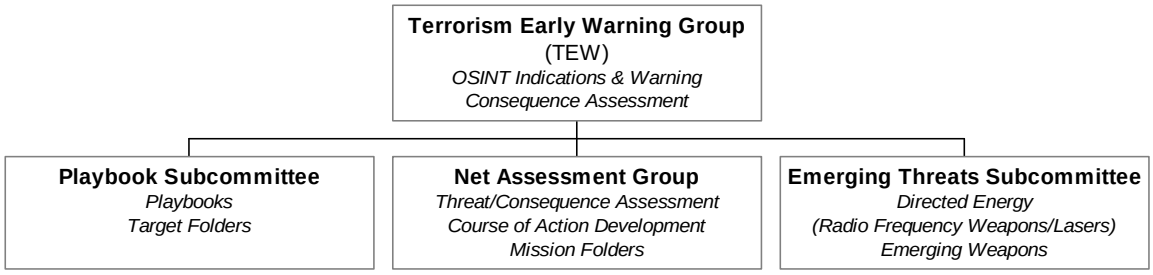


Figure 2. TEW Organizational Structure (Courtesy of EOB)

TEW Organizational Structure

In addition to the TEW's monthly general meetings to discuss indications and warnings, there are three subcommittees, whose members address specific counter-terrorism topics and tasks. The TEW's organizational structure is depicted in Figure 2.

The Playbook Subcommittee develops general guidance for responding to specific classes of threat. Biological and chemical terrorism as well as water distribution attack response playbooks already have been completed. The subcommittee is currently building food surety and radio frequency weapons (RFWs) playbooks. Future plans include work on a radiological and nuclear playbook as well as playbooks to address several other types of threats. Also in development are standardized response information folders (also known as "target folders") for key venues that might be subject to attack in Los Angeles County.

The Emerging Threats Subcommittee, previously known as the Directed Energy Subcommittee, has examined emerging weapons such as RFWs, transient electronic devices, and laser strikes against civil aircraft. These threats, while not fully mature, are evolving.

The Net Assessment Group is a subcommittee that operates when a threat emerges or an incident occurs. The Net Assessment Group develops incident-driven, task-oriented advice for the Unified Command Structure. Specifically, the group will provide the UCS with an assessment of the impact of an actual attack on the operational area, gauge resource needs and shortfalls, continuously monitor and assess situational awareness and status, and act as the point of contact for inter-agency liaison in order to develop options for courses of action toward incident resolution. In the process, the group develops an intelligence collection plan toward the development of available courses of action specific to the given threat or scenario. The courses of action are packaged with target folders and other intelligence products to create a mission folder to be delivered to the incident commander and/or other relevant players. The group is currently standardizing the mission folder format.

Figure 3 details the directions of information flow in and out of the Net Assessment Group. Using virtual "reachback" tools, the Net Assessment Group, the incident commander and/or other off-site specialists could discuss the mission folder and response parameters while they are en route to the incident scene. Five cells make up the group.

The Officer-in-Charge (OIC) Cell represents the commander's intent, and interacts with the various agencies that participate in the field response. The real hub of the group, however, is the Analysis and Synthesis Cell. This cell is comprised of analysts that coordinate intelligence tasking for the other group cells as part of the overall collection plan in order to estimate the scope and impact of the event. The cell will synthesize gathered information and generate a clear product for the Unified Command Structure and others via the OIC Cell. Attachment II details the dissemination paths for the various TEW products.

The remaining three cells support the OIC and Analysis and Synthesis cells. The Consequence Management Assessment Cell includes representatives of the law enforcement side of consequence management, the fire service, HAZMAT specialists, and health practitioners. These specialists bring their respective expertise to bear on the net assessment. The Public Health/Epidemiological Intelligence Cell, like the Consequence Management Cell, includes relevant specialists, in this case coming from the public health sector. In order to generate more informed medical analysis, this cell also makes use of real-time disease surveillance. Finally, the Crisis Management/Investigative Liaison Cell draws on the expertise of criminal intelligence groups, such as the Los Angeles Task Force on Terrorism, the FBI, LAPD Anti-Terrorist Division and the local bomb squads. If needed, this cell can send information directly to the officer in charge.

The last component of the group is the “Intelligence Toolbox,” which includes forensic intelligence support and all other resources that can assist in the assessment. Forensic intelligence offers traditional forensic support as well as CBRN-specific applications such as plume modeling, detection, etc. Among the other “tools” at the county’s disposal are the national laboratories, the Centers for Disease Control, police agencies around the United States and overseas, as well as universities and other research institutions.

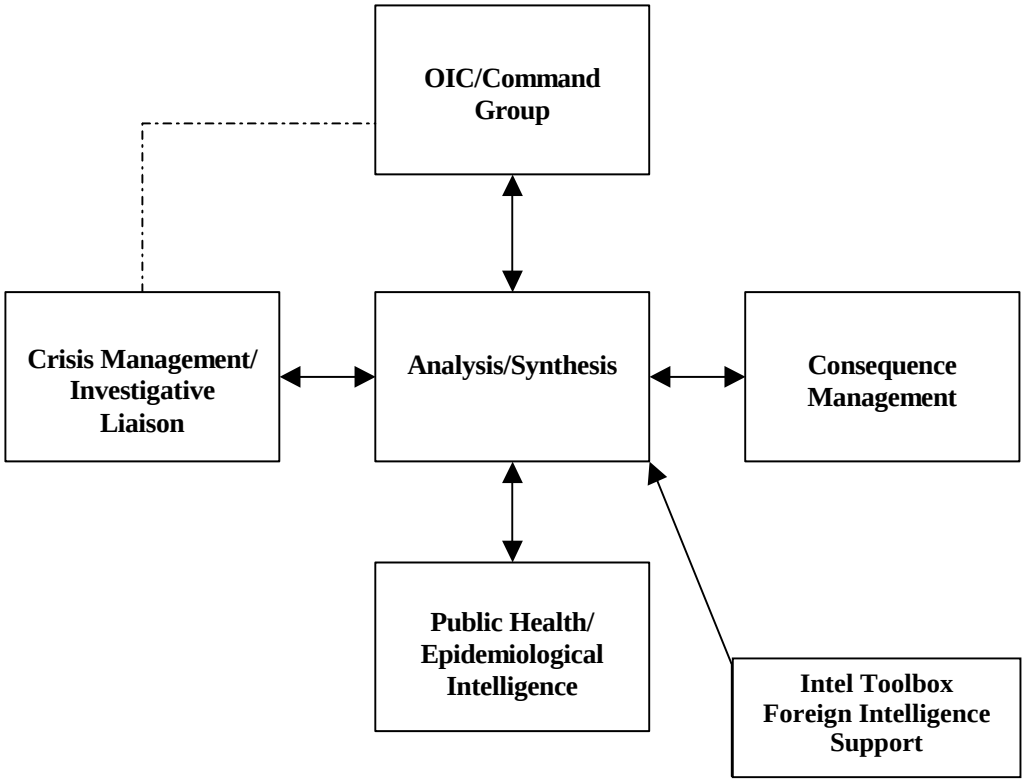


Figure 3. Net Assessment Group Information Flow-Chart. (Courtesy EOB)

LOCAL RESPONDER TRAINING IN LOS ANGELES

In 1997, officials and technical specialists from Los Angeles area local responder agencies began training in CBRN response. In September 1997, approximately 50 representatives of six local agencies attended the National Interagency Civil-Military Institute (NICI) five-day course, "Preparing For and Managing the Consequences of Terrorism." This was followed in November 1997 by participation in a Department of Defense (DoD)-sponsored "train the trainer" course that was funded by the Nunn-Lugar-Domenici Domestic Preparedness Program (NLD). At the same time, and also in the NLD framework, Los Angeles was scheduled to conduct a large-scale CBRN exercise ("Westwind"), for which Los Angeles City and County Fire Departments, in cooperation with the Western National Medical Response Team (NMRT), began training. This latter training included bimonthly mass decontamination exercises involving the respective departments' hazardous materials (HAZMAT) teams. Of particular significance is that this initial training focused almost exclusively on operators, rather than on commanders or policymakers.

Reflecting the state of training and the perceived threat, the LAPD Emergency Operations Section (EOS) and the LASD EOB released operational advisories addressing the CBRN threat starting in the second half of 1998.

Additional training has been motivated by a combination of federal initiatives (e.g., NLD) and preparation for large-scale local events (e.g., the 2000 Democratic National Convention [DNC]). In the months leading up to the DNC, for example, DHS provided decontamination training to personnel at the hospitals closest to the Staples Center, where the DNC was held. This training supplemented a DoD-designed course, which 1,100 hospital personnel from 50 facilities had received starting in 1998.

Six locally produced videos, which collectively run approximately two hours, and an accompanying workbook are employed to introduce local responders to the CBRN threat, specific issues relating to each of the types of CBRN weapons, mass casualty decontamination, scene management and other topics. Viewing of the video series is considered a prerequisite for participation in local CBRN preparedness courses.

Four courses have been modularly developed to address the varying needs of local responders. At the most basic level for all responders is a four-hour responder awareness course. Next is an eight-hour responder operations course. There is a 16-hour medical operations course, the last half of which is aimed at hospital personnel. Finally, LACoFD has developed an eight-hour mass casualty mass decontamination course. There are plans for an additional eight-hour course on force protection for law enforcement personnel.

The goal, through the use of the courses and video suite, is to have all local responders trained by the end of 2001. The initial training that responders receive at their respective academies will ultimately include the CBRN material that today is being given to veteran responders, depending upon the availability of fiscal support.

ANTHRAX HOAXES IN LOS ANGELES

Since December 1998, Los Angeles has witnessed more than four dozen threats of the intentional dissemination of anthrax, all of which have proven to be hoaxes. As such, Los Angeles has the dubious distinction of being the nation's anthrax hoax capital. The upside of this title is that the local responder community rapidly has learned valuable lessons in dealing with this phenomenon and its analogues. Additionally, these lessons were translated quickly from ideas to policies to actions.

As noted above, for over a year prior to the December 1998 local outbreak of anthrax hoaxes, officials and technical specialists from Los Angeles area local responder agencies began training in CBRN response.

Reflecting the state of training, and the perceived threat, the LAPD EOS released an Emergency Preparedness Bulletin, entitled "Terrorism Awareness," in August 1998. The Bulletin, which functions as a supplement to the LAPD *Supervisor's Field Operations Guide*, included LAPD guidelines for response to terrorist attacks, including those

involving CBRN weapons. Anthrax was mentioned as a specific example of a biological agent.

Anthrax hoaxes in the United States started with an incident in Wichita, Kansas on August 18, 1998, four months before the first one in Los Angeles. The media took hold of this event, and through the "copycat syndrome" other hoaxes began to slowly proliferate across the country. The significance of this proliferation of anthrax hoaxes was quickly identified by the Los Angeles TEW, which saw fit to discuss the Wichita incident during its August 27 meeting. Additional anthrax hoaxes were reported during the TEW's October, November and December meetings.[136] By the November TEW meeting, it was felt that "anthrax hoaxes are coming to L.A." As a result of this early assessment, the EOB formulated a preliminary policy advisory, entitled *Responding to Potential Weapons of Mass Destruction (WMD) and Anthrax Threat Incidents*, which was released on December 12, 1998 to all LASD field operations units.

Anthrax Hoaxes Arrive in Los Angeles

Four incidents in the latter half of December 1998 were formative for the Los Angeles local responders' procedures for addressing CBRN weapon threats.

December 17, 1998 – Executive Parking Company

An employee of the company received an anonymous letter, which informed its recipient that she had been exposed to anthrax. LAPD, LAFD, LACoFD Health/HAZMAT Division, DHS and the FBI's Los Angeles field office all responded to the 911 call placed by company employees.

Serendipitously, among the host of responders were at least four who had attended the 1997 "Preparing For and Managing the Consequences of Terrorism" course at NICI. Despite the presence of these qualified personnel, the incident commander, as well as other on-site senior officials, had little or no exposure to or training for CBRN terrorism response. As such, these officials chose to err on the side of caution, and followed the existing paradigm for dealing with hazardous materials. The hazardous materials approach is governed by strict Occupational Safety and Health Administration (OSHA) regulations and procedures regarding unknown substances that forced the responders into their most aggressive possible response. The result was that HAZMAT technicians had to don maximum protective gear and set up decontamination facilities for themselves and the 25 employees who were decontaminated on-site, in the building's parking structure. The victims' decontamination process entailed their being stripped and scrubbed down with a diluted hypochlorite (bleach) solution. Their personal effects (e.g., clothing, wallets, keys, etc.), considered both contaminated and evidence, were confiscated and sealed. These items could not be unsealed and/or released until their safety had been confirmed. These individuals were subsequently transferred to UCLA Medical Center.

[136] Specifically, the following incidents were mentioned: Colorado Springs (October 15, 1998), Jacksonville, FL (November 3, 1998), Miami (November 20, 1998) and multiple incidents in Indiana that occurred throughout November.

Hospital officials, as unfamiliar with anthrax as many of the other senior responders, elected to decontaminate the 25 patients a second time at the hospital. Each patient was discharged with a week's supply of antibiotics and a prescription for more, if need was determined, as well as a health and safety (medical exposure) advisory letter from DHS/UCLA. At the time of their release, an important logistical oversight became apparent in that the by-now tired and traumatized victims were wearing only hospital clothing while their wallets and car keys, along with their street clothes, were still being held as potentially contaminated evidence.

The office in which the envelope was opened and all adjoining offices were ordered closed until lab results confirmed that no anthrax spores were present, a process that took approximately 48 hours. The response to this incident was estimated to cost between $500,000 and $600,000.

December 18, 1998 – U.S. Bankruptcy Court

An anonymous caller to the U.S. Bankruptcy Court advised, "You should check the air conditioning system for possible anthrax." The building was evacuated, and 105 people were identified as possibly having been exposed, and consequently isolated for the eight hours it took to search and sample the building.[137] The same agencies responded as had done so the day before. Consultation with experts at the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) and DHS, combined with the realization that the previous day's decontamination probably had been unnecessary, led to the decision not to similarly decontaminate the victims at the courthouse. Two physicians from DHS wrote prescriptions for antibiotics that accompanied a health and safety (medical exposure) advisory letter given to all 105 victims upon their release. The letter, issued jointly by LAFD, LAPD, LACoFD-Health/HAZMAT and DHS, instructed the individuals to self-decontaminate at home by showering for at least ten minutes. Further instructions were given regarding the decontamination of personal articles. Notably, it was pointed out in the letter that the authorities believed that the incident was likely a hoax.

The targeted courthouse also was ordered closed while samples were analyzed, which again took around 48 hours. The cost for the December 18 response was $600,521.87, the sum being repaid to the LAFD and LAPD by the now-convicted perpetrator.[138]

December 21, 1998 – Van Nuys Superior and Municipal Courthouses

As on the 18th, an anonymous caller to 911 initiated this incident, claiming that "anthrax has been released in the Van Nuys courthouse." While the same agencies responded as

[137] There is an important legal distinction between isolation and quarantine. Only the State Health Officer can order the latter, while the former is essentially a voluntary separation. In none of the incidents under review was a quarantine ordered.

[138] This odd figure, calculated to the penny, is what was ordered repaid by the United States District Court in restitution to the emergency response services. For more information, see http://www.usdoj.gov/usao/cac/pr/147.htm . This sum is being repaid at a rate of $200 per month, meaning that it will be paid in full in just over 250 years.

on the previous two occasions, the response itself was markedly more reserved. In this case, approximately 1,200 people were evacuated from the building and isolated until the building was fully searched and sampled, a process that took around five hours. The entire building was closed for the 48 hours required to process the collected samples. No prescriptions were issued. A health and safety (medical exposure) advisory letter detailing self-decontamination procedures and informing recipients that antibiotics would be issued if need was so determined. Again, it was emphasized that health and law enforcement authorities believed the incident to be a hoax.

December 23, 1998 – Time-Warner Cable

Time-Warner Cable was threatened by yet another anonymous call to 911. Response to this incident was more limited than to any of its predecessors. The approximately 70 evacuees were isolated for about six hours, during the search and sampling phase. Unlike the previous incidents, the building was reopened for normal business operations upon completion of the search and sampling. No prescriptions were issued, but a similar health and safety (medical exposure) advisory letter to that of the 21st was given to company employees.

Other December Incidents

There were a handful of other threat incidents in late December, all of which were met with responses of equal or lesser magnitude than that of the Time-Warner Cable incident.

With at least seven incidents in ten days, it was clear that local authorities were faced with a prohibitively expensive, media-fed, copycat epidemic. Local responders learned valuable lessons from each costly incident, and by the 28th, had "finally had it" with the overwhelmingly large reaction to what had turned out to be a string of hoaxes. The time had come to formalize the policies that heretofore had been conceptual and unwritten.

Revamping Anthrax Threat Response Policy

On December 28, representatives of the six major local responding agencies (LAFD, LACoFD, LAPD, LASD, DHS and the FBI's Los Angeles field office) convened a "big-6 summit" at the LACoFD headquarters. Participants decided that a more practical, measured response was needed, in light of the previous ten days' experience. Participants agreed that continuing with the same response model, costing the community approximately half a million dollars for each deployment, would quickly drain local resources and budgets as well as damage response capability to other, real emergencies. Additionally, the local responders now had gleaned valuable insight from their responses and from the collective wisdom of federal, state and local experts from across the nation, all of which suggested that such large-scale responses to every threat were both impractical and unnecessary.

Experience in Los Angeles and elsewhere led authorities to develop a dynamic yet structured set of indicators by which to assess the credibility of an anthrax threat. As a result, the summit participants decided that major components of prior responses now

would be employed if and only if credible evidence were present that contradicted perhaps less tangible indicators that the event was a hoax. Due to the sensitive nature of the subject, interviewed responders have requested that these indicators not be published as part of this unclassified report.

Within days (and in one case, hours) of the summit meeting, LAPD, LASD, LAFD and LACoFD all released intradepartmental bulletins outlining these newly formulated policies and procedures. These bulletins had department-wide distribution and implementation. It is believed that within a week of its release, the contents of the LAPD bulletin were in the hands of all field personnel.

Two points are especially noteworthy in the context of these newly authored policies. First, the turnaround time from field experience to written policies was remarkably short; the time from the Westwood incident to the summit meeting was just 11 days. Second, these written policies have remained virtually unchanged since their initial compilation almost 18 months ago. That is, not only were conclusions drawn quickly, so far they also appear to have withstood the test of time.

COMMENTS BY THE LOCAL RESPONDERS

In recent interviews conducted for the Gilmore Commission, a number of common themes emerged regarding the state of preparedness and the role the federal government has played in getting there. The most important of these themes are as follows:

- **The Need for Fiscal Sustainment**
  All of those interviewed expressed profound concern about the perceived "one-shot" nature of federal assistance. To be sure, preparedness entails large up-front costs for training and especially for equipment. However, both of these are perishable, and local responders worry that in the long run, without continued federal assistance, their communities might not be able to maintain the desired level of readiness envisioned by policymakers. Some responders wondered aloud whether, without ongoing support, the entire CBRN preparedness enterprise would end up an ephemeral waste of a great deal of resources and effort. This issue was the most emphatically and most often voiced in all meetings with Los Angeles responders.

- **Bearing the Burden of Training Costs**
  The Domestic Preparedness Program has provided "train the trainer" courses for responders throughout the United States. Interviewees were quick to point out that even a four-hour course, when multiplied by the thousands of responders in a large metropolitan area like Los Angeles, adds up to significant manpower costs. For example, every LASD deputy should optimally undergo 14-40 hours of training (as determined by the EOB), which is the equivalent of 1.75-5 workdays. This adds up to between approximately 3.75 and 10.73 million dollars for LASD alone.[139] No federal

[139] This is based on the top-step deputy's overtime pay of $33.52 per hour multiplied by 8,000 deputies multiplied by the 14-40 training hours needed. Most LASD deputies are top-step, and all internal fiscal calculations are based on this rank.

funding is provided for these training days. Responders almost unanimously believe that this training is beneficial and important, yet are worried that – given constrained training budgets – CBRN response training will come at the expense of other, perhaps no less vital, competencies.

- **The Need for Coordinated Procurement**
  Initially, NLD funds were granted to cities, with little or no consideration of the operational structure of the individual recipient metropolitan areas of which cities are but a part. For example, three cities within the Los Angeles operational area received NLD funding (Los Angeles, Glendale, Long Beach).[140] This allocation method was problematic because it led to the inefficient and inequitable distribution of NLD funds. That is, while multiple cities within a metropolitan area might have received more total assistance than was necessary for the area (inefficient), smaller individual cities within the same metropolitan area could be left with nothing (inequitable). This problem has since been resolved insofar as the federal government now allows agencies at other than the city level to apply for assistance. Given the county-as-operational-area structure mandated by California law, this change has been welcomed by responders in Los Angeles. Currently the EOB, through the TWG, coordinates the application for federal assistance and all CBRN-related purchasing for the operational area. All parties interviewed expressed satisfaction with this process. In the future, OEM will coordinate funding applications for all cities in the county.

  A positive side effect of the coordinated funding application process is that the focus of agency lobbying has moved from Washington, D.C. to the local, professional arena. In the past, agencies – often via their unions and other professional associations – have lobbied grant-giving federal institutions in direct competition with their local colleagues. Since in Los Angeles applications are done jointly, any such lobbying takes place at home, among cooperating, rather than competing agencies, and in accordance with the mutual understanding of the operational area's needs.

- **Redundant Training**
  There has been a proliferation of government-sponsored training options for local responders. A number of those who have taken the lead on the subject of CBRN preparation for their respective departments (i.e., those who will serve as agency trainers) commented on the redundant nature of the training being offered. While it is recognized, and indeed hoped, that receiving training from a variety of sources will enrich the response repertoire of local agencies, the individuals interviewed felt that in fact, some of the federal funds spent on their courses was wasted since each additional course added little or no value to their skill-sets. These responder-trainers had hoped that federal coordination and standardization of training would lead to a well defined training progression that would allow them to gain the level of expertise needed for their jurisdictions and job descriptions so that they can competently and effectively instruct others within their departments. This reflects the desire of Los Angeles CBRN response designers to maintain a small cadre of highly-trained

[140] For more information on the overlap of NLD assistance, see GAO, *Combating Terrorism: Opportunities to Improve Domestic Preparedness Program Focus and Efficiency*, GAO/NSIAD-99-3.

professionals whose job it is to 1) function as a skilled group of responders; 2) act as technical specialists within the Incident Command System, providing insights and relevant resources to an incident commander; and 3) train others within the response community to a pre-defined baseline level of capability. This desire, in turn, reflects the perceived threat and its scale within the Los Angeles operational area.

- **Who Has VX, Anyway?**
  Local responders have complained about the overwhelming emphasis in federal training programs on military quality CBRN weapons. For a host of reasons, it is widely thought that the likelihood of a CBRN attack is low, and that the likelihood of such an attack using weapons grade material is even more remote. Thus, the local responders would prefer to train based on realistic scenarios involving agents more likely to be seen in the United States today and in the near future (i.e., common industrial chemicals, etc.). As one TEW participant put it, "Vic from Ventura ain't got VX."

- **OSHA Needs to Step Up**
  It has been recognized in Los Angeles since the first Anthrax hoax incident in December 1998 that the standards set by OSHA, while appropriate for chemical spills and undoubtedly reflecting a desire to err on the side of caution, have no provisions for emerging terrorist threats, and especially those involving biological weapons. Specifically, threat analysis has no part in OSHA regulations. Local responders complained that despite their belief that no anthrax was present in the 1998 incidents, OSHA regulations "forced their hand" into an over the top, costly HAZMAT response. They feel that OSHA needs to be integrated into the policymaking process for addressing new and potentially unforeseen threats.

- **Know Your Counterparts**
  A silver lining to the CBRN threat cloud has been the unprecedented level of cooperation among emergency response agencies in Los Angeles, a fact almost unanimously recognized by interviewees. At the 1998 anthrax hoax incidents, the presence of on-scene experts from multiple agencies, who had routinely met (e.g., at the TEW) and trained (e.g., at various federally-funded courses and in joint exercises) together, enhanced the cooperative working environment that is essential for addressing CBRN threats, real or fake. The ongoing monthly meetings of the TEW reinforce the atmosphere of cooperation.

- **Elements of The Incident Command System Are Particularly Useful**
  As mentioned previously, by California law, all emergency response agencies operate according to the Standardized Emergency Management System (SEMS), which is a state adaptation of the Incident Command System (ICS). ICS is a standard management system for command, control and coordination of emergency responders. Two ICS principles are of particular relevance to the CBRN threat.

First is the concept of *Unified Command*, "a unified team effort which allows all agencies with responsibility for the incident, either geographic or functional, to manage an incident

by establishing a common set of incident objectives or strategies."[141] In the context of the CBRN threat, Unified Command promises to catalyze an effective, coordinated, on-scene decision-making process.

Second, as mentioned above, ICS calls for the employment of *technical specialists* wherever their special skills may be of use within an incident. In the case of the December 17, 1998 anthrax hoax incident, while there were numerous technical specialists present, their expertise was largely unknown and unappreciated by higher level decision makers within the incident command structure. In this light, and under the stressful circumstances of this first anthrax threat, the incident commander and the unified command chose to err on the side of safety, and thus decided to decontaminate the office workers. The Los Angeles area response plan now calls for maintaining a small cadre of highly trained local specialists to complement the much larger number of baseline-trained responders. ICS will allow the efficient use of expertise quickly and where most needed.

Noting that "all terrorism is local," local responders mentioned that given the anticipated degree of federal and local cooperation that a CBRN attack will entail, it is imperative for federal response agencies to become proficient in the use of ICS and familiar with their roles in it. Doing so will allow these federal resources to quickly and effectively "plug into" the local ICS structure.

- **Train the Commanders**

Like lower-level functionaries, commanders also need to have a certain (perhaps different) baseline level of CBRN training. Commanders stand to benefit in two ways from even basic training regarding CBRN weapons. First, they themselves will have a greater understanding of the nature of the CBRN threat, and thus be able to make more informed operational decisions, making better use of provided intelligence. Second, they will be more aware of technical expertise within their own and other responding agencies, and be more likely to bring it to bear on their decisions.

POLICY RECOMMENDATIONS FOR THE FEDERAL GOVERNMENT

Based on the interviews conducted for the Gilmore Commission, a number of policy recommendations for the federal government made themselves apparent.

- **Threat Analysis Needs a Cooperative Vehicle**

As has been noted elsewhere,[142] threat analysis is critical in the determination of appropriate response. Because of the complexity of terrorism threats in general, and the CBRN threat in particular, threat analysis is most effectively conducted by multiple agencies, each of which brings its own special skills and strengths to the table. In Los Angeles County, the TEW has filled the previously wanting role of a medium for

[141] Federal Emergency Management Agency, Emergency Management Institute, *Basic Incident Command System (ICS) Independent Study* IS-195, January 1998, p.A-12.
[142] See, for example, GAO, *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*, GAO/NSIAD-98-74.

information transfer, joint analysis and incident net assessment and thus has proven to be an exceptionally useful mechanism.

While Los Angeles County is unique in its size, the practice of bringing local, state and federal stakeholders together on a regular basis to provide threat analysis would be valuable in other jurisdictions around the United States, regardless of their size. Other California counties have established their own TEWs, and still others are in various stages of development. Cities across the country have turned to LASD for assistance in creating their own TEWs. The TEW is sufficiently flexible that it can be easily tailored to address the specific needs and concerns of America's variegated communities. For example, in Los Angeles the Emerging Threat Cell has focused on RFWs, but in other locales this cell's analog could concentrate on border concerns, infrastructure protection (e.g., ports, nuclear facilities, etc.) and other location-specific topics.

The federal government could assess the effectiveness of the TEW in Los Angeles and elsewhere and then, assuming the results are positive, facilitate its replication. The Federal Emergency Management Agency (FEMA) currently offers courses on the establishment and operation of emergency operations centers (EOCs). Incorporating the TEW into the EOC curriculum, for example, would provide a smooth, standardized means for teaching TEW operation to a broad national audience of emergency managers.

- **One Size Does Not Fit All**

While large American cities have a lot in common, no two are exactly alike. Aside from geography, demographics, climate, etc., cities vary greatly in terms of the structure of their emergency management systems and their jurisdictional and emergency response structures as well. The federal policies that provide funding, equipment recommendations and training to local responders need to be more flexible vis-à-vis inter-city variation. The federal government has improved in this regard, as when it allowed Los Angeles County to apply for assistance, in addition to the City of Los Angeles. The nation's diverse communities will welcome additional federal flexibility in the structural criteria for assistance application.

- **The Need for Ongoing Bottom-Up and Lateral Information Sharing**

While Los Angeles authorities have learned from field experience, exercises and their responses to the anthrax hoaxes, this learning occasionally has come at tremendous expense in terms of local resources and tax dollars. All localities that are in the process of building their response capabilities face a similar set of challenges – equipment procurement, protocol and policy development, training, the need to stay on top of current technical and other developments, etc. There is currently no formal mechanism for officials in these localities to share lessons learned or gain practical advice from their counterparts around the country or around the world. This gap often forces responders to start from scratch when confronted with situations that have already been successfully (or even unsuccessfully) negotiated by others. In this regard, even after Los Angeles had established and implemented its new set of anthrax threat response policies, other jurisdictions across the United States, when faced with similar threats, reinvented the wheel, again at great cost in terms of dollars and unnecessary stress. Likewise, Los

Angeles could have learned from those communities that experienced anthrax hoaxes prior to December 1998. In the future, this problem could be avoided if the federal government facilitated the creation of a bottom-up and horizontal communication system, which would allow local agencies to share lessons learned with each other, and with the federally sponsored training programs that will further educate responders from across the country.

The federal government should provide this communication system for two main reasons. First, the CBRN threat transcends state boundaries and the federal government is legally responsible for such issues of national security. Second, because the federal government has taken it upon itself to act as the national training authority for this subject, it follows that it should facilitate the transfer of information from the field to its own trainers as well as to other field locations.

ACKNOWLEDGEMENTS

The authors are grateful to the representatives of the following agencies for their generous assistance, without which this study would not have been possible:

Federal Bureau of Investigation, Los Angeles Field Office
Los Angeles City Fire Department
Los Angeles County Department of Health Services
Los Angeles County Fire Department
Los Angeles County Sheriff's Department
Los Angeles Police Department

The authors would like to give special thanks to the participants in the Los Angeles County Terrorism Early Warning Group, and particularly Sheriff's Sergeant John Sullivan who was extraordinarily generous with his time and expertise.

Any errors or omissions are the responsibility of the authors.

ATTACHMENT I. GLOSSARY

ATD	Los Angeles Police Department Anti-Terrorist Division
CBRN	Chemical, biological, radiological and/or nuclear
CEOC	County Emergency Operations Center
DHS	Los Angeles County Department of Health Services
DNC	Democratic National Convention
DoD	U.S. Department of Defense
DOJ	U.S. Department of Justice
EMS	Emergency Medical Service
EOB	Los Angeles County Sheriff's Department Emergency Operations Bureau
EOC	Emergency Operations Center
EOS	Los Angeles Police Department Emergency Operations Sectio
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GAO	United States General Accounting Office
HAZMAT	Hazardous materials
IAB	Inter-Agency Board
ICS	Incident Command System
IW	Information Warfare
LACoFD	Los Angeles County Fire Department
LAFD	Los Angeles City Fire Department
LAPD	Los Angeles Police Department
LASD	Los Angeles County Sheriff's Department
LAWA	Los Angeles World Airports
LAX	Los Angeles International Airport
MMRS	Metropolitan Medical Response System
NDPO	National Domestic Preparedness Office
NICI	National Interagency Civil-Military Institute
NLD	Nunn-Lugar-Domenici Domestic Preparedness Program
NMRT	National Medical Response Team
OEM	Los Angeles County Office of Emergency Management
OIC	Officer in Charge
OSHA	Occupational Safety and Health Administration
OSINT	Open source intelligence
PPE	Personal protective equipment
RFW	Radio Frequency Weapons
SEMS	Standardized Emergency Management System
SIS	Los Angeles County Sheriff's Special Investigations Section
TEW	Los Angeles County Terrorism Early Warning Group
TWG	Los Angeles County Terrorism Working Group
UCS	Unified Command Structure
USAMRIID	United States Army Medical Research Institute of Infectious Diseases

ATTACHMENT II. TEW PRODUCT DISSEMINATION[143]

<table>
<tr><th></th><th>Law</th><th>Fire</th><th>EMS</th><th>Hospital</th><th>Impacted</th><th>Elected</th></tr>
<tr><td>Advisory</td><td colspan="6">All</td></tr>
<tr><td>Alert</td><td>Group 1</td><td>Group 2</td><td colspan="2">Group 3</td><td rowspan="2">Group 4</td><td rowspan="3">Group 5</td></tr>
<tr><td>Warning</td><td>Group 1 plus Watch Commander and Area Command Teams</td><td>Group 2 plus Station Captains</td><td rowspan="2">Group 3</td><td>Group 3 plus trauma centers</td></tr>
<tr><td>Net Assessment</td><td>Group 1 plus incident commander, others as needed</td><td>Group 2 plus incident commander, others as needed</td><td>Group 3 plus others receiving casualties</td><td>Group 4 plus management as needed</td></tr>
<tr><td>Issue Specific White Papers</td><td colspan="5">Command level officers, other affected units</td><td>Group 5, particularly as regarding law/funding impacts</td></tr>
</table>

Group 1: All Command Officers (above Station Commanders), Unit Commanders, specialized units (Special Weapons Teams, Bomb Squads, Emergency Operations/tactical planning, MMRS members)

Group 2: All Chief Officers, HAZMAT teams, urban search and rescue teams, Counter-Terrorism Coordinators, MMRS members

Group 3: DHS EMS Section, Medical Alert Center, Epidemiological Surveillance Section, National Disaster Medical System Coordinator

Group 4: Directors, OIC's, Security Chief(s) of impacted entities

Group 5: As needed, based upon circumstances of situation and jurisdiction

[143] Courtesy of EOB.

APPENDIX H—CDC NEDSS and EPI-X

Supporting Public Health Surveillance through the National Electronic Disease Surveillance System (NEDSS)[144]

Methods for conducting public health surveillance may often differ considerably by program and disease. Regardless of these differences, however, all surveillance activities share many common practices in the way data are collected, managed, transmitted, analyzed, accessed and disseminated. The National Electronic Disease Surveillance System (NEDSS) will, primarily through the creation of standards, facilitate the handling of data through each of these steps. As described below, different interrelated activities supporting NEDSS will offer significant improvements in the way public health surveillance is conducted at the Federal, State, and local level. The long-term vision for NEDSS is that of complementary electronic information systems that automatically gather health data from a variety of sources on a real-time basis; facilitate the monitoring of the health of communities; assist in the ongoing analysis of trends and detection of emerging public health problems; and provide information for setting public health policy.

Data Collection

Cases of a disease or other condition of interest are primarily identified in the medical care system. Once identified, these cases are typically reported to a local health department, often using paper-based data collection forms. At the local health department, forms may be entered into a computerized electronic data management system and transmitted to the State, or they may be copied, filed at the local level and then sent directly to the State where they are manually entered into the State health department's electronic system. These reporting processes are generally the same, regardless of the disease or condition that is being reported. There are a number of problems that can arise during the reporting process. These problems, in turn, often place a large burden on medical care staff who have responsibility for disease reporting. For example, cases may be reported from a variety of sources from within the health care setting, such as clinical laboratories and private physicians. Physicians and laboratory supervisors and their office staff are already overworked. Nevertheless, it is often left up to health care providers to determine if a case meets public health surveillance case definitions and to figure out how to fill out the wide variety of forms produced by CDC and health departments. They may also spend significant time tracking down patient records in response to requests for more information from the health department. NEDSS will facilitate the collection of case report forms from providers in two important ways. First, standards are being developed to assure uniform data collection practices across the nation. The public health data model and the CIPHER (Common Information for Public

[144] Http://www.cdc.gov/nchs/otheract/phdsc/presenters/nedss.pdf. NEDSS is a program of the Health Information and Surveillance System Board, in the Agency for Toxic Substances and Disease Registry, Centers for Disease Control and Prevention. For more information, see http://www.cdc.gov/od/hissb/index.htm

Health Electronic Reporting) guidelines will recommend, for example, a minimum set of demographic data that should be collected as part of the routine surveillance. In addition, the CIPHER guidelines will provide a consistent method for coding data on the data collection forms. It is expected that standardizing data collection forms should ease the burden on physicians and their staff by providing forms that are similar in appearance and that do not require that someone figure out for each specific form where information is located and how it should be coded.

Second, NEDSS will include recommended standards that can be used for the electronic reporting of surveillance data. Specifically, NEDSS will recommend a standard data architecture and electronic data interchange format to allow computer systems to generate automatically electronic case reports that can be sent to local or State health departments. These types of standards would both ease the burden on large organizations that already have computerized data systems (such as regional laboratories, hospitals, managed care organizations) and would ensure that all cases that are in the provider's data systems are being reported to public health.

Data management issues: a) multiple case reports

To whom cases should be and are reported is often unclear. For example, a physician reporting a case would likely send the form to the county health department. A State or regional laboratory may also report the same case to the State health department. Given the number of potential sources of information regarding a single patient, the possibility exists that persons may be entered into the system more than once or may have discrepant data reported about them on the multiple reports. In addition, undoing these duplicate records after the reports have been received at the health department (often weeks or months later) is more cumbersome than detecting those duplicate records and consolidating them prior to entry into the system database. For example, the original paper records needed to resolve discrepant data may not be easily retrievable or may be lost. To address this problem, NEDSS will identify standard software components/tools that may be used at the local and State health department levels to detect duplicate reports based on a person's demographic data (e.g., name, address, date of birth, sex). This process is known as registry matching (also referred to as "record matching"). As paper forms are entered into the electronic system, the database of prior records would be scanned and potential duplicates identified. Next, data entry operators could decide whether to enter the particular case as a new report or to update the record already present. The need for an automated system of registry matching is even more important as we move toward increasing reliance on automated electronic case reporting. While paper forms are generally handled one at time for entry and processing, electronic records are usually received in bulk and are processed together. The record matching software must be able to reliably determine which records are new and which should update existing reports. In addition, the software must also be capable of detecting instances of discrepant data, and, as deemed appropriate by the programs, it must be able to resolve those discrepancies. Finally, the tool must provide a mechanism for saving enough information on the individual reports in electronic archives if necessary, so that if at a

later date two records were found to be merged inappropriately, the original records can be restored.

Data Management Issues: b) Data Entry at the Health Departments

The multiple data entry systems that CDC has created for local and State health department use have led to many complaints. Chief among these is that that data for an individual person must be entered into multiple, disparate systems. Given recent advances in technology, this is an unnecessary and burdensome step. A second common complaint is that each of the CDC-provided systems works differently, so that using more than one of them is onerous and time-consuming. An analogous situation that most office workers could relate to would be having to use three different word processors in an average day. Image if you had to be trained on and familiar with all the subtleties of Microsoft Word, Corel WordPerfect and Lotus WordPro! These problems created by different surveillance systems are being addressed through the definition of standards for system development activities. As previously mentioned, creation of data architecture standards will ensure, just as it did for the data collection forms, that information is entered and stored in a consistent and uniform way. Having data stored in a uniform way also means that they can more easily be transferred from one system to another so that duplicate data entry is reduced. Another relevant set of standards has to do with the user interface of CDC-developed surveillance systems. A person trained on any one system, for example, should be able to move to another without changing the way they interact with the software. A set of standards for a common user interface will guarantee that all systems look and work similarly. It is expected that the same set of user interface standards will be applied both to Windows-based applications and to Internet-browser based data collection systems. This type of integration through interface of the web and the stand-alone PC is the same approach that Microsoft is taking with its operating systems and application interfaces.

Data Transmission from Local to State Health Department and to CDC

Once surveillance data are entered into computerized data management systems, they are not only analyzed within the organization to which they were reported, but are also transmitted for analysis at other levels. Simply speaking, electronic reporting may occur as data are sent from the health care setting to local (city or county) health departments, then on to State health departments, and finally to CDC. With the current myriad of systems in place, there are many different methods for reporting data. For example, diskettes may be mailed, dial-up modems may be used to connect over public telephone lines, leased telephone lines may provide wide area network used for reporting, or the public Internet may be used. Currently, just for reporting to CDC, all of these methods are in place. There are also different levels of security in terms of electronic encryption methods that are applied. For example, in a recent inventory, over 73 different surveillance systems developed at CDC sent or received surveillance data electronically. Only 19, however, reported encrypting the data for transmission. While virtually all programs do not consider the encryption of their data an issue because individual person or site identifiers are removed before reporting to the next level, there is at least a small

risk that a person could be indirectly identified based on data in these individual records. There are two coordinated efforts that are addressing this problem. The first is the creation of the "Health Alert Network (HAN)" that will use the Internet as a backbone for communicating surveillance data (as well as a host of other information such as surveillance reports, training materials, policy documents, etc.) between health departments and CDC. This system is expected one day to connect the myriad of local health departments with State and territorial health departments and federal agencies, including CDC, nationwide. The second part is the Secure Data Network (SDN – sometimes called the "secure Internet pipeline"). This pipeline will provide CDC program areas with a secure method for encrypting and transferring files from a health department to a CDC program application across the Internet. (As an Internet-based system, the SDN may be considered to be part of HAN, not independent of it.) It will also allow CDC to eliminate the multiple methods of receiving data. In addition, using digital certificates and the MD5 message digest, the SDN will provide a consistent, transparent method for authenticating the source and ensuring the integrity of those data. This network will raise the standard on security for most of the surveillance activities now supported by CDC. Eventually the combination of the HAN and the standards that are used for the Secure Data Network can be extended to support standardized security beyond just reporting to CDC. They will allow any two or more partners in public health, whether they are heath care providers, clinical labs or local and State health departments, to exchange information without risk of eavesdropping by unauthorized parties.

Data Analysis

Individual program areas at CDC and State and local health departments have, over the years, developed many innovative methods for the analysis of data. For example, recent efforts have led to development of techniques that accurately detect some changing or unusual patterns of trends or outbreaks of diseases. In addition, statistical methods have been developed to account for the delays in reporting of data from providers to health departments to CDC and, where appropriate, to estimate the true incidence of a disease or condition even when not all cases have been reported.

The tools for implementing these methods have been provided to local and State health departments as part of individual surveillance systems, but in general they are not widely available. The closest thing that CDC has to the universal distribution of analysis tools are those contained in the DOS-based EpiInfo software package, however the DOS version of the application does not include some of the more sophisticated techniques described above.

The issue of how to provide standardized data analysis tools will be addressed by NEDSS through the identification, adoption and promotion of statistical component standards. Software written to these standards will be able to be used and incorporated into a variety of surveillance systems – not only those developed by the CDC but also those that are being used by local and State health departments. As an example of the application of components, state-of-the-art analytic software would be able to be dropped into other software applications in the same way that spreadsheets, presentation graphics and e-mail components are now a standard part of many systems.

Data Analysis: Linkage

Another common problem is the need to link data collected in different surveillance and information systems. For example, persons responsible for notifiable diseases are interested both in the cases reported by providers and also, whether those cases might be linked to those reported in a laboratory-based system, where there is available species or serotype information that indicates that these cases may be part of an outbreak. Or, persons investigating an increase in the number of cases of a vaccine-preventable disease would be interested in determining whether persons with these illness received a certain type or lot of vaccine, information increasingly available, but in a separate location such as an immunization registry. And persons responsible for maternal and child health programs at the State level have noted that how they define and count cases of infectious disease among children does not match the *Case Definitions for Infectious Conditions under Public Health Surveillance* developed by CDC and the Council of State and Territorial Epidemiologists (CSTE) for notifiable disease surveillance. This issue is also being addressed by the surveillance data standards. The data standards will promote the linkage of data, as appropriate to public health needs, either at the individual patient or record level, or more broadly by place and time. Having standardized definitions for data elements will help ensure the correct interpretation of data elements. Having data stored using the same sets of codes will mean that epidemiologists and others needing merged data sets will not need to spend as much time understanding the peculiarities of any one system. Finally, these standards, by ensuring consistent definitions of data and coding of variables, will also facilitate the development of State data warehouses and the virtual State data centers envisioned by the National Association for Public Health Statistics and Information Systems (NAPHSIS).

Data Access and Dissemination

The ability to access and disseminate appropriate public health data and information in a timely fashion to targeted audiences is key to making an impact on the population's health. Often, however, there are significant delays in providing access. For example, program areas at CDC often complain that they spend much of their time generating data sets and responses to requests for information by State health departments, other Federal and State agencies, non-profit organizations, the news media, the public, etc. In addition, providing this information typically requires that staff redirect their activities away from other responsibilities. States also point to the same level of resources required to respond to the myriad of organizations within their own area that frequently request public health data and information.

While providing easy access to appropriate public health data and information has been difficult in the past, program areas have also struggled with how to disseminate and/or present data and information results to interested parties. For example, one program area may use the 1990 population census as the denominator for generating rates, while another program area in the same State uses the projected 1998 rates. In addition, program areas may present rates by age in five-year intervals for one disease while

disseminating results for another disease using different age ranges, leading to an inability to compare the data (when indicated). Finally, no central location at CDC or in many State health departments exists where people can go to locate these data. This lack of a standardized approach to disseminating data and information at CDC, and often in State and local health departments as well, impedes the ability of public health professionals to have a direct impact on public health policy and decision-making.

To address these challenges, NEDSS will include the development of best-practice specifications for a method to analyze and disseminate data and information, primarily using data warehouses. Through collaboration with people within CDC and State health departments currently developing data warehouses, a method will be developed to solicit specification requirements from potential users, to review available COTS (commercial off-the-shelf) products based on these functionalities, and to provide logical justification for choices, with empirical justification when available and appropriate. Through this process, a form of a standard off-the- shelf or internally developed software application will be identified to provide data access capacity to a variety of users with various needs.

Conclusion

As this document illustrates, CDC staff working on NEDSS are focusing on the development, testing, and implementation of standards. These standards will serve as the framework that will support more complete and comprehensive integration of systems in the future. The standards focus on five important areas: data architecture (data model and data standards), user interface, information systems software architecture , tools for interpretation, analysis, and dissemination of data, and secure data transfer. While the various systems developed by CDC and State and local health departments will remain distinct from one another, the use of standards will assure that surveillance data may be easily shared, that users familiar with one system can easily use another, and that software can be easily shared across programs. In addition this approach will ensure that State-of-the-art statistical methods are readily available to epidemiologists, and that a single secure method is in place for reporting data to CDC.
These standards are just the first step to achieving the desired level of integration among CDC-developed, as well as State- and locally-developed, surveillance systems. However, they will provide an important degree of integration for the collection, management, transmission, analysis, and dissemination of data that does not currently exist. It is expected that this integration will better support public health professionals in their efforts to improve the health of the populations they serve.

Epidemic Information Exchange (*EPI-X*): A Rapid Communication System to Notify Public Health Officials of Emerging Health Events

Background

With the capacity for local outbreaks to develop into pandemics in a matter of days, the emergence of previously unidentified diseases, the potential for contaminated food or products to be widely disseminated, and the increased threat of bio-terrorism, the need for rapid communication, research and response has become an essential element of the public health profession. To keep pace with these emerging challenges, the CDC recently launched *Epi-X, the Epidemic Information Exchange*. *Epi-X* is a secure, Web-based communications network for public health officials that will both simplify and expedite the exchange of routine and emergency public health information between CDC and state health departments. This information will prompt investigative and prevention efforts, and help bioterrorism preparedness efforts by helping officials share preliminary information about outbreaks and other health events across jurisdictions, and gain every day experience in the use of a secure communication system. Examples of postings include disease outbreaks, newly recognized environmental, product and occupational or recreational hazards, vaccine recalls, bioterrorism threats, and disaster *response.* *EPI-X* is guided by an editorial board, and has been endorsed by the Council of State and Territorial Epidemiologists. *Epi-X* became operational in November 2000.

System Description: Developed using a user centered design process, the construction of *Epi-X* was facilitated by the input of over one hundred health officials and scientists. *Epi-X* enables state and local epidemiologists, laboratory technicians, and other members of the public health community to:

- Instantly notify colleagues and experts of urgent public health events;
- Receive a daily email of information in their area of interest
- Create reports and track information;
- Research outbreaks and unusual health events through an easily searchable database;
- Rapidly communicate with colleagues through e-mail, Web and telecommunications capabilities;
- Quickly find people and information;
- Customize their home page, information and options based upon specific needs; and
- Request assistance from CDC online.

Future needs: Epi-X is an initial effort to build secure public health communications capacity at the national level and as such will have to grow to fully link officials across

jurisdictions and disciplines into a responsive public health work force. Future needs identified in discussions with health officials include technical changes to provide secure communications for multi-state outbreak response teams, links to disease surveillance systems to merge disease reporting with health alerting, and improved software to automate the recognition of similar disease outbreaks across jurisdictions.

Project Contacts

Carol Pertowski, M.D., Medical Director, *Epi-X*
John W. Ward, M.D., Editor, *MMWR*, Director OSHC, EPO (404) 639-3636

APPENDIX I—NEW ENGLAND AND EASTERN CANADIAN MUTUAL ASSISTANCE COMPACT

INTERNATIONAL EMERGENCY MANAGEMENT ASSISTANCE MEMORANDUM OF UNDERSTANDING

This document follows from Resolution 23-5 resolved at the 23rd Annual Conference of New England Governors and Eastern Canadian Premiers and is compliant with Article II (j) of the Agreement between the Government of the United States and the Government of Canada on Cooperation in Comprehensive Emergency Planning and Management renewed on December 2, 1998.

Purpose and Authorities - Article I

The International Emergency Management Assistance Memorandum of Understanding, hereinafter referred to as the "compact," is made and entered into by and among such of the jurisdictions as shall enact or adopt this compact, hereinafter referred to as "party jurisdictions." For the purposes of this agreement, the term "jurisdictions" may include any or all of the States of Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, and Connecticut and the Provinces of Québec, New Brunswick, Prince Edward Island, Nova Scotia and Newfoundland, and such other states and provinces as may hereafter become a party to this compact.

The purpose of this compact is to provide for the possibility of mutual assistance among the jurisdictions entering into this compact in managing any emergency or disaster when the affected jurisdiction or jurisdictions ask for assistance, whether arising from natural disaster, technological hazard, man-made disaster or civil emergency aspects of resources shortages.

This compact also provides for the process of planning mechanisms among the agencies responsible and for mutual cooperation, including, if need be, emergency-related exercises, testing, or other training activities using equipment and personnel simulating performance of any aspect of the giving and receiving of aid by party jurisdictions or subdivisions of party jurisdictions during emergencies, with such actions occurring outside actual declared emergency periods. Mutual assistance in this compact may include the use of emergency forces by mutual agreement among party jurisdictions.

General Implementation - Article II

Each party jurisdiction entering into this compact recognizes that many emergencies may exceed the capabilities of a party jurisdiction and that intergovernmental cooperation is essential in such circumstances. Each jurisdiction further recognizes that there will be emergencies that may require immediate access and present procedures to apply outside resources to make a prompt and effective response to such an emergency because few, if any, individual jurisdictions have all the resources they need in all types of emergencies or the capability of delivering resources to areas where emergencies exist.

The prompt, full and effective utilization of resources of the participating jurisdictions, including any resources on hand or available from any other source that are essential to the safety, care and welfare of the people in the event of any emergency or disaster, shall be the underlying principle on which all articles of this compact are understood.

On behalf of the party jurisdictions participating in the compact, the legally designated official who is assigned responsibility for emergency management is responsible for formulation of the appropriate inter-jurisdictional mutual aid plans and procedures necessary to implement this compact, and for recommendations to the jurisdiction concerned with respect to the amendment of any statutes, regulations or ordinances required for that purpose.

Party Jurisdiction Responsibilities - Article III

1. Formulate plans and programs. It is the responsibility of each party jurisdiction to formulate procedural plans and programs for inter-jurisdictional cooperation in the performance of the responsibilities listed in this section. In formulating and implementing such plans and programs the party jurisdictions, to the extent practical, shall:

   A. Review individual jurisdiction hazards analyses that are available and, to the extent reasonably possible, determine all those potential emergencies the party jurisdictions might jointly suffer, whether due to natural disaster, technological hazard, man-made disaster or emergency aspects of resource shortages;
   B. Initiate a process to review party jurisdictions' individual emergency plans and develop a plan that will determine the mechanism for the inter-jurisdictional cooperation;
   C. Develop inter-jurisdictional procedures to fill any identified gaps and to resolve any identified inconsistencies or overlaps in existing or developed plans;
   D. Assist in warning communities adjacent to or crossing jurisdictional boundaries;
   E. Protect and ensure delivery of services, medicines, water, food, energy and fuel, search and rescue and critical lifeline equipment, services and resources, both human and material to the extent authorized by law;
   F. Inventory and agree upon procedures for the inter-jurisdictional loan and delivery of human and material resources, together with procedures for reimbursement or forgiveness; and
   G. Provide, to the extent authorized by law, for temporary suspension of any statutes or ordinances, over which the province or state has jurisdiction, that impede the implementation of the responsibilities described in this subsection.

2. Request assistance. The authorized representative of a party jurisdiction may request assistance of another party jurisdiction by contacting the authorized representative of that jurisdiction. These provisions only apply to requests for assistance made by and to authorized representatives. Requests may be verbal or in writing. If verbal, the request must be confirmed in writing within 15 days of the verbal request. Requests must provide the following information:

   A. A description of the emergency service function for which assistance is needed and of the mission or missions, including but not limited to fire services, emergency medical, transportation, communications, public works and engineering, building inspection, planning and information assistance, mass care, resource support, health and medical services and search and rescue;
   B. The amount and type of personnel, equipment, materials and supplies needed and a reasonable estimate of the length of time they will be needed; and

C. The specific place and time for staging of the assisting party's response and a point of contact at the location.

3. Consultation among party jurisdiction officials. There shall be frequent consultation among the party jurisdiction officials who have assigned emergency management responsibilities, such officials collectively known hereinafter as the International Emergency Management Group, and other appropriate representatives of the party jurisdictions with free exchange of information, plans and resource records relating to emergency capabilities to the extent authorized by law.

Limitation - Article IV

Any party jurisdiction requested to render mutual aid or conduct exercises and training for mutual aid shall undertake to respond as soon as possible, except that it is understood that the jurisdiction rendering aid may withhold or recall resources to the extent necessary to provide reasonable protection for that jurisdiction. Each party jurisdiction shall afford to the personnel of the emergency forces of any party jurisdiction, while operating within its jurisdictional limits under the terms and conditions of this compact and under the operational control of an officer of the requesting party, the same powers, duties, rights, privileges and immunities as are afforded similar or like forces of the jurisdiction in which they are performing emergency services. Emergency forces continue under the command and control of their regular leaders, but the organizational units come under the operational control of the emergency services authorities of the jurisdiction receiving assistance. These conditions may be activated, as needed, by the jurisdiction that is to receive assistance or upon commencement of exercises or training for mutual aid and continue as long as the exercises or training for mutual aid are in progress, the emergency or disaster remains in effect or loaned resources remain in the receiving jurisdiction or jurisdictions, whichever is longer. The receiving jurisdiction is responsible for informing the assisting jurisdictions of the specific moment when services will no longer be required.

Licenses and Permits - Article V

Whenever a person holds a license, certificate or other permit issued by any jurisdiction party to the compact evidencing the meeting of qualifications for professional, mechanical or other skills, and when such assistance is requested by the receiving party jurisdiction, such person is deemed to be licensed, certified or permitted by the jurisdiction requesting assistance to render aid involving such skill to meet an emergency or disaster, subject to such limitations and conditions as the requesting jurisdiction prescribes by executive order or otherwise.

Liability - Article VI

Any person or entity of a party jurisdiction rendering aid in another jurisdiction pursuant to this compact are considered agents of the requesting jurisdiction for tort liability and immunity purposes. Any person or entity rendering aid in another jurisdiction pursuant to this compact are not liable on account of any act or omission in good faith on the part of such forces while so engaged or on account of the maintenance or use of any equipment or supplies in connection therewith. Good faith in this article does not include willful misconduct, gross negligence or recklessness.

Supplementary Agreements - Article VII

Because it is probable that the pattern and detail of the machinery for mutual aid among two or more jurisdictions may differ from that among the jurisdictions that are party to this compact, this compact contains elements of a broad base common to all jurisdictions, and nothing in this compact precludes any jurisdiction from entering into supplementary agreements with another jurisdiction or affects any other agreements already in force among jurisdictions. Supplementary agreements may include, but are not limited to, provisions for evacuation and reception of injured and other persons and the exchange of medical, fire, public utility, reconnaissance, welfare, transportation and communications personnel, equipment and supplies.

Workers' Compensation and Death Benefits - Article VIII

Each party jurisdiction shall provide, in accordance with its own laws, for the payment of workers' compensation and death benefits to injured members of the emergency forces of that jurisdiction and to representatives of deceased members of those forces if the members sustain injuries or are killed while rendering aid pursuant to this compact, in the same manner and on the same terms as if the injury or death were sustained within their own jurisdiction. Reimbursement - Article IX

Any party jurisdiction rendering aid in another jurisdiction pursuant to this compact shall, if requested, be reimbursed by the party jurisdiction receiving such aid for any loss or damage to or expense incurred in the operation of any equipment and the provision of any service in answering a request for aid and for the costs incurred in connection with those requests. An aiding party jurisdiction may assume in whole or in part any such loss, damage, expense or other cost or may loan such equipment or donate such services to the receiving party jurisdiction without charge or cost. Any two or more party jurisdictions may enter into supplementary agreements establishing a different allocation of costs among those jurisdictions. Expenses under article VIII are not reimbursable under this section.

Evacuation - Article X

Each party jurisdiction shall initiate a process to prepare and maintain plans to facilitate the movement of and reception of evacuees into its territory or across its territory, according to its capabilities and powers. The party jurisdiction from which the evacuees came shall assume the ultimate responsibility for the support of the evacuees, and after the termination of the emergency or disaster, for the repatriation of such evacuees.

Implementation - Article XI

1. This compact is effective upon its execution or adoption by any two jurisdictions, and is effective as to any other jurisdiction upon its execution or adoption thereby: subject to approval or authorization by the U.S. Congress, if required, and subject to enactment of provincial or state legislation that may be required for the effectiveness of the Memorandum of Understanding.
2. Any party jurisdiction may withdraw from this compact, but the withdrawal does not take effect until 30 days after the governor or premier of the withdrawing jurisdiction has given notice in writing of such withdrawal to the governors or premiers of all other party jurisdictions. The action does not relieve the withdrawing jurisdiction from obligations assumed under this compact prior to the effective date of withdrawal.

3. Duly authenticated copies of this compact in the French and English languages and of such supplementary agreements as may be entered into shall, at the time of their approval, be deposited with each of the party jurisdictions.

Severability - Article XII

This compact is construed to effectuate the purposes stated in Article I. If any provision of this compact is declared unconstitutional or the applicability of the compact to any person or circumstances is held invalid, the validity of the remainder of this compact and the applicability of the compact to other persons and circumstances are not affected.

Inconsistency of Language - Article XIII

The validity of the arrangements and agreements consented to in this compact shall not be affected by any insubstantial difference in form or language as may be adopted by the various states and provinces.

Amendment - Article XIV

This compact may be amended by agreement of the party jurisdictions.

Signed this 18th day of July, 2000 at Halifax, Nova Scotia, Canada.

APPENDIX J– STATES' RECOMMENDATIONS

States' Regional Terrorism Policy Forums
"Protecting States' Critical Infrastructures"

SPONSORED BY THE NATIONAL GOVERNORS' ASSOCIATION
CENTER FOR BEST PRACTICES AND
THE NATIONAL EMERGENCY MANAGEMENT ASSOCIATION

In February 1999, the National Governors' Association (NGA) Center for Best Practices and the National Emergency Management Association (NEMA) co-sponsored the *States' Terrorism Policy Summit* in Williamsburg, Virginia. One of the many significant outcomes arising from that summit, which was hosted by Governor James S. Gilmore, was the concept that states needed to work together in partnership with the federal government to develop a coordinated national strategy to prepare for and deal with the consequences of domestic terrorism. As such, NGA and NEMA have again combined efforts to co-sponsor a series of regional forums to address domestic terrorism preparedness by bringing together state[145], local, and federal officials to share information and explore emerging issues about state and federal efforts. These regional meetings have been conducted throughout 2000, with meetings in Atlanta, Georgia, and Des Moines, Iowa that were hosted by Governor Roy Barnes and Governor Tom Vilsack, respectively. Another forum was held in Salt Lake City, Utah, and an additional regional meeting is planned for December in Boston, Massachusetts. In May, 2001 NGA and NEMA anticipate hosting a second national summit to discuss progress since February 1999, and to define the next steps in finalizing a national preparedness strategy.

STATES' RECOMMENDATIONS

At each of the policy forms, state officials were asked to make recommendations for improving the nation's ability to more effectively prepare for, respond to, and recover from the consequences of terrorism. The following is a compilation of these recommendations from the first three forums:

Threat/Awareness

1. Credible threat information on WMD is needed that is based on solid research, analysis and sound science rather than worst-case scenarios based on fiction.

2. States should put more emphasis on the awareness of vulnerabilities and threats concerning bioterrorism.

3. States should develop an effective strategy for communicating the potential threat to the public and the media.

4. States need additional training and technical assistance with conducting vulnerability assessments.

5. States should put more emphasis on the awareness of vulnerabilities and threats concerning cyberterrorism.

[145] The following states attended various regional meetings: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Florida, Hawaii, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, South Carolina, South Dakota, Tennessee, Texas, Virginia, Utah, Washington, West Virginia, Wyoming, Puerto Rico, the Virgin Islands and the District of Columbia.

6. States need to take action to ensure that awareness of the possibility of WMD incident at the executive level and to ensure continuity between Administrations.

Preparedness/Response

7. All levels of government should utilize and improve upon the existing emergency management and response systems and should not seek to "reinvent the wheel."

8. The federal government must develop an overall terrorism preparedness strategy that includes program consolidation between all agencies, funding consolidation, integration of goals and objectives, and a federal single point of contact. The strategy must address sustainability issues and also identify ways to engage the private sector in domestic preparedness. Further, this strategy should provide general guidelines and recommendations for state preparedness in order to tie the nation together in a united planning effort.

9. Long-term sustainability of federal funding and focus is a major concern for states. The answer is to integrate domestic preparedness into an all-hazards response capability, utilize available resources to enhance overall capabilities of state and local response systems.

7. All levels of government should adopt the Incident Command System.

8. All levels of government should formalize interagency relationships through operational protocols.

9. States should develop mutual aid agreements across multiple jurisdictions and consider developing a regional WMD response capability.

10. States should mandate WMD specific planning, training, and exercises beyond natural hazard approach and take advantage of all training opportunities.

11. All levels of government should ensure that crisis management and consequence management occur in coordination and in parallel.

12. States need to consider a statewide interoperable communications system.

13. States should develop teams (and consider using existing Y2K teams) to deal with cyberterrorism.

14. A WMD Overhead Management Team should be established to rapidly deploy and establish a Joint Operations Center (JOC). This team would be activated during a credible or actual terrorist event involving a weapon of mass destruction. It could be modeled after the National Incident Management Teams of the National Interagency Coordinating Group. They provide an overhead management system in response to major wildfires around the nation. They have also been used during other significant national events. A DOJ/FEMA component and training could be added to the National Interagency Coordinating Group for this purpose.

15. States need recommended templates, model legislation, and recognized "best practices" to assist them in WMD preparedness planning and response. NGA and NEMA were identified as the appropriate organizations to collect and disseminate these resources to the states.

16. A national interoperable Exercise Design and Planning System with an efficient After Action Reporting (AAR) mechanism is needed to design plan and conduct WMD exercises. The

Exercise Design and Planning System, EDAPS™ being developed for the New Mexico WMD program provides this type of application. It is a platform to greatly improve exercises and, it also provides a measure of standardization and interface without dictating a policy of standardization. http://demo.edaps.net.

17. States need to develop procedures to access National Pharmaceutical Stockpile including how to formally request resources and how local governments will receive it.

18. Agricultural terrorism needs to be addressed by states and the federal government.

Coordination/Information Sharing

19. Increased federal coordination is critical to the nations' overall capability to respond to a terrorist event.

20. States should require the establishment of joint terrorism working groups for coordination.

21. All levels of government should mandate a formal communication network between the intelligence community and medical community.

22. States should identify what intelligence information is needed at the state level and who can receive it and assess security clearances with the FBI.

23. Effective relationships should be built and maintained to enhance information sharing among agencies and levels of government.

24. With regard to the Joint Information Center (JIC), there must be a coordinated message from all three levels of government.

25. The NDPO, NGA or NEMA should serve as a clearinghouse for "best practices" and share model plans, effective programs, policy determinations, conference and training information, etc.

26. A national policy is needed for threat-based information sharing. States recommend that a national task force be established, with state and local representation, to develop new protocols for information sharing.

27. A national interoperable communications system with secure access is needed for responders. This system should utilize the newest available technology. States further recommend that the Federal Communications Commission (FCC) become engaged in communications interoperability issues.

Legal Authority/Constitutional Issues

28. Every state should examine state laws and authorities that relate to search and seizure, invasion of privacy, quarantine, evacuation, relocation or restricting access. States should develop comprehensive preparedness strategies that utilize all legally available assets.

29. Each Governor must have the appropriate authority to address the above issues as soon as the situation occurs and have these authorities in place before a WMD incident.

30. States should coordinate with each other regarding restricted access across state lines in a WMD incident.

31. The federal government and states may need to consider legislation to protect WMD intelligence information from Freedom of Information Act Requests.

Medical Issues

32. State public health capabilities must be enhanced nationwide. States recommend that the medical community be included as first responders in order to place increased emphasis on life-saving efforts.

33. States should plan, train, and exercise on a regular basis with the medical community including: HMOs; PPOs; and private hospitals.

34. States should develop a system that mandates information sharing with medical facilities and state epidemiological offices regarding actual, suspected, and potential terrorist activity.

35. All levels of government should identify ways to provide needed resources to hospitals such as equipment, training programs, pharmaceuticals, etc.

36. The Joint Commission on Hospital Accreditation should have a standard for hospital preparedness for terrorism.

37. There should be legal requirements for private hospitals to work cooperatively with the state on preparedness, particularly with regard to bio-terrorism surveillance and reporting.

Military Issues

38. States should integrate the WMD Civil Support Teams (formerly known as RAID Teams) into state planning, training, and exercises.

39. States and the military require specific funding to train and exercise together.

Funding

40. States must determine appropriate funding levels (state and federal contributions) for long-term sustainability such as multi-year funding to match multi-year planning goals and objectives. One-year funding does not allow long range planning and implementation for domestic preparedness. Federal funding levels are also not adequate when divided between all states and thousands of local communities.

41. States need to examine and address the funding needs of hospitals.

42. Congress and the federal government should consider threat and risk as a component of the criteria for state funding.

43. Congress and federal agencies should develop an expedited funding mechanism for grants to states.

44. Congress and federal agencies should consider setting aside a percentage of funds within grants to states for discretionary use based on the needs assessment and strategic plan of the state.

Training

45. All levels of government should seek to standardize training and exercises.

46. States should train with all agencies and volunteer organizations.

47. States should be aware of and take advantage of all federal training opportunities.

48. Many states have developed excellent WMD training courses. Increased federal support is needed for these state training programs so that they can be sustained and shared between states. A comprehensive compendium of all available federal training programs and funding would facilitate this process.

49. More training opportunities and forums are needed regarding vulnerability assessments. Cross discipline training is also needed to develop a common terminology.

Political

50. Given that a new Administration will be in place soon, Congress, the federal government, and states need to codify the funding authorizations and WMD preparedness programs that are in place now to ensure continuity and consistency in the future.

51. Much progress has been made with regard to WMD preparedness within a short period of time. All levels of government need to set baselines for where we are now and establish measurable goals and objectives for the future.

APPENDIX K—NATIONAL SURVEY METHODOLOGY

A Survey of Local Responder Organizations to Assess Federal Government Programs for CBRN Incident Preparation

Purpose of the Survey

The survey will elicit State and local response organizations' assessments of Federal programs intended to improve preparedness to respond to a CBRN terrorism incident. In addition to soliciting local responders' assessments of Federal programs, the survey will evaluate local awareness of CBRN issues and self-assessed local preparedness to respond to a CBRN incident, in order to put the assessments in context.

The survey differs from past surveys in that it is *not* a capability assessment, nor is it a readiness assessment. Rather, it is a vehicle for responder organizations to provide the Panel with a local responder assessment of Federal programs. The information collected will be used to inform and validate the Panel's deliberations, and the results will be presented as part of the final Panel report.

Assessment questions will fall into two major categories: (1) Questions pertaining to a subjective assessment of existing Federal government programs aimed at improving local responder CBRN preparedness, and (2) local responder desires and needs for Federal Government programs, both those programs that exist but have not yet been provided or made available to certain local responder organizations and those that are desired or required but do not exist. A general description of the survey follows.

Survey Outline

Survey questions will be tailored to the individual local responder organization—e.g., police department, EMS organization, and public health department—but designed with a significant amount of similarity and commonality between organizations. This design will allow evaluation within individual responder organizations and comparisons between types of responder organizations. The survey will ask questions in several categories:

Organizational Descriptive Information. These questions will characterize the organization in terms of function, size, location, and other characteristics.

Organizational Threat Perceptions and Experience. These questions will capture how credible the organizations consider the various types of CBRN threats and whether the organization has had experience with actual or threatened incidents.

Readiness Assessment, Using Both Subjective and Objective Measures. These questions will provide some information about current organizational readiness for CBRN incidents.

Local Responder Assessment of Their Support Needs and of Current Federal Programs. Assessment will include existing Federal Government programs aimed at improving local responder CBRN preparedness and local responder desires and needs for support and for Federal Government programs. Queries will include awareness of and participation in key Federal programs intended to support and improve preparedness efforts at the local and State-levels, as well as barriers encountered in terms of participation such as cost, availability, time constraints, and others. Examples include grant programs for equipment purchasing, funding for training and joint exercise opportunities, information sources and threat assessment updates, technical assistance programs.

Survey Methodology

The survey will be fielded in March of 2001. The survey will be conducted by mail and will be approximately 1/2 hour in length in order to maximize the response rate. Questions will primarily be scenario-based and closed ended for specificity, with some open-ended final questions to allow for unstructured input. Respondent and organizational anonymity will be promised.

The survey will employ a two-stage sampling strategy in which 200 counties will first be randomly chosen[146] throughout the United States and then one of each of the following types of local responder organizations will be chosen within each county:

- Law enforcement
- Fire departments, both professional and volunteer
- HAZMAT organizations (separate from fire departments)
- Hospitals
- Emergency medical services (separate from hospitals and fire departments)
- County coroners
- Public health departments
- Offices of emergency management and/or local CBRN/terrorism working groups

The sample will be chosen so that it is statistically representative of each responder organization population and of local responders in general. In addition, public health departments and offices of emergency management of every State will be surveyed.

For the county organizations, we will sample 200 organizations. An 80 percent response rate, yielding 160 completed surveys per type of organization, will result in a confidence interval half-width of 10 percent at the organizational level, meaning that a 95 percent confidence interval around the percentage of organizations agreeing with a binary response question will be plus or minus 10 percent. For questions and analyses that span all the organizations, the confidence intervals will be significantly smaller.

[146] The probability of selection into the sample will be a function of county population. The probabilities will be set so that counties with larger populations have a higher probability of selection; however, small and rural counties will also be included in the sample. This sampling scheme was specifically chosen so that the maximum amount of information can be obtained.

APPENDIX L—TOPOFF OBSERVATIONS

Several members of the Advisory Panel[147] and its support staff observed the conduct of the national exercise, directed by Congress, called "Top Officials 2000" or TOPOFF, during the period May 20-24, 2000. Members and staff also observed two of the "after-action" reviews following the exercise.

The major purpose of the exercise was to engage "top" or senior officials at the Federal level, especially the heads of agencies with significant responsibilities for combating terrorism. The exercise was conducted under the joint direction of the Department of Justice Office of State and Local Domestic Preparedness Support and the Federal Emergency Management Agency.

There were two "field venues" for the exercise[148]—Portsmouth, New Hampshire, and Denver, Colorad0—in addition to the Federal agency exercise locations in the National Capital area. There was each field venue had a its own terrorist "attack" scenario. In Portsmouth, the attack involved a mustard gas chemical device; in Denver, there was a biological attack involving a release of "plague."

General Observations

The exercise was only partially successful in engaging the heads of Federal agencies. Observers made special note of the direct and intense involvement of the Attorney General of the United States, who participated in many of the pre-exercise orientations, and was in the national emergency operations center (the FBI's Strategic Information and Operations Center) for much of the exercise itself. The Director of the Federal Emergency Management Agency also devoted considerable personal time prior to and during the exercise. Beyond that, many agency "heads" were designated stand-ins for actual agency heads.

There is significant value in exercises like TOPOFF, that are more than "table-top" paper shuffles. With its two major "field" events and separate scenarios, the exercise provided a degree of realism on issues such as the potential stress on health and medical treatment activities, as well as the identification of numerous coordination problems among various governmental agencies at all levels. We encourage additional exercises, and have recommended more coordination and structure to a national plan for that purpose.

Realism

TOPOFF was intended to be a "no-notice" exercise, with the realistic objective of little or no advance warning of a terrorist attack. In large measure, the exercise failed to achieve

[147] Vice Chairman Jim Clapper, and members Richard Falkenrath, George Foresman, Jim Greenleaf, and Paul Maniscalco.

[148] A third field venue – the National Capital area – was originally designed as part of the total TOPOFF exercise. For reasons not fully explained to observers, that part of the exercise – a radiological release - was removed from TOPOFF and run as a "concurrent" exercise, National Capital Region 2000.

that objective. Almost everyone directly involved knew the general exercise time frame weeks in advance and were able to pinpoint the actual start several days in advance. Some of the reasons advanced for that result include the requirement to arrange logistics and other administrative details well in advance, ensuring that certain key officials were actually available, scheduling response personnel in order not to disrupt real-life activities, potential problems with overtime pay for response personnel, and others. All of those factors will, however, pertain if an actual attack occurs. It is our view that a true test of the ability of various systems and processes, with virtually no notice, is better for learning lessons than a carefully structured one.

The unfortunate result was a substantial loss of realism. Equipment and personnel assets were "pre-positioned," normal leaves were cancelled; certain advance coordination that might not ordinarily be accomplished in advance had already been undertaken.

Recognizing that such reaction may be hard to replicate in an exercise, one observer noted that there was generally no simulated "panic" or the intense sense of urgency that would attend an actual event.

Moreover, the perception among State and local officials at the Portsmouth venue was that, given the specific scenario, the level of Federal response provided was much greater than would be required if it had been an actual attack of the same magnitude, one senior official musing that State and local entities could have handled the attack without any Federal assistance.

Cost of the Exercise

Observers were critical at the apparently excessive cost of the exercise. It is our view that exercises of this nature can and should be conducted "internally." We believe that there is no need to "contract out" most of the exercise design and execution. Several agencies of the Federal government, notably numerous elements of the Department of Defense, the Federal Emergency Management, various Federal law enforcement agencies, and other entities have significant expertise in the design and conduct of exercises. Contractors are not likely to be readily available when an event occurs; actual systems need to be tested.

In addition, panel observers came away with the impression that too much money was spent unnecessarily, on such items as T-shirts, pins, caps, other "commemorative" items, and costly facilities.

"Consequence" and "Crisis" Management

The exercise reinforced our concern with the attempt to draw a bright line between "crisis" and "consequence" management responsibilities and authority.

One panel observer noted that the FBI does not focus on anything other than "crisis management." The FBI agents in Portsmouth did not appear to be sensitive to

"consequence management" issues or coordination. While it is true that the FBI has the Federal lead for "crisis management," it is clear that the two overlap to such an extent that coordination of all response activities must have a central, not bifurcated, focus.

Use of the Military

The exercise highlighted both advantages in using the obviously robust capability of the military, and problems in its coordination and execution. The FBI learned that, for "crisis management" activities, there are potentially major differences in their understanding of the military mission, and they way the military structure itself views their roles and missions.

Who's in Charge?

This question was not resolved in TOPOFF. Coordination issues arose that can, nevertheless, be fixed; and we are confident that some will.

There were clearly problems with the organization and location of various "operations" centers. Part of the problem had to do with available facilities, but part is cultural or parochial or both. We address the issue with specific recommendations in Chapter Three.

As late a 4:00 PM on the day that the attacks actually took place, no Federal agency had stepped forward and announced its "lead agency" role. That designation should not be assumed. It must be clear, preferably in advance of an incident. (See more discussion on operational relationships in Chapter 3.)

Even as late as the after-action review four weeks after the exercise, relationships were not clear. A state official asked the senior FEMA representative if FEMA is "in charge" of all consequence management or only the Federal piece. After some thought, the answer was, "Only the Federal piece."

During the exercise, FEMA representatives were not able to list the full range of support available at the Federal level to assist State and local responders.

Independent Exercise Evaluation

For valuable lessons to be captured for future reference, it is essential in our view that there be a thorough and independent evaluation of such exercises. Other than the fact that the General Accounting Office also observed the exercise and has prepared a briefing on its observation, there was not structured evaluation of TOPOFF.

APPENDIX M—DEPARTMENT OF DEFENSE PROGRAM INFORMATION[149]

Civilian Oversight and Accountability

A large number of DoD entities (including elements of the military departments and defense agencies, and the combatant Commanders-in-Chief) have varying responsibilities for parts of DoD activities for combating terrorism.[150] The Assistant Secretary of Defense-Special Operations/Low Intensity Conflict is responsible for most "anti-terrorism" programs—primarily the engagement, outside of the United States, of special purpose forces, equipment, and other capabilities. The Secretary has designated another civilian as Assistant *to* the Secretary for Civil Support,[151] who has principal responsibility for policy development for "consequence management" activities, including direct coordination. Other Assistant Secretaries and senior agency officials have responsibility for other aspects of the Department's total effort. The Congress is now requiring the DoD to designate an Assistant Secretary of Defense as the senior civilian "with the overall supervision of the Department's combating terrorism activities,"[152] apparently for the purpose of vesting political accountability and responsibility in a person appointed by the President and confirmed by the Senate.

In addition, the Congress has directed the Secretary to provide to the Congress a detailed report on activities to protect military installations from terrorist attack, and to provide adequate response capability on those installations to respond to such attacks.[153]

Command and Control

In 1999, DoD established a new headquarters for the planning efforts, and command and control of subordinate military elements, for providing "consequence management" support to domestic civil authorities. The Joint Task Force-Civil Support (JTF-CS) is a

---

[149] This is an on-going assessment of several aspects of DoD combating terrorism programs and activities. It is not an exhaustive review of all such DoD programs. Such an undertaking would require considerable time and significant resources. The Advisory Panel will, nevertheless, continue to analyze, assess, and comment on certain DoD activities.

[150] See chart attached.

[151] This is not an Assistant Secretary position, *i.e.*, appointed by the President, subject to Senate confirmation.

[152] Section 901, National Defense Authorization Act for Fiscal Year 2001 (NDAA FY01)(HR 4205, Pub. L. 106-398). See discussion in Conference Report to accompany NDAA FY01, p. 833.

[153] Section 1031, NDAA FY01 requires the Secretary of Defense "to submit to Congress a report on the program of the Department of Defense (DOD) to ensure the preparedness of DOD first responders for incidents involving weapons of mass destruction on military installations." The provision directs the Secretary "to include within the report the following: (1) a detailed description of the program; (2) the schedule and costs associated with the implementation of the program; (3) how the program is being coordinated with first responders in the communities in the localities of the installations; and (4) the plan for promoting the interoperability of the equipment used by first responders on DOD installations with the equipment used by the first responders in the local communities. . ." as well as "a description of deficiencies in the preparedness of DOD installations to respond to a weapon of mass destruction incident and the plans of the Department to correct those deficiencies." Conference Report to accompany NDAA FY01, p. 848.

major subordinate command of the U.S. Joint Forces Command (previously U.S. Atlantic Command), headquartered at Norfolk Naval Base, Virginia. On the surface, this new structure seems to provide an appropriate focus for activities for combating terrorism. Nevertheless, it now creates two separate systems for providing military assistance to civil authorities.

Military activities to support civil authorities in emergency response had previously been coordinated through the U.S. Army's Director of Military Support (DOMS).[154] JTF-CS will now direct consequence management support for terrorism, while DOMS will be responsible for similar support in other emergencies, especially any military assistance for response to a natural disaster under provisions of the Stafford Act. The commander of JTF-CS has made it clear that his organization will only engage in "consequence management" support activities, and events during TOPOFF 2000 substantiated that position. While the JTF-CS and staff were present at Portsmouth, New Hampshire, to respond to requests for "consequence management" support, special purpose forces deployed to the same venue, under different command structure, to provide direct support to the FBI. Other structures, including additional JTFs under various combatant commands, could be used for such "crisis" purposes, but such structures are not well defined.

National Guard Activities and Structure

Congress and DoD have considered a number of missions and structures for the National Guard to provide additional combating terrorism support to civilian authorities. There have been numerous studies and analyses on the subject, including an exhaustive study in 1998-1999.[155]

National Guard units and personnel have been thought to be an especially attractive asset for several reasons, including:

- Guard elements are normally under the authority of State Governors, under provisions of U.S. Code, Title 32. It is only when Guard personnel conduct overseas training or when they have been mobilized and deployed under provisions of Title 10 or other statutes that they become "Federal" forces. In that Title 32 status, the Governor can direct their employment anywhere in the state that they may be needed. Moreover, Governors of several States may agree to use Guard elements for mutual support.
- Guard personnel in a Title 32 or "state" status are not automatically subject to the restrictions of 18 U. S. Code, Section 1385 – the so-called Posse Comitatus Act – and other statutory restrictions on the use of the military domestically.[156]
- Guard units and personnel are "local." They are viewed as integral parts of communities; many are employed in their civilian capacity in law enforcement, fire services, and other "response" occupations. Being local, they are likely to be

[154] The Department of the Army had been serving as "Executive Agent" of the DoD for such purposes.
[155] National Guard Support for Terrorism Response, SAIC, March 1999.
[156] See Appendix R for a discussion of those statutory restrictions.

able to respond more quickly than an active duty military element from somewhere else in the country.

In 1998, Congress directed the creation of certain National Guard detachments or teams, designed specifically to assist State and local response entities in "consequence management" activities. Those units, originally designated Rapid Assessment and Initial Detection (RAID) teams, are now known as Weapons of Mass Destruction Civil Support Teams or WMDCSTs. Starting with ten teams, composed of 22 full-time National Guard active duty personnel, in 1999, Congress directed an additional 17 teams in fiscal year 2000, and recently added five more,[157] for a total of 32.[158]

Training

In Chapter Three, there is a discussion of the Domestic Preparedness Program (the "120 Cities" training program established under the provisions of the Nunn-Lugar-Domenici Act). Even with the transfer of most aspects of that program to the Department of Justice, DoD continues to have a number of other training and exercise programs, several of which involve direct participation by State and local responders.[159] Nevertheless, there apparently is no comprehensive DoD plan or standard for the conduct of such training activities, nor a senior official designated for the oversight of terrorism-related training programs.

Domestic Preparedness Programs for Combating Terrorism

DoD had a total budget for combating terrorism of approximately $4.5 billion for FY 2000. A significant portion of that budget goes to support DoD anti-terrorism programs.

What follows is programmatic description that is limited to major research, development, training, and equipment programs within DoD deemed relevant to domestic preparedness and response for terrorist incidents. Some programs may only be indirectly related to State and local terrorism preparedness. The spending on such programs totaled $766.5 million in FY2000, about 18% of the total DoD budget of $4.5 billion for programs to combat terrorism.

In its 18 May 2000 Annual Report to Congress, the Office of Management and Budget records only $476 million in FY2000 WMD preparedness spending for the entire "national security community"—a further indication that it is difficult to discern what programs are included in the OMB report.

The information contained in this analysis is derived from a 200-page DoD Combating Terrorism budget document, one that is primarily informational. It appears to be a compilation of programs, rather than an attempt to establish spending priorities or

[157] Section 1032, NDAA FY01.
[158] WMDCSTs are being allocated on the basis of one per State, with the exception of California, which has two.
[159] The U.S. Marine Corps Chem-Bio exercise program is one example.

provide direction to the numerous DoD agencies involved. That is especially true with research and development programs.

Having said that, the DoD budget document, which provides a description of each program, is much more comprehensive and inclusive than any that we have found in any other agency. Individual program descriptions are grouped according to the entity in DoD with which each is associated.

UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY AND LOGISTICS

1. Physical Security Equipment Program**,** $25.4 million (FY00)

The Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics) is responsible for the execution of the PSE Program. This program utilizes an ongoing DoD-coordinated Joint Action Group, including the three Services and the Defense Threat Reduction Agency. Other representatives may include DoE, DoJ and NIJ. The Joint Action Group's primary functions include monitoring, directing and prioritizing potential and existing PSE programs. Each of the Services or CINC users can nominate products for Force Protection commercial off the shelf evaluation and testing.

2. Chemical/Biological Defense Program, $15.4 million (FY00)

The Defense Threat Reduction Agency (DTRA) is responsible for the Chemical/Biological Defense Program. Among its projects, this program assesses military installations' vulnerabilities to chemical and biological threats. In addition, FY2000 plans included providing technical support and upgrades to the CD-ROM planning tools for Joint Staff Anti-Terrorism/Force Protection initiatives.

JSIVA Teams (Joint Staff Integrated Vulnerability Assessment) became indigenous to DTRA in FY2000, giving installation commanders and First Responders the training and tools necessary to limit their vulnerability to the threat of WMD terrorism and react in a manner that will save lives.

The Chemical/Biological Program also provided equipment and training for 5 WMD Civil Support Teams in FY2000 and will provide funds for improved Chemical Agent Monitors and Chemical Agent Monitor simulators in FY2001.

3. Biological Warfare Defense Program, $131.7 million (FY00)

The Defense Advanced Research Project Agency manages and directs this program, which develops and tests medical response, detection, defensive/protective systems, genetic sequencing, and consequence management to protect against the possible use of biological warfare agents (including bacterial, viral and bio-engineered organisms and toxins) by both military and terrorist opponents. DARPA coordinates its activities with DTRA, the Food and Drug Administration, the Centers for Disease Control and Prevention, the Department of Energy, and the intelligence community.

Some examples of the technologies that this program will explore in FY2001 are included below:

- Build and test a prototype air purification system for collective protection

- Test, in model systems, one or more of the most promising candidate strategies for rapid detection based on bodily responses or other biomarkers to provide early indicators of infection or exposure
- Develop neutralization technologies for aerosolized agents

UNDER SECRETARY OF DEFENSE FOR POLICY

4. Combating Terrorism Technology Support (CTTS) Program, $43.6 million (FY00)

The Office of the Assistant Secretary for Special Operations and Low Intensity Conflict, OASD (SO/LIC), administers the CTTS Program. This program helps fund research and development efforts as part of DoD's Technical Support Working Group, which is the R&D component of the Interagency Working Group on Counterterrorism. The program also works with the White House Office of Science and Technology to determine current government-wide deficiencies that could be addressed with non-medical research and development. Examples of CTTS Program projects for FY01 are as follows:

- Detection and defeat of improvised explosive devices,
- Protection and assurance of critical government, public and private infrastructure systems required to maintain the national and economic security of the U.S,
- Investigative and forensic support to terrorist related cases,
- Improvements in personnel protective equipment for escaping the immediate vicinity of a terrorist attack, and
- Development of systems to support the treatment of mass casualties, as well as WMD threat remediation in urban areas.

CHAIRMAN, JOINT CHIEFS OF STAFF

5. Deputy Directorate for Operations (Combating Terrorism), $2.1 million (FY00)

In 1999 this office coordinated the JSIVAs program that managed and allocated 96 JSIVAs that assessed DoD installations in the area of physical security, counter-operations, intelligence and counterintelligence, operational readiness, structural engineering, and infrastructure engineering. These teams provided commanders with expert assessments of their vulnerability to terrorist attacks.

Funding also includes a Force Protection Equipment Demonstration that will showcase commercial off-the-shelf force protection equipment. The funding for FY2001 includes Executive Seminars on antiterrorism and implementation of the Best Practices Study.

DEPARTMENT OF THE ARMY

6. Domestic Preparedness Program, $32.1 million (FY00)

With the transition of the Domestic Preparedness Program to the Department of Justice, overall FY01 program funding will be significantly reduced from FY00 (by $10 million). The U.S. Army will still maintain the following programs in FY01:

- *Expert Assistance Program*: The Chem-Bio Database is one of three components that comprise the Rapid Response Information System (RRIS) being developed and maintained

by FEMA with interagency members for use by State and local authorities; its maintenance will continue to be a U.S. Army responsibility.

- *Equipment Testing Program*: The Equipment Testing Program evaluates and tests commercial protective equipment using live agents.

- *Chemical and Biological Improved Response Program*: This program relates to DoD activities with the chemical stockpile emergency preparedness program (CSEPP) and the WMD Civil Support Teams. As a result, the funding projects for these programs assume that DoD will bear half of the estimated total program cost, while DoJ assumes the other half.

- *Chemical-Biological Rapid Response Team*: DoD is required to maintain at least one domestic rapid response team per Section 1414 of Pub. L. 104-201. This requirement does not include the WMD Civil Support Teams since they are under the direction of State governors.

7. Security, Force Protection and Law Enforcement Division, $136.6 million (FY00)

The Office of the Deputy Chief of Staff for Operations, U.S. Army provides for anti-terrorism functional courses in the Army's Service School System and the Military Police School. Mobile Training Teams also conduct training at various locations. This training is not part of the Domestic Preparedness Program nor other programs for training State and local law enforcement and first responders.

8. Consequence Management Program (CoMPIO), $107.2 million (FY00)

The Secretary of the Army, as Executive Agent for Military Support to Civil Authorities, established a Consequence Management Program and Integration Office. The CoMPIO program responsibilities include: management of the operational training exercises for the WMD Civil Support Teams and Military Support Detachment, and existing Reserve Component domestic response, casualty decontamination, NBC reconnaissance, medical, engineering, security, information, communications, logistics, and transportation organizations supporting civil authorities in preparing for and responding to the consequences of terrorist attacks using weapons of mass destruction within the United States.

9. Additional U.S. Army Programs, specific combating terrorism funding unknown.

In addition to the three programs listed above, the U.S. Army is involved in various research, development, training, and exercising programs that may relate indirectly to WMD response and yet are not included in the overall DoD combating terrorism FY2001 budget. These programs include: US Army 52nd Ordnance Group, US Army Technical Support Unit, US Army Response Task Forces, US Army Medical Research Institute of Chemical Defense, US Army Medical Research Institute of Infectious Diseases, US Army Edgewood Chemical and Biological Forensic Analytical Center Modular On-Site Laboratory, US Army Radiological Control Team, and the US Army Radiological Advisory Medical Team.

DEPARTMENT OF THE NAVY

10. Joint Task Force-Civil Support, Atlantic Command, $5.6 million (FY00)

Costs associated with the headquarters and for coordination and planning activities of the joint task force.

11. Chemical Biological Incident Response Force, $1.4 million (FY00)

The Marine Corps System Command's CBIRF research and development programs work towards the development of key technologies that will benefit CBIRF and the armed forces as a whole. These improvements are in the areas of reconnaissance, decontamination, emergency medical support, communications and general support and force protection.

12. Navy Force Protection Division, $152.0 million (FY00)

Like the U.S. Army force protection programs, these training efforts do not directly apply to domestic response capabilities. However it is important to note that the U.S. Navy is also conducting anti-terrorism awareness and training program and a cross-agency dialogue may inform each organization's "best practices." The funding noted above includes material, supplies, equipment and travel costs to conduct criminal investigative services and antiterrorism awareness training program ashore and afloat, as well as domestic terrorism coordination and investigation of theft of navy ordnance.

DEPARTMENT OF THE AIR FORCE

13. First Responder -- WMD Threat Response Program, $73.0 million (FY00)

This program provides first responder (fire, EOD, security forces, medical personnel, and CE readiness) WMD planning, training, exercising and equipment capabilities for Air Force installations. The training is modeled after the WMD Civil Support Teams and the Texas A&M Training Academy programs and is intended to provide direct support for CBIRF deployment. In FY2000 the Air Force spent $73 million on Foreign Emergency Support Team (FEST) aircraft, but nothing on first responder training. The FY2001 budget proposal ($2.7 million) does not reflect any additional procurement.

14. Air Force Office of Special Investigations, FY 40.5 million (FY00)

The Air Force also has its own antiterrorism training program. The FY 01 program funding includes: 9,748 antiterrorism training sessions and 6 interactive courses for senior Air Force leaders and their drivers.

MILITARY PERSONNEL SPENDING FOR COMBATING TERRORISM

The budget numbers attached to the brief program descriptions listed above do not include spending for military personnel. Not all spending for domestic preparedness for terrorism has been, nor perhaps can be, captured. Spending for such personnel costs that has been included in the DoD budget document is summarized below.

The first chart provides personnel costs for the Consequence Management and Domestic Preparedness Programs. The Consequence Management program personnel funding for FY2000 is primarily for the National Guard WMDCSTs. For FY2001, according to the DoD budget submission, costs also include the "local Department of Defense installation commander's training for first responders." The Domestic Preparedness program costs for FY2000 reflect DoD's exclusive responsibility for its implementation. Most of that program transferred to DOJ on October 1, 2000.

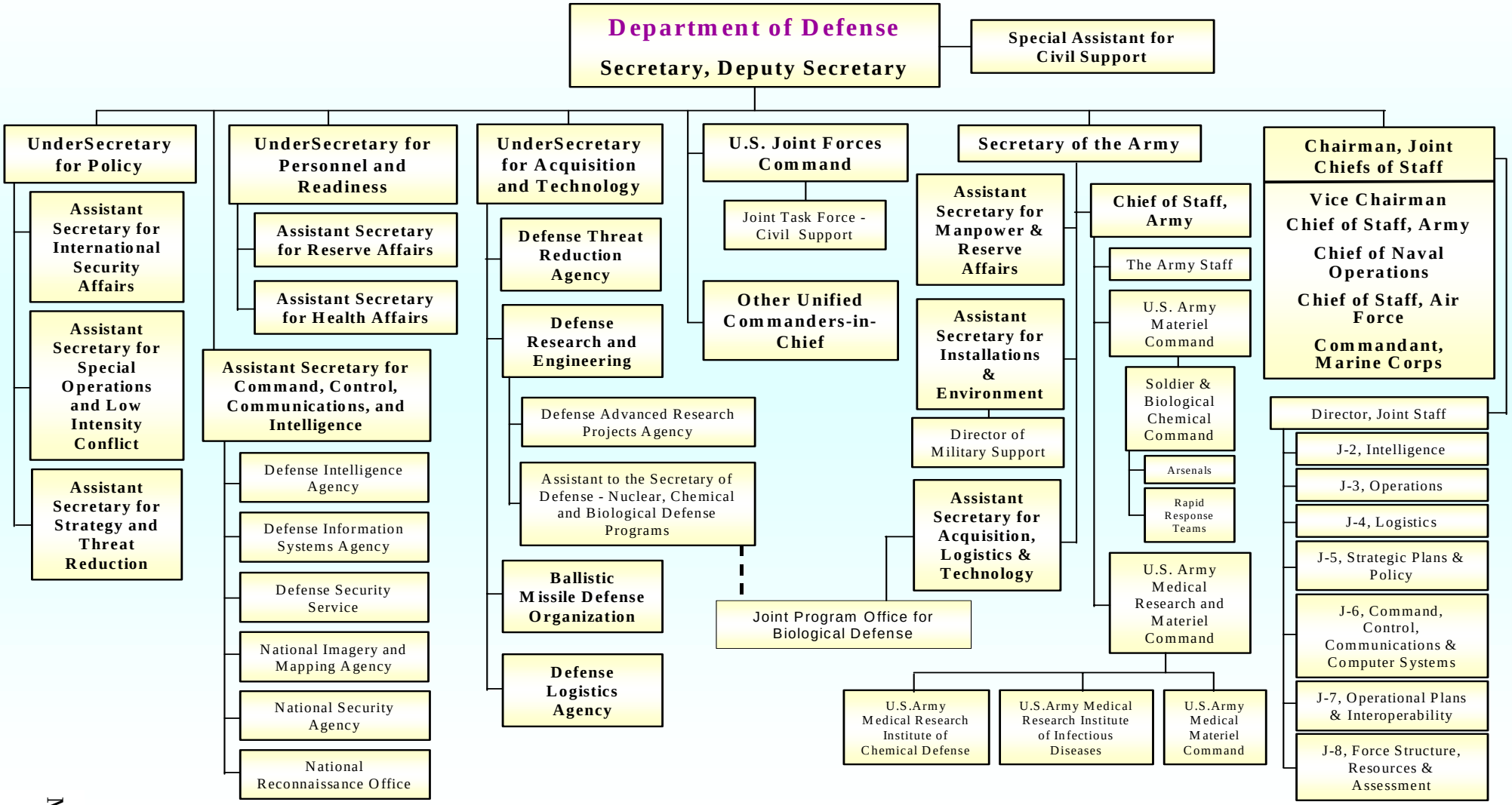
Consequence Management and Domestic Preparedness Programs			
Agency	Category	FY2000	FY2001
Army	AC Military personnel	$ 600,000	$ 100,000
	National Guard	20,000,000	27,500,000
	Reserve	2,100,000	100,000
Navy	*	*	*
Marine Corps	*	*	*
Air Force	National Guard	5,400,000	6,700,000
Consequence Management Totals		$ 28,100,000	$ 34,400,000

*Note: The Navy and the Marine Corps did not provide a breakdown of spending on personnel. The Navy had 26 personnel (primarily for JTF-CS) and the Marine Corps had 373 personnel dedicated to consequence management in FY2000. (primarily for CBIRF). In neither case were personnel costs provided.

Personnel costs reflected in the following chart represent spending for all terrorism programs—anti-terrorism, counter-terrorism, "crisis management," and "consequence management," domestic preparedness, force protection, and installation defense—worldwide. Personnel costs in the preceding chart are include in the totals below.

Total Military Personnel Spending for Combating Terrorism			
Agency	Category	FY2000	FY2001
Army	AC Military personnel	$ 676,500,000	$ 698,200,000
	National Guard	85,100,000	94,100,000
	Reserve	46,800,000	45,200,000
Navy	AC Military personnel	155,190,000	167,240,000
	Reserve	11,959,000	12,678,000
Marine Corps	AC Military personnel	308,809,000	322,418,000
	Reserve	4,290,000	4,540,000
Air Force	AC Military personnel	901,000,000	938,500,000
	National Guard	95,900,000	100,900,000
	Reserve	34,800,000	35,500,000
SOCOM	AC Military personnel	92,596,000	99,025,000
Totals		$2,320,440,596	$ 2,518,301,000

Department of Defense Organizational Structure for Combating Terrorism



APPENDIX N—DEPARTMENT OF JUSTICE PROGRAM INFORMATION

The Department of Justice has not produced a document that provides program description for all combating terrorism programs in DOJ. Most such programs are administered either through the Office of Justice Programs (OJP), and its subordinate entities, especially the Office of State and Local Domestic Preparedness Support, or through the Federal Bureau of Investigation. As the following charts indicate, the OMB budget document for the DOJ portion of "WMD Preparedness" also provides limited details.

OMB Summary of DOJ's Combating Terrorism Spending

Dollars in Millions	*FY99 Actual*	*FY00 Enacted*	*FY01 Request*
WMD Preparedness	$201.20	$217.20	$254.70
CIP	54.10	44.00	45.50
Totals (Dollars in Millions)	$255.30	$261.20	$300.20

Within the main body of the report (Chapter 3), we have commented favorably on specific aspects of the DOJ programs, particularly the equipment grant program, and the "assessment" tool developed by OSLDPS as part of that process; we have also expressed our concern about the potential impact of the transfer of the Domestic Preparedness Program from the DoD to DOJ. In Appendix L, we have included specific comments on the observation of the TOPOFF exercise by members of the Advisory Panel.

As noted elsewhere in this report, the vast majority of the programs under OJP have never been authorized. They only exist through a funding stream provided in a succession of appropriations bills. That will continue to be the case in FY2001, assuming that applicable provisions of the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act for 2001 is eventually signed into law in substantially the form passed by the Congress.

OJP FY2000 Program Plan Summary

Office	*Program*	*FY00 Enacted*
Bureau of Justice Assistance	**State and Local Anti-Terrorism Training**	$ 2.00
National Institute of Justice	**Counterterrorism Technology**	37.20
Office for Victims of Crime	**N/A**	0.70
Office for State and Local Domestic Preparedness Support	**See OSLDPS chart below**	94.80
Totals	**(Dollars in Millions)**	**$134.70**

Provisions contained in the FY2001 Conference Report to accompany that appropriations act are descriptive of the problems with programs not properly authorized and the impact of special funding earmarks:[160]

"Counterterrorism Assistance. A total of $220,980,000 to continue the initiative to prepare, equip, and train State and local entities to respond to incidents of chemical, biological, radiological, and other types of domestic terrorism. Funding is provided as follows:

"Equipment. $109,400,000 is provided for grants to equip State and local first responders, including, but not limited to, firefighters and emergency services personnel, as follows:

"$97,000,000 for Domestic Preparedness Equipment Grants to be used to procure specialized equipment required by State and local first responders to respond to terrorist incidents involving chemical, biological, radiological, and explosive weapons of mass destruction (WMD). The conference agreement continues the direction included in the fiscal year 2000 Appropriations Act, allowing funds to be allocated only in accordance with an approved State plan, and adopts the direction included in the Senate report requiring 80 percent of each State's funding to be provided to local communities with the greatest need.

"Within the total amount provided for these grants, up to $2,000,000 shall be made available for continued support of the Domestic Preparedness Equipment Technical Assistance program at the Pine Bluff Arsenal; $5,000,000 is for equipment grants for State and local bomb technicians; and$7,400,000 is for pre-positioned equipment.

"Nunn-Lugar-Domenici Program (NLD). $20,980,000 is for the NLD Domestic Preparedness Program authorized under the National Defense Authorization Act, 1997, and previously funded by the Department of Defense, to provide training and other assistance to the 120 largest U.S. cities. On April 6, 2000, the President proposed the transfer of responsibility for completion of the NLD program to the Department of Justice. The conference agreement provides the full amount necessary to complete the NLD program, of which $8,100,000 is for training and $6,880,000 is for exercises for the remainder of the 120 cities; $3,000,000 is for Improved Response Plans; and $3,000,000 is for management and administrative costs associated with this program. Within the amounts provided for Domestic Preparedness Equipment grants, the Office of Justice Programs may provide equipment to NLD cities if such equipment is necessary to fulfill the requirements of the program. The conference agreement includes a series of new programs to address training and exercise requirements on a national basis, and expects the Office of Justice Programs to provide any future training and exercises assistance through these programs.

[160] Conference Report 106-1005, 106th Congress, 2nd Session, Title I extract.

"Training. $45,500,000 is for training programs for State and local first responders, to be distributed as follows:

"$33,500,000 is for the National Domestic Preparedness Consortium, of which $15,500,000 is for the Center for Domestic Preparedness at Ft. McClellan, Alabama, including $500,000 for management and administration of the Center; $5,250,000 is for the Texas Engineering Extension Service at Texas A&M; and $12,750,000 is to be equally divided among the three other Consortium members; $8,000,000 is for additional training programs to address emerging training needs not provided for by the Consortium or elsewhere. In distributing these funds, OJP is expected to consider the needs of firefighters and emergency services personnel, and State and local law enforcement; $3,000,000 is for continuation of distance learning training programs at the National Terrorism Preparedness Institute at the Southeastern Public Safety Institute to provide training through advanced distributive learning technology and other mechanisms; and $1,000,000 is for continuation of the State and Local Antiterrorism Training Program.

"Exercises. $7,000,000 is for exercise programs, of which $4,000,000 is for grants to assist State and local jurisdictions in planning and conducting exercises to enhance their response capabilities, and $3,000,000 is for planning, execution, and analysis of TOPOFF II.

"Technical Assistance. $2,000,000 is for technical assistance to States and localities.

"Counterterrorism Research and Development. $36,100,000 is for counterterrorism research and development, of which $18,000,000 is for the Dartmouth Institute for Security Technology Studies (ISTS),$18,000,000 is for the Oklahoma City National Memorial Institute for the Prevention of Terrorism (MIPT), and $100,000 is for a pilot project to develop an RDT&E system similar to the Department of Defense System, as proposed in the Senate report. Within the amount provided for MIPT, up to $4,000,000 is to be used to support the development of performance standards in a biological and chemical environment for respirators and personal protective garments. The MIPT and the ISTS are directed to work with the Technical Support Working Group and the National Domestic Preparedness Office to develop and implement a process whereby WMD equipment is standardized."

Broad programmatic descriptions of the application of similar funds for FY2000 are shown in the following table.

Office for State and Local Domestic Preparedness Support		
Program/Grant		**FY00 Enacted**
National Domestic Preparedness Consortium		$10.50
Center for Domestic Preparedness		13.00
Metropolitan Firefighters and Emergency Medical Services Training Program		1.50
WMD Awareness for Sheriffs		0.60
Personal Scene Safety Training		0.50
State Domestic Preparedness Equipment Support Program		64.50
State and Local Domestic Preparedness Exercise Program		1.20
State and Local Domestic Preparedness Technical Assistance Program		1.50
Executive Session on Domestic Preparedness		0.75
Terrorism Policy Workshops		0.75
Totals	**(Dollars in Millions)**	**$94.80**
* Note: In FY01, the Domestic Preparedness Training Program, formerly at DoD will shift to DOJ, costing approximately $31 million.		

APPENDIX O—PANEL ACTIVITIES

Calendar Year 2000

During the past year, the panel held four formal meetings:

March 29, 2000 at the Pentagon, Washington, DC
July 17-18, RAND Washington Office, Arlington, VA
September 28-29, Library of Virginia, Richmond, VA
November 27-28, RAND Washington Office, Arlington, VA

During the course of those meetings, panel members received formal presentations from the following:

- Barry Kelman, DePaul University School of Law, and Michael Wermuth, RAND Project Director, on International and Domestic Law regarding Terrorism
- Pam Berkowsky, Assistant to the Secretary of Defense-Civil Support, and BG Bruce Lawlor, Commander, Joint Task Force-Civil Support, on DoD Terrorism Policy and Force Structure Issues
- Ed Plaugher, Chief, Arlington County (VA) Fire Department, Dr. Henry Siegelson, Emory University Medical Center, and Panel Members Dr. Patricia Quinlisk and Dr. Ken Shine, on Critical Health and Medical Issues
- Richard Clarke, Special Assistant to the President for Transnational Threats and National Coordinator for Infrastructure Protection and Counter-terrorism, and Lisa Gordon Hagerty, NSC Director for Transnational Threats, with NSC Terrorism Updates
- Ted Macklin, Office of State and Local Domestic Preparedness Support (DOJ), and Anne Martin, Federal Emergency Management Agency, Exercise Co-Directors for TOPOFF 2000
- George Goodwin and Richard Babarsky, Ph.D., Joint Assessment of Catastrophic Events, National Ground Intelligence Center; Major Adrian Bogart and Special Agent John Frank, InterAgency Board for Equipment Standardization and InterOperability (IAB); Andy Mitchell, Office of State and Local Domestic Preparedness Support, Department of Justice; and LTC Don Buley, Joint Program Office for Biological Defense, Department of Defense, on Technology, Equipment and Standards
- Panel Member L. Paul “Jerry” Bremer, on the Report of the National Commission on Terrorism
- Panel Members Jim Clapper, Jim Greenleaf, Richard Falkenrath, George Foresman, and Paul Maniscalco, and RAND Project Director Mike Wermuth, on Observations from the TOPOFF 2000 Exercise
- Ambassador Michael Sheehan, and Sam Brinkley, U.S. Department of State, on the U.S. International Strategy for Combating Terrorism

- Bruce Morris, Chief Deputy Secretary, Virginia Department of Public Safety, on the Meeting of the Advisory Committee for Assistance to State and Local Authorities
- The Honorable William Webster, former Director of the FBI, and former Director of Central Intelligence on Coordination of Terrorism Intelligence and Investigative Activities
- Jeffrey Hunker, NSC Director for Critical Infrastructure Protection; John Tritak, Critical Information Assurance Office (CIAO); Leslie Wiser, National Infrastructure Protection Center (NIPC); Captain Robert West, Joint Task Force-Computer Network Defense (US Space Command) (JTFCND); and Lee Zeichner, LegalNetWorks, on Providing Cyber Security and Defending Other Critical Infrastructure

At the March 2000 meeting, panel members determined that one-day meetings were insufficient for the amount of information that needed to be presented and adequate time to discuss the issues involved. As a result, starting with the July 2000 meeting, the panel now conducts two-day sessions.

Under the provisions of the Federal Advisory Committee Act, meetings of the panel are generally open to the public, except when national security classified information is being presented or discussed, or for one of the other exceptions stated in the Act. Notices of meetings are published in the Federal Register and posted on the panel's web page on the RAND web site: http://www.rand.org. Unclassified minutes of panel meetings are posted to the same web page as soon as the panel has approved them.

In addition to its regular meetings, panel members and support staff attended and participated directly in numerous conferences, workshops ands symposia on the subject of terrorism. In addition panel members and staff attended several Congressional hearings on terrorism. Panel Vice Chairman Jim Clapper presented testimony on the work of the panel before the Subcommittee on Investigations, Oversight, and Emergency Management, Committee on Transportation and Infrastructure, U.S. House of Representatives; and Project Director Michael Wermuth presented testimony on the work of the panel before the Subcommittee on National Security and Veteran's Affairs, Committee on Governmental Reform, U.S. House of Representatives.

Calendar Year 2001 Planned

Continuing Review and Analysis of Federal Programs

The panel, in conjunction with its supporting FFRDC, will continue its review and analysis of existing Federal programs that are designed, in whole or in part, to support or enhance domestic preparedness programs for terrorist incidents.

The review and analysis will place particular emphasis on those areas specifically mentioned in the enabling legislation: training, communications, equipment, planning

requirements, the needs of maritime regions, and coordination among the various levels of government.

The review and analysis of equipment issues will continue to focus on research, development, testing, and evaluation of equipment currently available, as well as emerging technologies, communications interoperability, and the development and timely dissemination of various categories of critical information between and among entities at the Federal, State, and local level.

Most significantly, the review and analysis with concentrate on several issues:

- Use of the military to respond domestically
- Policies and programs for dealing with the threat of cyber terrorism
- Health and medical issues
- Combating Terrorism fiscal strategies at the Federal, State and local levels

Survey of Local Responders and State Emergency Management and Response Organizations

During the coming months, the panel will complete its nationwide survey of State and local entities. The survey will be designed to elicit the views of those surveyed with respect to the efficacy of current Federal programs, particularly in the areas of training, equipment, planning, communications, and Federal agency coordination among the various levels of government. The survey will be conducted with a targeted survey audience that will include all geographic regions of the country, and in states and localities with a broad range of population densities.[161]

Interviews with Federal, State, and Local Officials

The panel members and support staff will continue to conduct interviews with selected senior and mid-level officials at the Federal, State, and local level—including, at the local level, law enforcement, fire services, emergency and other medical providers, public health personnel, and other emergency service officials. The purpose of the interviews will be to obtain more detailed information on programs and activities currently being conducted in certain jurisdictions, as well as specific proposals or recommendations that any of those persons interviewed may have to improve or enhance Federal efforts designed to strengthen local emergency responses to any such incident.

[161] For a complete description of the survey, see Appendix K.

APPENDIX P—Glossary of Terms

ACLU	American Civil Liberties Union
ACPR	Ariel Center for Policy Research, Tel Aviv
ATD	Anti-Terrorist Division, Los Angeles Police Department
BSD	Biosensor Systems Design, Inc.
BW	Biological Weapons
CB	Chemical and Biological
CBO	Civilian Behavior Officer
CBRN	Chemical, Biological, Radiological, and Nuclear
CBW	Chemical and Biological Weapons
CDC	Centers for Disease Control and Prevention
CEOC	County Emergency Operations Center
CERTCC	Computer Emergency Response Team Coordination Center, Carnegie Mellon University
CFR	Code of Federal Regulations
CIA	Central Intelligence Agency
CIAO	Critical Information Assurance Office, Department of Commerce
CIP	Critical Infrastructure Protection
CIPHER	Common Information for Public Health Electronic Reporting
CJS	Departments of Commerce, Justice, and State, and the Judiciary and Related Agencies Appropriations Act
CoMPIO	Consequence Management Program, Secretary of the Army
CONPLAN	U.S. Interagency Domestic Terrorism Concept of Operations Plan
COTS	Commercial Off-the-Shelf
CSEPP	Chemical Stockpile Emergency Preparedness Program, Department of the Army
CSTE	Council of State and Territorial Epidemiologists
CT	Counter-Terrorism
CTTS	Combating Terrorism Technical Support Program, Department of Defense
CW	Chemical Weapons
DCI	Director of Central Intelligence
DDOS	Distributed Denial of Service
DHHS	U.S. Department of Health and Human Services
DHS	Department of Health Services, Los Angeles County
DNC	Democratic National Convention
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOMS	Director of Military Support, U.S. Army
DPP	Domestic Preparedness Program, Department of Defense/Department of Justice
DTRA	Defense Threat Reduction Agency, Department of Defense
EMAC	Emergency Management Assistance Compact

EMS	Emergency Medical Service
EOB	Los Angeles County Sheriff's Department Emergency Operations Bureau
EOC	Federal Emergency Operations Center
EOS	Los Angeles Police Department Emergency Operations Section
EPA	Environmental Protection Agency
EPI-X	Epi-X, Centers for Disease Control and Prevention, Department of Health and Human Services
FBI	Federal Bureau of Investigation, Department of Justice
FCC	Federal Communications Commission
FDA	Food and Drug Administration, Department of Health and Human Services
FedCIRC	Federal Computer Incident Response Center, General Services Administration
FEMA	Federal Emergency Management Agency
FEST	Foreign Emergency Support Teams, Department of State
FIRM	First Responders Mask
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FRP	Federal Response Plan
FY	Fiscal Year
GAO	General Accounting Office
HAN	Health Alert Network (CDC)
HAZMAT	Hazardous Materials
HFC	Home Front Command, Israel Defense Forces
HHS	Department of Health and Human Services
HUMINT	Human Intelligence
IAB	Inter-Agency Board for Equipment Standardization and InterOperability
ICS	Incident Command System
ICT	International Policy Institute for Counter-Terrorism
IDF	Israel Defense Forces
ISAC	Information Sharing and Analysis Center
ISTS	Institute for Security Technology Studies, Dartmouth
IW	Information Warfare
JAMA	Journal of the American Medical Association
JIC	Joint Information Center
JOC	Joint Operation Center
JSIVA	Joint Staff Integrated Vulnerability Assessment Teams
JTFCND	Joint Task Force Command
JTF-CS	joint Task Force-Civil Support, U.S. Joint Forces Command
JTTF	Joint Terrorism Task Force, Federal Bureau of Investigation
LACoFD	Los Angeles County Fire Department
LAFD	Los Angeles City Fire Department
LAPD	Los Angeles Police Department
LASD	Los Angeles County Sheriff's Department
LAWA	Los Angeles World Airports
LAX	Los Angeles International Airport

LEO	Law Enforcement Online
LFA	Lead Federal Agency
MASINT	Measurement and Signature Intelligence
MDA	*Magen David Adom*, Israeli EMS
MIPT	Memorial Institute for Preventing Terrorism, Oklahoma City
MMRS	Metropolitan Medical Response System
MOD	Israel Ministry of Defense
MOE	Israel Ministry of the Environment
MOH	Israel Ministry of Health
MOU	Memorandum of Understanding
NAPHSIS	National Association for Public Health Statistics and Information Systems
NBC	Nuclear, Biological and Chemical
NDAA	National Defense Authorization Act
NDPO	National Domestic Preparedness Office, Federal Bureau of Investigation
NEMA	National Emergency Management Association
NGA	National Governors Association
NICI	National Interagency Civil-Military Institute
NIH	National Institutes of Health, Department of Health and Human Services
NIJ	National Institute of Justice, Office of Justice Programs, Department of Justice
NIO	National Intelligence Officer
NIOSH	National Institute for Occupational Safety and Health, Department of Health and Human Services
NIPC	National Infrastructure Protection Center, Federal Bureau of Investigation,
NIST	National Institute for Standards and Technology, Department of Commerce
NLD	Nunn-Lugar-Domenici Act
NMRT	National Medical Response Team
NSC	National Security Council
NTS	Nevada Test Site
OEM	Los Angeles County Office of Emergency Management
OIC	Officer in Charge
OIPR	Office of Intelligence Policy and Review, Department of Justice
OJP	Office of Justice Programs, Department of Justice
OMB	Office of Management and Budget
ONDCP	Office of National Drug Control Policy
OSD	Office of the Secretary of Defense, Department of Defense
OSHA	Occupational Safety and Health Administration, Department of Health and Human Services
OSINT	Open source intelligence
OSLDPS	Office for State and Local Domestic Preparedness Support, Office of Justice Programs
OSTP	Office of Science and Technology Policy
PCCIP	President's Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive

PPE	Personal Protective Equipment
PUB L	Public Law
R&D	Research and Development
RAID	Rapid Assessment Initial Detection teams
RDT&E	Research, Development, Test and Evaluation
RFW	Radio Frequency Weapons
RRIS	Rapid Response Information System, Department of the Army
SDN	Secure Date Network (CDC)
SEMS	Standardized Emergency Management System
SIS	Los Angeles County Sheriff's Special Investigations Section
SO/LIC	Special Operations/Low Intensity Conflict, Department of Defense
TEWG	Terrorism Early Warning Group, Los Angeles Operational Area
TSWG	Technical Support Working Group
TWG	Terrorism Working Group, Los Angeles Operational Area
UCS	Unified Command System
USAMRIID	U.S. Army Medical Research Institute of Infectious Diseases
WHO	World Health Organization
WMD	Weapons of Mass Destruction

APPENDIX Q—WORKING DEFINITIONS

"Weapons of Mass Destruction"

For reasons of clarity and precision, the report uses the term CBRN (chemical, biological, radiological, and nuclear) terrorism, in preference to the more commonly used, yet potentially misleading term, "weapons of mass destruction" or WMD, to describe the unconventional types of weapons that terrorists may use. As recognized in at least one Federal statute, moreover, even small amounts of conventional explosives could potentially have "mass destructive" effects.[162] Indeed, few Americans would likely conclude that the device used in the attack by Timothy McVeigh and his cohorts on the Murrah Federal Building in Oklahoma City was anything other than a "weapon of mass destruction," despite the more limited definition in the Nunn-Lugar-Domenici Act. It is intended that the term CBRN within the construct of this report include, as an example, potential terrorist attacks on industrial chemical facilities that do not necessarily involve an actual CBRN weapon, where the purpose is to engineer the hazardous release of a toxic gas or other substance intended to kill and injure surrounding populations.

"Mass Casualties"

With the exception of nuclear weapons, none of the unconventional weapons by itself is, in fact, capable of wreaking mass destruction, at least not in structural terms. Indeed, the terminology "weapons of mass casualties" may be a more accurate depiction of the potentially lethal power that could be unleashed by chemical, biological, or nonexplosive radiological weapons. The distinction is more than rhetorical and is critical to understanding the vastly different levels of technological skills and capabilities, weapons expertise, production requirements, and dissemination or delivery methods needed to

[162]The NLD (Nunn-Lugar-Domenici) Act defines a "weapon 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, (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."

undertake an effective attack using either chemical or biological weapons in particular.[163] Nevertheless, there continues to be no universally accepted definition of "mass casualties." The panel has, instead, chosen to describe casualties in a range:

Terrorist acts of that fall into the category of "higher probability" (e.g., with the use of conventional high explosives) will produce casualties of "lower consequences" in the dozens, compared to a "lower probability" attack (the mass release of an infectious biologic), that can cause "higher consequence" casualties in the thousands or tens of thousands.

Terrorism

There continues to be no universally accepted definition of terrorism. The definition of terrorism employed in this report, and used as the framework for its first report and the Panel's deliberations to date, is essentially one used by RAND for more than a quarter of a century:

Terrorism is violence, or the threat of violence, calculated to create an atmosphere of fear and alarm, through acts designed to coerce others into actions they otherwise would not undertake or into refraining from actions that they desired to take. All terrorist acts are crimes. Many would also be violations of the rules of war, if a state of war existed. This violence or threat of violence is generally directed against civilian targets. The motives of all terrorists are political, and terrorist actions are generally carried out in a way that will achieve maximum publicity. The perpetrators are usually members of an organized group, although increasingly lone actors or individuals who may have separated from a group can have both the motivation and potentially the capability to perpetrate a terrorist attack. Unlike other criminals, terrorists often claim credit for their acts. Finally, terrorist acts are intended to produce effects beyond the immediate physical damage that they cause.[164]

Terrorist Group

For the purposes of this report, a terrorist group is defined as a collection of individuals belonging to an autonomous nonstate or subnational revolutionary or antigovernment movement who are dedicated to the use of violence to achieve their objectives. Such an entity is seen as having at least some structure and command and control apparatus that, no matter how loose or flexible, nonetheless provides an overall organizational

[163]Although biological agents "are often described as 'weapons of mass destruction,' it does not follow that the ability to inflict mass casualties is an intrinsic property. Key variables in determining the impact of a [biological] terrorist attack are the quantity of agent employed and the means of dissemination." See Jonathan B. Tucker and Amy Sands, "An Unlikely Threat," *Bulletin of the Atomic Scientists*, Vol. 55, No. 4 (July/August 1999), which can be accessed at: http://www.bullatomsci.org/issues/1999/ja99/ja99tucker.html

[164]From Karen Gardela and Bruce Hoffman, *The RAND Chronology of International Terrorism for 1986* (Santa Monica, Calif.: RAND, R-3890-RC, 1990), p. 1 (with slight modifications), which in turn is taken from Brian Michael Jenkins, *International Terrorism: A New Kind of Warfare* (Santa Monica, Calif.: RAND , P-5261, 1974).

framework and general strategic direction. This definition is meant to include contemporary religion-motivated and apocalyptic groups, and other movements that seek theological justification or divine sanction for their acts of violence.

State-Sponsored Terrorism

State-sponsored terrorism is defined here as the active involvement of a foreign government in training, arming, and providing other logistical and intelligence assistance as well as sanctuary to an otherwise autonomous terrorist group for the purpose of carrying out violent acts on behalf of that government against its enemies. State-sponsored terrorism is, therefore, regarded as a form of surrogate warfare.

APPENDIX R—CONSTITUTIONAL AND LEGAL AUTHORITIES FOR THE USE OF THE MILITARY DOMESTICALLY

There are several constitutional bases for the use of the military domestically in support of civil authorities. Article One gives Congress the power to create military forces, and provide for their regulation, and contains explicit language for "calling forth the militia" to enforce laws, and suppress rebellions and insurrections.[165]

Article Two designates the President as commander in chief not only of regular Federal forces, but also of the state militias, when in Federal service—"militia" in each of these cases being what we now know as the National Guard of the various States.[166]

Article Four says that the United States shall protect each of the states not only against invasion, but also against "domestic violence." Note the use of the word of the obligatory "shall" and not the permissive "may."[167]

In the first century of the Republic, there were a number of instances in which the military was used to enforce laws, which gave rise to some criticism of those activities, most particularly, military actions in the reconstruction and post-reconstruction periods in the South. It was the latter circumstances that caused Congress, in June of 1878, to pass what has come to be called the "Posse Comitatus Act."[168] Posse Comitatus translated from Latin means "the power or force of the county."[169]

The Congress did not proscribe the use of the military in Title 10—the code title for military activities generally—as a "posse comitatus," or otherwise as a means of enforcing the laws, it made it a crime under Title 18 to do so. Moreover, the statute does not refer to the laws "of the United States," it refers to "the laws" generally, which can include the laws of the various States.

---

[165] "ARTICLE I, Section 8. The Congress shall have power. . .;
"To raise and support Armies . . .;
"To provide and maintain a Navy;
"To make rules for the Government and Regulation of the land and naval Forces;
"To provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions; . . . ."

[166] **"**ARTICLE II, Section 2. The President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual Service of the United States . . . ."

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

[168] "18 U. S. Code, Section 1385 — Use of Army and Air Force as a posse comitatus. Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both."

[169] *Black's Law Dictionary*, West Publishing Company, St. Paul, MN, citing case references. See also *The American Heritage Dictionary*, Second College Edition, special print for the Virginia Polytechnic Institute and State University, Houghton Mifflin Company, Boston, 1985.

But the Congress created an exception for those cases authorized in the Constitution or other Acts of Congress. As noted above, there is at least one specific and preexisting Constitutional mandate.

In the years following the enactment of the Posse Comitatus Act, the Congress has created a number of statutory exceptions to that Act, which fall into four major categories:

- Insurrections/Civil Disturbances
- Counterdrug Operations
- Disaster Relief
- Counter-terrorism/Weapons of Mass Destruction

There are also a number of "minor" exceptions, covering a wide range of activities.[170]

In 1956, Congress created broad authority for use of the military to suppress insurrections, rebellions, and unlawful combinations and conspiracies in the various states – an extension of the Constitutional mandate to protect the states against domestic violence.[171]

Beginning in 1981, and as amended in the intervening years, Congress has created a number of authorized activities for use of the military in counterdrug operations, both inside the United States, and extraterritorially.[172] Those activities include intelligence and information sharing; the use of military equipment and facilities; training and advice to law enforcement agencies; the maintenance and operations of a vast array of equipment—owned at the Federal, state and local level. There is also specific authority in these provisions for air, sea, and ground detection and monitoring of the illegal transit of drugs into the United States—which includes some authority for "hot pursuit" inside U.S. borders, as well as some interception authority for vessels and aircraft detected outside of our borders for purposes of identifying and communicating with the vessel or aircraft, and directing them to a location specified by civilian law enforcement. That authority also includes the transportation of domestic and foreign law enforcement and military personnel engaged in counterdrug operations; the operation of bases of operation inside the u.s. and extraterritorially; aerial and ground reconnaissance—but not surveillance—operations inside and outside the U.S.; and the implementation of procedures for civilian law enforcement agencies to procure certain military equipment for counterdrug activities.

The military, as has been the case a number of times in recent years, may also be used for disaster relief operations, both domestically, pursuant to provisions of the Stafford Act in Title 42;[173] and internationally, under the provisions of section 404 of Title 10.

---

[170] See list attached at Tab 1.
[171] 10 U.S. Code, Section 331, et seq.
[172] !0 U.S. Code, Section 124, and Sections 371, et seq.
[173] 42 USC 5121, et seq.

In 1988, Congress added to this series of provisions the authority to operate equipment in the conduct of counter-terrorism operations both foreign and domestically, including transporting suspected terrorists to the U.S. for trial.[174]

Most significantly in the specific terrorism context, Congress has also provided the authority to assist in biological and chemical incident responses, which may, under certain exceptional circumstances, include direct involvement in arrests, searches, seizures, and the collection of specific intelligence;[175] and authority in Title 18, to provide assistance in nuclear terrorism cases, which may also include participation in arrest, search and seizure activities.[176]

Some of the specific authority, and the conduct of activities pursuant to that authority, have not of course been without their detractors. From both within and outside of military circles, there have been concerns about the use of the military in this fashion, as being outside of the scope of normal military operations. And military leaders have often expressed concern about the effect of such activities on military preparedness for war and other contingencies.

Some in Congress and elsewhere also express concern that, in times of reduced force structure and other limitations on defense spending, the military should focus on preparing for and participating in purely military operations.

Others raise the specter of the military engaging in widespread violations of civil rights. As examples, in connection with anti-terrorism legislation in 1995, a group of law professors suggested that soldiers had no grounding in the Constitution, and knew nothing about minimum force; and the ACLU and others made vague reference to Constitutional issues, citing the Posse Comitatus Act (which is not, of course, a Constitutional protection).

There are, however, a number of protections against abuse that are built directly into some of the statutes and contained in a number of Federal regulations and policy documents. In several statutes, there are conditions precedent, which must occur or exist, for the use of the military. Examples include:

- A Presidential Declaration of Disaster for support under the Stafford Act[177]
- A proclamation to persons engaged in civil disorders to disperse and retire, contained in the Insurrections Statutes[178]

---

[174] 10 U.S. Code, Section 374. See statutory text at Tab 2.
[175] 10 U.S. Code, Section 382. See statutory text at Tab 3.
[176] 18 U.S. Code, Section 831. See statutory text at Tab 4.
[177] See 42 U.S. Code, Section 5170, 5170b, and 5191.
[178] 10 U.S. Code, Section 374. There have been nine times that such proclamations have been issued, primarily for integration of schools in the South and for the various riots in major U.S. cities in the1960s:
- Arkansas, 1957 (Little Rock public schools)
- Mississippi, 1962 (Mississippi public schools)
- Alabama, 1963 (University of Alabama)
- Alabama, 1963 (Alabama public schools)

- A specific order from the President in cases of suppressing insurrections and other civil disobedience;[179] for foreign disaster relief; and in the case of many of the "minor" statutes that are listed in Tab1
- Either a specific request from a State governor or legislature for assistance to suppress an insurrection,[180]or a determination that others have refused, failed, or are not capable of enforcing the laws to suppress insurrection and other civil disorder[181]

In a number of cases, senior Federal officials must request or approve, either individually or jointly with others, the use of military support:

- For several activities in the counterdrug arena, a specific support request must come from the head of a Federal law enforcement agency—the Drug Enforcement Administration, U.S. Customs Service, U.S Coast Guard, U.S. Marshals, U.S. Border Patrol, Federal Bureau of Investigation—even if the support is ultimately intended for a State or local government.[182]
- The Secretary of Defense and the Attorney General (and for foreign operations, the Secretary of State as well) must approve the transportation of law enforcement and military personnel, and the operation of bases of operation for counterdrug activities.[183]
- For response to biological, chemical, and nuclear terrorist incidents, as well as for many of the minor statutes, the Secretary of Defense and the Attorney General must approve the specific activity.[184]

There are also numerous statutory, regulatory, and other policy limitations on military activities in support of civil authorities:

- There are provisions in several sections that require a determination that the activity will not have an adverse impact on military preparedness.[185]
- Several sections also require reimbursement from the supported agency under provisions of the Economy Act, although there is an exception where the activity is conducted in the course of training or provides equivalent training.[186]
- Although the Legal Counsel at the Department of Justice at one point opined that many of these statutes do not, unless stated explicitly, apply outside of the border of the United States, the Department of Defense has consistently done so, and the key

---

- Alabama, 1965 (Selma to Montgomery march)
- Michigan, 1967 (Detroit riot)
- Washington, DC, 1968 (DC riot)
- Illinois, 1968 (Chicago riot)
- Maryland, 1968 (Baltimore riot)

[179] 10 U.S. Code, Sections 331 and 334.
[180] 10 U.S. Code, Section 331.
[181] 10 U.S. Code, Section 334.
[182] 10 U.S. Code, Section 374.
[183] 10 U.S. Code, Section 374.
[184] 10 U.S. Code, Section 382, and 18 U.S. Code, Section 831.
[185] E.g., 10 U.S. Code, Sections 376 and 382; and 18 U.S. Code, Section 831.
[186] See 10 U.S. Code, Sections 374 and 381.

DoD Directive for such support states that exceptions to such extraterritorial application will be considered on a case-by-case basis, and then only in "compelling and extraordinary circumstances."[187]

- There is an overarching provision in the counterdrug statutes that prohibits military involvement in search, seizure, arrest or similar activity[188] (but *cf* 10 U.S. Code, Section 382, and 18 U.S. Code, Section 831).
- Although the specific provisions of the Posse Comitatus Act do not apply to the U.S. Navy and the U.S. Marines, they have been included in the provisions of the counterdrug statute that prevents direct involvement in law enforcement; the Navy and Marines are also covered under Posse Comitatus Act provisions by regulation;[189] and other provisions require the presence on naval vessels of U.S. Coast Guard law enforcement personnel during counterdrug operations.[190]
- The DoD Directive covering "military assistance to civil authorities" requires that each such request be evaluated against the six criteria, most of which are a regulatory expression of statutory requirements, as are many other provisions in regulatory and policy guidance.[191]

The rulings and interpretations of the Federal courts, in construing the specific statutory language and the legal implications of domestic activities conducted by the military, are relatively few and they have been remarkably consistent. Two are notable:

In *Laird v. Tatum*,[192] the U.S. Supreme Court very succinctly noted that the Constitutionality of the Insurrection Statutes was not an issue; nor was the Posse Comitatus Act a limiting factor. In *Gilligan*, the Supreme Court noted both Constitutional and Federal statutory authority for the use of the National Guard for executing the Insurrection Statutes (although the Guard was actually not Federalized at Kent State).[193]

While the terrorism-specific statutes have not been tested in Federal court, there is no reason to believe that courts would find a Constitutional deficiency in them.

---

[187] DoD Directive 5525.5.
[188] 10 U.S. Code, Section 375.
[189] 10 U.S. Code, Section 375; 32 CFR 213.2.
[190] 10 U.S. Code, Section 379.
[191] Legality (compliance with laws); lethality (potential use of lethal force by or against DoD forces); risk (safety of DoD forces); cost (who pays, impact on DoD budget); appropriateness (whether the requested mission is in the interest of the Department to conduct); and readiness (impact on the DoD's ability to perform its primary mission). DoD Directive 3025.15.
[192] *Laird v. Tatum*, 408 U.S. 1 (1971) (1967 Detroit riots), ruling on 10 U.S. Code, Section 333, citing Art. IV, Sec. 4 of the Constitution.
[193] *Gilligan v. Morgan*, 413 U.S. 1(1972) (1970 Kent State shootings), citing Congressional authority under Art. I, Sec. 8, and Presidential authority under the Constitution, and the use of the National Guard [10 U.S. Code, Section 331, et seq.] to assist in controlling civil disorders.

TAB 1 TO APPENDIX R—MINOR STATUTES AUTHORIZING MILITARY SUPPORT

- Protect national parks, other Federal lands (16 USC23, 78, and 593)
- Assist in case of crimes against members of Congress (18 USC 351)
- Protect the President, Vice President, other dignitaries (18 USC 1751)
- Enforce the Fishery Conservation and Management Act (16 USC 1861)
- Support the neutrality laws (22 USC 408 and 461-462)
- Execute quarantine and certain health laws (42 USC 97)
- Support certain customs laws (50 USC 220)
- Remove persons unlawfully present on Indian lands (25 USC 180)
- Execute warrants for enforcement of civil rights laws (42 USC 1989)
- Remove unlawful inclosures from public lands (43 USC 1065)
- Protect the rights of a discoverer of a guano island (48 USC 1418)
- Support territorial governors in civil disorders (48 USC 1422 and 1591)
- Assist in case of crimes against foreign officials, official guests, other internationally protected persons (18 USC 112 and 1116)

TAB 2 TO APPENDIX R—TITLE 10, U.S. CODE, SECTION 374

TITLE 10 - ARMED FORCES
Subtitle A - General Military Law
PART I - ORGANIZATION AND GENERAL MILITARY POWERS
CHAPTER 18 - MILITARY SUPPORT FOR CIVILIAN LAW ENFORCEMENT AGENCIES

Sec. 374. Maintenance and operation of equipment

(a) The Secretary of Defense may, in accordance with other applicable law, make Department of Defense personnel available for the maintenance of equipment for Federal, State, and local civilian law enforcement officials, including equipment made available under section 372 of this title.

(b)(1) Subject to paragraph (2) and in accordance with other applicable law, the Secretary of Defense may, upon request from the head of a Federal law enforcement agency, make Department of Defense personnel available to operate equipment (including equipment made available under section 372 of this title) with respect to -

(A) a criminal violation of a provision of law specified in paragraph (4)(A);

(B) assistance that such agency is authorized to furnish to a State, local, or foreign government which is involved in the enforcement of similar laws;

(C) a foreign or domestic counter-terrorism operation; or

(D) a rendition of a suspected terrorist from a foreign country to the United States to stand trial.

(2) Department of Defense personnel made available to a civilian law enforcement agency under this subsection may operate equipment for the following purposes:

(A) Detection, monitoring, and communication of the movement of air and sea traffic.

(B) Detection, monitoring, and communication of the movement of surface traffic outside of the geographic boundary of the United States and within the United States not to exceed 25 miles of the boundary if the initial detection occurred outside of the boundary.

(C) Aerial reconnaissance.

(D) Interception of vessels or aircraft detected outside the land area of the United States for the purposes of communicating with such vessels and aircraft to direct such vessels and aircraft to go to a location designated by appropriate civilian officials.

(E) Operation of equipment to facilitate communications in connection with law enforcement programs specified in paragraph (4)(A).

(F) Subject to joint approval by the Secretary of Defense and the Attorney General (and the Secretary of State in the case of a law enforcement operation outside of the land area of the United States) -

(i) the transportation of civilian law enforcement personnel along with any other civilian or military personnel who are supporting, or conducting, a joint operation with civilian law enforcement personnel;

(ii) the operation of a base of operations for civilian law enforcement and supporting personnel; and

(iii) the transportation of suspected terrorists from foreign countries to the United States for trial (so long as the requesting Federal law enforcement agency provides all security for such transportation and maintains custody over the suspect through the duration of the transportation).

(3) Department of Defense personnel made available to operate equipment for the purpose stated in paragraph (2)(D) may continue to operate such equipment into the land area of the United States in cases involving the pursuit of vessels or aircraft where the detection began outside such land area.

(4) In this subsection:

(A) The term "Federal law enforcement agency" means a Federal agency with jurisdiction to enforce any of the following:

(i) The Controlled Substances Act (21 U.S.C. 801 et seq.) or the Controlled Substances Import and Export Act (21 U.S.C. 951 et seq.).

(ii) Any of sections 274 through 278 of the Immigration and Nationality Act (8 U.S.C. 1324-1328).

(iii) A law relating to the arrival or departure of merchandise (as defined in section 401 of the Tariff Act of 1930 (19 U.S.C. 1401) into or out of the customs territory of the United States (as defined in general note 2 of the Harmonized Tariff Schedule of the United States) or any other territory or possession of the United States.

(iv) The Maritime Drug Law Enforcement Act (46 U.S.C. App. 1901 et seq.).

(v) Any law, foreign or domestic, prohibiting terrorist activities.

(B) The term "land area of the United States" includes the land area of any territory, commonwealth, or possession of the United States.

(c) The Secretary of Defense may, in accordance with other applicable law, make Department of Defense personnel available to any Federal, State, or local civilian law enforcement agency to operate equipment for purposes other than described in subsection (b)(2) only to the extent that such support does not involve direct participation by such personnel in a civilian law enforcement operation unless such direct participation is otherwise authorized by law.

(Added Pub. L. 97-86, title IX, Sec. 905(a)(1), Dec. 1, 1981, 95 Stat. 1115; amended Pub. L. 98-525, title XIV, Sec. 1405(9), Oct. 19, 1984, 98 Stat. 2622; Pub. L. 99-570, title III, Sec. 3056, Oct. 27, 1986, 100 Stat. 3207-77; Pub. L. 99-661, div. A, title XIII, Sec. 1373(c), Nov. 14, 1986, 100 Stat. 4007; Pub. L. 100-418, title I, Sec. 1214(a)(1), Aug. 23, 1988, 102 Stat. 1155; Pub. L. 100-456, div. A, title XI, Sec. 1104(a), Sept. 29, 1988, 102 Stat. 2043; Pub. L. 101-189, div. A, title XII, Sec. 1210, 1216(b), (c), Nov. 29, 1989, 103 Stat. 1566, 1569; Pub. L. 102-484, div. A, title X, Sec. 1042, Oct. 23, 1992, 106 Stat. 2492; Pub. L. 105-277, div. B, title II, Sec. 201, Oct. 21, 1998, 112 Stat. 2681-567; Pub. L. 106-65, div. A, title X, Sec. 1066(a)(4), Oct. 5, 1999, 113 Stat. 770.)

TAB 3 TO APPENDIX R—TITLE 10, U.S. CODE, SECTION 382

TITLE 10--ARMED FORCES
Subtitle A--General Military Law
PART I--ORGANIZATION AND GENERAL MILITARY POWERS
CHAPTER 18--MILITARY SUPPORT FOR CIVILIAN LAW ENFORCEMENT AGENCIES

Sec. 382. Emergency situations involving chemical or biological weapons of mass destruction

(a) In General.--The Secretary of Defense, upon the request of the Attorney General, may provide assistance in support of Department of Justice activities relating to the enforcement of section 175 or 2332c of title 18 during an emergency situation involving a biological or chemical weapon of mass destruction. Department of Defense resources, including personnel of the Department of Defense, may be used to provide such assistance if--

(1) the Secretary of Defense and the Attorney General jointly determine that an emergency situation exists; and

(2) the Secretary of Defense determines that the provision of such assistance will not adversely affect the military preparedness of the United States.

(b) Emergency Situations Covered.--In this section, the term ``emergency situation involving a biological or chemical weapon of mass destruction'' means a circumstance involving a biological or chemical weapon of mass destruction--

(1) that poses a serious threat to the interests of the United States; and

(2) in which--

(A) civilian expertise and capabilities are not readily available to provide the required assistance to counter the threat immediately posed by the weapon involved;

(B) special capabilities and expertise of the Department of Defense are necessary and critical to counter the threat posed by the weapon involved; and

(C) enforcement of section 175 or 2332c of title 18 would be seriously impaired if the Department of Defense assistance were not provided.

(c) Forms of Assistance.--The assistance referred to in subsection (a) includes the operation of equipment (including equipment made available under section 372 of this title) to monitor, contain, disable, or dispose of the weapon involved or elements of the weapon.

(d) Regulations.--(1) The Secretary of Defense and the Attorney General shall jointly prescribe regulations concerning the types of assistance that may be provided under this section. Such regulations shall also describe the actions that Department of Defense personnel may take in circumstances incident to the provision of assistance under this section.

(2)(A) Except as provided in subparagraph (B), the regulations may not authorize the following actions:

(i) Arrest.

(ii) Any direct participation in conducting a search for or seizure of evidence related to a violation of section 175 or 2332c of title 18.

(iii) Any direct participation in the collection of intelligence for law enforcement purposes.

(B) The regulations may authorize an action described in subparagraph (A) to be taken under the following conditions:

(i) The action is considered necessary for the immediate protection of human life, and civilian law enforcement officials are not capable of taking the action.

(ii) The action is otherwise authorized under subsection (c) or under otherwise applicable law.

(e) Reimbursements.--The Secretary of Defense shall require reimbursement as a condition for providing assistance under this section to the extent required under section 377 of this title.

(f) Delegations of Authority.--(1) Except to the extent otherwise provided by the Secretary of Defense, the Deputy Secretary of Defense may exercise the authority of the Secretary of Defense under this section. The Secretary of Defense may delegate the Secretary's authority under this section only to an Under Secretary of Defense or an Assistant Secretary of Defense and only if the Under Secretary or Assistant Secretary to whom delegated has been designated by the Secretary to act for, and to exercise the general powers of, the Secretary.

(2) Except to the extent otherwise provided by the Attorney General, the Deputy Attorney General may exercise the authority of the Attorney General under this section. The Attorney General may delegate that authority only to the Associate Attorney General or an Assistant Attorney General and only if the Associate Attorney General or Assistant Attorney General to whom delegated has been designated by the Attorney General to act for, and to exercise the general powers of, the Attorney General.

(g) Relationship to Other Authority.--Nothing in this section shall be construed to restrict any executive branch authority regarding use of members of the armed forces or equipment of the Department of Defense that was in effect before September 23, 1996.

(Added Pub. L. 104-201, div. A, title XIV, Sec. 1416(a)(1), Sept. 23, 1996, 110 Stat. 2721; amended Pub. L. 105-85, div. A, title X, Sec. 1073(a)(6), Nov. 18, 1997, 111 Stat. 1900.)

TAB 4 TO APPENDIX R—TITLE 18, U.S. CODE, SECTION 831

TITLE 18--CRIMES AND CRIMINAL PROCEDURE
PART I--CRIMES
CHAPTER 39--EXPLOSIVES AND OTHER DANGEROUS ARTICLES

Sec. 831. Prohibited transactions involving nuclear materials

(a) Whoever, if one of the circumstances described in subsection (c) of this section occurs-

(1) without lawful authority, intentionally receives, possesses, uses, transfers, alters, disposes of, or disperses any nuclear material and--

(A) thereby knowingly causes the death of or serious bodily injury to any person or substantial damage to property; or

(B) knows that circumstances exist which are likely to cause the death of or serious bodily injury to any person or substantial damage to property;

(2) with intent to deprive another of nuclear material, knowingly--

(A) takes and carries away nuclear material of another without authority;

(B) makes an unauthorized use, disposition, or transfer, of nuclear material belonging to another; or

(C) uses fraud and thereby obtains nuclear material belonging to another;

(3) knowingly--

(A) uses force; or

(B) threatens or places another in fear that any person other than the actor will imminently be subject to bodily injury;

and thereby takes nuclear material belonging to another from the person or presence of any other;

(4) intentionally intimidates any person and thereby obtains nuclear material belonging to another;

(5) with intent to compel any person, international organization, or governmental entity to do or refrain from doing any act, knowingly threatens to engage in conduct described in paragraph (2)(A) or (3) of this subsection;

(6) knowingly threatens to use nuclear material to cause death or serious bodily injury to any person or substantial damage to property under circumstances in which the threat may reasonably be understood as an expression of serious purposes;

(7) attempts to commit an offense under paragraph (1), (2), (3), or (4) of this subsection; or

(8) is a party to a conspiracy of two or more persons to commit an offense under paragraph (1), (2), (3), or (4) of this subsection, if any of the parties intentionally engages in any conduct in furtherance of such offense;

shall be punished as provided in subsection (b) of this section.

(b) The punishment for an offense under--

(1) paragraphs (1) through (7) of subsection (a) of this section is--

(A) a fine under this title; and

(B) imprisonment--

(i) for any term of years or for life (I) if, while committing the offense, the offender knowingly causes the death of any person; or (II) if, while committing an offense under paragraph (1) or (3) of subsection (a) of this section, the offender, under circumstances manifesting extreme indifference to the life of an individual, knowingly engages in any conduct and thereby recklessly causes the death of or serious bodily injury to any person; and

(ii) for not more than 20 years in any other case; and

(2) paragraph (8) of subsection (a) of this section is--
(A) a fine under this title; and
(B) imprisonment--
(i) for not more than 20 years if the offense which is the object of the conspiracy is punishable under paragraph (1)(B)(i); and
(ii) for not more than 10 years in any other case.

(c) The circumstances referred to in subsection (a) of this section are that--
(1) the offense is committed in the United States or the special maritime and territorial jurisdiction of the United States, or the special aircraft jurisdiction of the United States (as defined in section 46501 of title 49);
(2) the defendant is a national of the United States, as defined in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101);
(3) at the time of the offense the nuclear material is in use, storage, or transport, for peaceful purposes, and after the conduct required for the offense occurs the defendant is found in the United States, even if the conduct required for the offense occurs outside the United States; or
(4) the conduct required for the offense occurs with respect to the carriage of a consignment of nuclear material for peaceful purposes by any means of transportation intended to go beyond the territory of the state where the shipment originates beginning with the departure from a facility of the shipper in that state and ending with the arrival at a facility of the receiver within the state of ultimate destination and either of such states is the United States.

(d) The Attorney General may request assistance from the Secretary of Defense under chapter 18 of title 10 in the enforcement of this section and the Secretary of Defense may provide such assistance in accordance with chapter 18 of title 10, except that the Secretary of Defense may provide such assistance through any Department of Defense personnel.
(e)(1) The Attorney General may also request assistance from the Secretary of Defense under this subsection in the enforcement of this section. Notwithstanding section 1385 of this title, the Secretary of Defense may, in accordance with other applicable law, provide such assistance to the Attorney General if--
(A) an emergency situation exists (as jointly determined by the Attorney General and the Secretary of Defense in their discretion); and
(B) the provision of such assistance will not adversely affect the military preparedness of the United States (as determined by the Secretary of Defense in such Secretary's discretion).

(2) As used in this subsection, the term ``emergency situation'' means a circumstance--
(A) that poses a serious threat to the interests of the United States; and
(B) in which--
(i) enforcement of the law would be seriously impaired if the assistance were not provided; and
(ii) civilian law enforcement personnel are not capable of enforcing the law.

(3) Assistance under this section may include--
(A) use of personnel of the Department of Defense to arrest persons and conduct searches and seizures with respect to violations of this section; and
(B) such other activity as is incidental to the enforcement of this section, or to the protection of persons or property from conduct that violates this section.

(4) The Secretary of Defense may require reimbursement as a condition of assistance under this section.

(5) The Attorney General may delegate the Attorney General's function under this subsection only to a Deputy, Associate, or Assistant Attorney General.

(f) As used in this section--

(1) the term ``nuclear material'' means material containing any--

(A) plutonium with an isotopic concentration not in excess of 80 percent plutonium 238;

(B) uranium not in the form of ore or ore residue that contains the mixture of isotopes as occurring in nature;

(C) uranium that contains the isotope 233 or 235 or both in such amount that the abundance ratio of the sum of those isotopes to the isotope 238 is greater than the ratio of the isotope 235 to the isotope 238 occurring in nature; or

(D) uranium 233;

(2) the term ``international organization'' means a public international organization designated as such pursuant to section 1 of the International Organizations Immunities Act (22 U.S.C. 288) or a public organization created pursuant to treaty or other agreement under international law as an instrument through or by which two or more foreign governments engage in some aspect of their conduct of international affairs;

(3) the term ``serious bodily injury'' means bodily injury which involves--

(A) a substantial risk of death;

(B) extreme physical pain;

(C) protracted and obvious disfigurement; or

(D) protracted loss or impairment of the function of a bodily member, organ, or mental faculty; and

(4) the term ``bodily injury'' means--

(A) a cut, abrasion, bruise, burn, or disfigurement;

(B) physical pain;

(C) illness;

(D) impairment of a function of a bodily member, organ, or mental faculty; or

(E) any other injury to the body, no matter how temporary.

(Added Pub. L. 97-351, Sec. 2(a), Oct. 18, 1982, 96 Stat. 1663; amended Pub. L. 100-690, title VII, Sec. 7022, Nov. 18, 1988, 102 Stat. 4397; Pub. L. 103-272, Sec. 5(e)(6), July 5, 1994, 108 Stat. 1374; Pub. L. 103-322, title XXXIII, Sec. 330016(2)(C), Sept. 13, 1994, 108 Stat. 2148.)

APPENDIX S—Interagency Comments

Copies of the report were provided to the Federal Interagency on December 13, 2000, for review and comments. The agencies have until January 12, 2000, to provide comments. Subsequent to that date, the Advisory Panel will submit to the President and the Congress a supplement to this report containing agency comments and Advisory Panel responses.

APPENDIX T—Transmittal Letters

Attached are facsimiles of the letters transmitting the report.

A copy of the report under similar covering letter was delivered to each of the following:

The President

The President-Elect

The Honorable J. Dennis Hastert
Speaker of the House

The Honorable Al Gore, Jr.
President of the Senate

The Honorable Strom Thurmond
President Pro Tempore
United States Senate

The Honorable Richard K. Armey
Majority Leader
U.S. House of Representatives

The Honorable Richard A. Gephardt
Minority Leader
U.S. House of Representatives

The Honorable Trent Lott
Majority Leader
United States Senate

The Honorable Thomas Daschle
Minority Leader
United States Senate

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

December 14, 2000

The President
The White House
Washington, DC 20500

Dear Mr. President:

On behalf of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, it is my pleasure to submit to the Congress the second of three annual reports of the advisory panel. The advisory panel is authorized and the annual reports are required by Section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105-261 (H.R. 3616, 105th Congress, 2nd Session) (October 17, 1998).

The report provides several policy recommendations for consideration by the President and the Congress, including matters involving the development of a national strategy for combating terrorism, Federal coordinating structure, improvements in Congressional coordination, and specific functional areas.

The report is being simultaneously provided to the Federal Interagency for comment. After comments are received, the advisory panel will submit a supplement to this report, forwarding the comments and any responses to them that we may have.

Very respectfully,

/s/

James S. Gilmore, III
Chairman

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

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

December 14, 2000

The Honorable J. Dennis Hastert
Speaker of the House
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Speaker:

On behalf of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, it is my pleasure to submit to you the second of three annual reports of the advisory panel. The advisory panel is authorized and the annual reports are required by Section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105-261 (H.R. 3616, 105th Congress, 2nd Session) (October 17, 1998).

The report provides several policy recommendations for consideration by the President and the Congress, including matters involving the development of a national strategy for combating terrorism, Federal coordinating structure, improvements in Congressional coordination, and specific functional areas.

The report is being simultaneously provided to the Federal Interagency for comment. After comments are received, the advisory panel will submit a supplement to this report, forwarding the comments and any responses to them that we may have.

Very respectfully,

/s/

James S. Gilmore, III
Chairman

Please address comments or questions to:

RAND
1200 South Hayes Street, Arlington, Virginia 22202-5050 Telephone: 703-413-1100 FAX: 703-413-8111

The Federally-Funded Research and Development Center providing support to the Advisory Panel

APPENDIX U—RAND STAFF PROVIDING SUPPORT TO THE ADVISORY PANEL

Project Director

Michael Wermuth

Research Staff for the Report

Janice Blanchard
David Brannan
Jennifer Brower
Peter Chalk
Kim Cragin
Lois Davis
Paul Davis
Margaret Harrell
Marvin Heinze
Bruce Hoffman
Brian Houghton
Gerald Jacobsen
Sarah Cotton Nelson
Jennifer Pace
William Rosenau
Jonathan Schachter
Michael Wermuth
Traci Williams
Ron Fricker

Administrative Support

Nancy Rizor
Priscilla Schlegel

Other RAND Staff Providing Support

Nykolle Brooks
Roger Brown
Shirley Burch
Mary Evans
David Feliciano
Tyrone Greene
Kenneth Myers
Christel Osborn
Carolyn Rogers
John Schrader
Deanna Webber

RAND Corporate Leadership on the Project

Jeffrey Isaacson, Vice President, National Security Research Division, and Director, National Defense Research Institute (NDRI)

Susan Hosek, Director (Until 1 March 2000), and Susan Everingham, Director (1 March 2000-Present), Forces and Resources Policy Center (NDRI)

Stuart Johnson, Director, International Security and Defense Policy Center (NDRI)

LIST OF KEY RECOMMENDATIONS

Essential Characteristics of a Comprehensive Functional Strategy for Combating Terrorism

***NATIONAL* IN SCOPE, NOT JUST FEDERAL**

APPROPRIATELY RESOURCED AND BASED ON MEASURABLE PERFORMANCE OBJECTIVES

Focused on the full range of deterrence, prevention, preparedness, and response

ACROSS THE SPECTRUM OF THREATS—DOMESTIC AND INTERNATIONAL

FOR DOMESTIC PROGRAMS, BUILT ON REQUIREMENTS FROM AND FULLY COORDINATED WITH RELEVANT LOCAL, STATE, AND FEDERAL AUTHORITIES

Executive Branch:

- ♦ **Develop national strategy approved by the ~~Preside~~**
- ♦ **Create a "National Office for Combating Terrorism"**
  - Director appointed by the President, confirmed by the Senate
  - Point of contact for the Congress
  - Strategy formulation
  - Plans Review
  - Multidisciplinary staffing
  - No operational control
  - Specified control of Federal programs/budgets
  - Supported by Advisory Board for Domestic Programs
  - Assistants for Domestic Preparedness, Intelligence, Health and Medical, RDT&E/National Standards, and Management and Budget

Congress:

- ♦ **Create a "Special Committee for Combating Terrorism"**
  - Bipartisan membership with full-time staff from relevant committees
  - Direct link to the new "National Office for Combating Terrorism"
  - Develops consolidated legislative plan for authorization, budget, and appropriations
  - Clearinghouse and first referral for relevant legislation

Functional Recommendations:

- ♦ **Enhance Intelligence/Threat Assessments/Information Sharing**
  - Improve human intelligence by rescinding CIA guidelines on certain foreign informants (DCI)
  - Improve measurement and signature intelligence through enhanced RDT&E (Intelligence Community)
  - Review/modify guidelines and procedures for domestic investigations (Review Panel/Attorney General)
  - Review/modify authorities on certain CBRN precursors and equipment (Executive and Congress)
  - Improve forensics technology/analysis, and enhance indications and warnings systems (National Office)
  - Provide security clearances and more information to designated State and local entities (National Office)
  - Develop single-source, protected, web-based, integrated information system (National Office)
- ♦ **Foster Better Planning/Coordination/Operations**
  - Designate Federal Response Plan as single-source "all hazards" planning document (National Office)
  - Develop "model" State plan (NEMA and FEMA)
  - Conduct inventories of State and local programs for nationwide application (National Office)
  - Promote/facilitate the adoption of multi-jurisdiction/multi-state mutual aid compacts (National Office)
  - Promote/facilitate adoption of standard ICS, UCS, and EOC (National Office)
  - Designate agency other than DoD as "Lead Federal Agency" (President)
- ♦ **Enhance Training, Equipping, and Exercising**
  - Develop input to strategy and plans in close coordination with State and local entities (National Office)
  - Restructure education and training opportunities to account for volunteers in critical response disciplines
  - Develop realistic exercise scenarios that meet State and local needs (National Office)
- ♦ **Improve Health and Medical Capabilities**
  - Obtain strategy input/ program advice from public health/medical care representatives (National Office)

- Promote certification programs for training and facilities (National Office)
- Clarify authorities and procedures for health and medical response (All jurisdictions)
- Improve surge capacity and stockpiles (All jurisdictions)
- Evaluate and test response capabilities (All public health and medical entities)
- Establish standards for communications/mandatory reporting (All public health/medical entities)
- Establish laboratory standards and protocols (All public health/medical entities)

♦ **Promote Better Research and Development and Developing National Standards**

- Develop, with OSTP, equipment testing protocols and long-range research plan (National Office)
- Establish national standards program with NIST and NIOSH as co-leads (National Office)

♦ **Enhance Efforts to Counter Agroterrorism**

♦ **Improve Cyber Security Against Terrorism**