

CSIS

**Center for Strategic and International Studies
1800 K Street N.W.
Washington, DC 20006
(202) 775-3270
Updates from: CSIS.ORG, "Homeland Defense"
Comments to: Acordesman@aol.com**

**DEFENDING AMERICA
REDEFINING THE CONCEPTUAL BORDERS
OF HOMELAND DEFENSE**

**HOMELAND DEFENSE: FEDERAL POLICY AND
PROGRAMS TO DEAL WITH THE THREAT OF
ATTACKS WITH WEAPONS OF MASS
DESTRUCTION**

Rough Draft for Comment

**Anthony H. Cordesman
Senior Fellow for Strategic Assessment**

REVISION: JULY 18, 2000

The following report is a rough initial draft section of a full report on Homeland Defense being prepared as part of the CSIS Homeland Defense project. It is a rough working draft, and reflects solely the views of the author and not of the CSIS team working on the project. It is being circulated for comment and reaction and will be substantially modified and updated before being included in the final report.

Executive Summary

There is a wide spectrum of potential threats to the American homeland that do not involve the threat of overt attacks by states using long-range missiles or conventional military forces. Such threats include covert attacks by state actors, state use of proxies, independent terrorist and extremist attacks by foreign groups or individuals, and independent terrorist and extremist attacks by residents of the US. These threats are currently limited in scope and frequency. No pattern of actual attacks on US territory has yet emerged that provides a clear basis for predicting how serious any given form of attack will be in the future, what means of attack will be used, or how lethal new forms of attack will be if they are successful.

As a result, there is a major ongoing debate over the seriousness of the threat and how the US government should react. A GAO report on terrorism summarizes the various views within the US government regarding these uncertainties as follows:¹

...there are three schools of thought on the terrorist threat: (1) some believe the threat and likelihood of terrorist attack is very low and does not pose a serious risk ; (2) others believe the threat and likelihood of terrorist attack is high and could seriously disrupt the U.S. national and economic security; and (3) still others believe assessments of the threat and vulnerability to terrorist attack need to be accompanied by risk assessments to rationally guide the allocation of resources and attention. The expert further stated that such risk assessments would include analyses of vulnerability and susceptibility to terrorist attack and the severity of potential damage. According to U.S. intelligence agencies, conventional explosives continue to be the weapon of choice for terrorists. Although the probability of their use may increase over time, chemical and biological materials are less likely terrorist weapons because they are more difficult to weaponize and the results are unpredictable. Agency officials also noted that terrorist's use of nuclear weapons is the least likely scenario, although the consequences could be disastrous.

It is difficult to predict how these threats will evolve in the future. Potential attackers have good reason to fear American military power, and most are unlikely to launch such attacks without considering the risks. At the same time, America's very strengths create an incentive to attack it using asymmetric forms of warfare. The US homeland is vulnerable. Waging asymmetric warfare against the US offers both the greatest chance of success and the least risk of retaliation, and some key technologies are evolving in ways that aid the attacker. For example, biological warfare and information warfare will inevitably make the potential threat from both foreign and domestic attackers more serious over time.

It is equally difficult to predict whether attackers will emerge with both the capability and

willingness to use weapons of mass destruction. It is not difficult to predict that such attacks are possible. Attacks involving very large amounts of high explosives or chemical, biological, radiological, and nuclear (CBRN) attacks have long been technically feasible, and the “globalization” of chemical and biological technologies and production facilities is making some weapons easier to develop or acquire. Nuclear proliferation continues and the levels of control over weapons, fissile material, and radioactive material are uncertain. Attacks using such weapons can involve a wide range of different levels of casualties, but they can involve attacks that could kill well over 10,000 to 100,000 Americans, with economic, physical, psychological, and political effects that are radically different from any covert, terrorist, or extremist attacks that have occurred to date.

These risks help explain why the US has steadily refined its policy toward terrorism and the risk of such attacks since Vice President's Task Force on Terrorism issued a report in 1985 which highlighted the need for improved, centralized interagency coordination of the significant federal assets to respond to terrorist incidents. The US response to potential threats from covert attacks by state actors, their proxies, or independent extremists and terrorists has changed even more since the mid-1990s.

The National Defense Authorization Act for Fiscal Year 1994, Public Law No.103-160, Section 1703 (50 USC 1522) mandated the coordination and integration of all Department of Defense chemical and biological (CB) defense programs. As part of this coordination and integration, the Secretary of Defense was directed to submit an assessment and a description of plans to improve readiness to survive, fight and win in a nuclear, biological and chemical (NBC) contaminated environment..

The bombing of the federal building in Oklahoma City led to the issuance of Presidential Decision Directive 39 (PDD-39) in June 1995. PDD-39 built on the previous directive and contained three key elements of a national strategy for combating terrorism: (1) reduce vulnerabilities to terrorist attacks and prevent and deter terrorist acts before they occur; (2) respond to terrorist acts that do occur-crisis management-and apprehend and punish terrorists; and (3) manage the consequences of terrorist acts, including restoring capabilities to protect

public health and safety and essential government services and providing emergency relief. This directive also further elaborates on agencies' roles and responsibilities and some specific measures to be taken regarding each element of the strategy.²

These policies have since been further developed by two key Presidential Decision Directives, PDD-62 and PDD-63, which were issued in 1998. PDD-62 reaffirmed the basic principles of PDD-39, but clarified and reinforced the specific missions of the US agencies charged with defeating and defending against terrorism, and created a new and more systematic federal approach to fighting the emerging threat posed by weapons of mass destruction (WMD). This includes programs to deter terrorist incidents involving chemical, biological, radiological, and nuclear weapons, and to manage the consequences if such incidents should occur. PDD-63 called for a national effort to assure the security of critical infrastructure. It covers both critical infrastructure protection and cyber crime, and the security of both government and private sector infrastructure to ensure national security, national economic security, and public health and safety.

New legislation has also shaped US policy. "The Defense Against Weapons of Mass Destruction Act," contained in the National Defense Authorization Act for Fiscal Year 1997 (title XIV of P.L. 104-201, Sept. 23, 1996), established the Nunn-Lugar-Domenici Domestic Preparedness Program. This act made the Department of Defense the lead federal agency for implementing the program, and is to work in cooperation with the FBI, the Department of Energy, the Environmental Protection Agency, the Department of Health and Human Services, and the Federal Emergency Management Agency.³ Equally important, major new funds have been spent on federal programs to deal with these threats, and federal spending increases by at least 43% between FY1998 and FY2001.

At the same time, there is no way for federal, state, and local governments to predict what attackers will actually take the risk of launching attacks on the US, or to predict the kind of event or crisis that could suddenly change their willingness to use any given means and level of attack. There are no clear boundaries that separate one form of attack from another, or that allow the US government to predict where and how it will have to attack to defend against an attack or to

respond to one.

While it is tempting governments to plan for the kind of cleanly defined single incident with which governments can best cope, there is no reason to assume that an attacker must follow such rules. Multiple attacks can greatly complicate defense and response and use different means of attack. A single attack can use a variety of weapons ranging from a mix of biological agents to a mix of chemical and information warfare. One attacker can piggyback on the attack of another, and attacks on the US homeland can be linked to attacks on Americans overseas or our allies. The very threat of an attack can be used to try to deter the US from attacking or exercising its diplomatic or military power or to try to force a domestic political agenda on federal, state, or local governments.

Equally important, Homeland defense must respond to a constantly changing threat. Many of the actions necessary to defend the American homeland will take years – sometimes well over a decade – to fully implement. In many cases, research and development is required, and the end result must then be transformed into deployed and effective capabilities at the federal, state, and local level. Such action can only be cost-effective, however, if it has a reasonable life cycle or period of effectiveness.

As a result, the US must take decisions now that shape programs that will affect its capabilities as much as a quarter of a century in the future. It must do so knowing that it cannot predict what new threats will or will not emerge, and that grave uncertainties exist regarding the emergence of new methods of attack and defense, and the balance of technology between them. The world can evolve in radically different directions, and is almost certain to do so. The level of foreign threats can vary sharply by region, and the level of domestic threats can change strikingly. Santayana's warning that those who cannot remember the past are condemned to repeat it is as valid as ever, but those who ignore the uncertainty of future change may well face far more serious problems.

These uncertainties have polarized part of the debate over the threat posed by weapons of mass destruction and attacks producing mass casualties. There are those who believe passionately that such attacks on the US homeland are inevitable. There are those who believe

the threat is unreal, and its an exaggeration that has grown out the search for new threats following the end of the Cold War. There are debates over how the threat should be categorized and prioritized, what response measures are needed if any, and what kinds of attack are most likely. So far, these debates have provided many insights as to what may happen, but no basis for resolving the many uncertainties involved.

Commission Recommendations

Three major commissions have released reports with recommendations applying to federal counterterrorism efforts in 1999 and 2000. The Advisory Panel to Assess Domestic Response Capabilities, also known as the Gilmore Commission, released its first report, “Assessing the Threat,” on December 15, 1999. The National Defense Authorization Act for Fiscal Year 1999 created the Gilmore Commission. The Act directed the Gilmore Commission to assess federal domestic preparedness programs, including training for local responders, coordination and funding, and local equipment deficiencies, and to release three annual reports. The Commission gave eight recommendations on domestic preparedness in its first report.

The National Commission on Terrorism, also known as the Bremer Commission, released its report, “Countering the Changing Threat of International Terrorism,” in June 2000. The 1999 Foreign Operations, Export Financing, and Related Programs Act established the Bremer Commission and directed the Commission to review federal counterterrorism policies regarding the prevention and punishment of international terrorism against the United States. The Commission excluded domestic terrorism and consequence management from the scope of its study. The Commission had a wide variety of recommendations ranging from intelligence to domestic preparedness.

Comparison of Major Recommendations

The U.S. Commission on National Security/21st Century, also known as the Hart-Rudman Commission, was mandated to examine and propose changes to the national security strategy to prepare for the 21st Century. The Hart-Rudman Commission released its strategy report, “Seeking a National Strategy: A Concert for Preserving Security and Promoting

Freedom,” on April 15, 2000. Though the Hart-Rudman Commission gave broad strategic recommendations, some apply to federal counterterrorism efforts. Since each commission had a different area of focus, no identical recommendation came from all three commissions. However, there are areas where the recommendation of two of the three commissions match. Many recommendations from the Gilmore Commission and the Hart-Rudman Commission coincide with the Bremer Commission because the Bremer Commission had the widest scope on terrorism

Evaluating Major Recommendations

The previous analysis validates many of these recommendations, although it raises important questions about others.

Gilmore and Bremer Commissions: Executive Coordination and Management

The Gilmore Commission had similar recommendations to the Bremer Commission in four areas: executive coordination, congressional coordination, information collection and dissemination, and authority roles. For executive coordination, both commissions recognize that the federal agencies are uncoordinated in regards to counterterrorism. To alleviate this problem, the Gilmore Commission supports the concept of the NDPO:

...the Federal bureaucratic structure is massive and complex. In various forums, state and local officials consistently express frustration in understanding where or how to enter this bureaucratic maze to obtain information, assistance, funding and support. In addition, Federal programs, especially those involving grants for funding or other resources, may be overly complicated, time consuming, and repetitive.

In recent months, the Federal Bureau of Investigation, pursuant to its “lead-agency” role (specified in the related Presidential Decision Directives) for crisis management for terrorism involving weapons of mass destruction, was directed by the Attorney General of the United States to organize, within its own resources, a National Domestic Preparedness Office (NDPO). The ostensible purpose of the NDPO is to serve as a focal point and “clearinghouse” for related preparedness information and for directing state and local entities to the appropriate agency of the Federal government for obtaining additional information, assistance, and support. There has been discussion about the issue of whether the FBI is the appropriate location or whether the NDPO structure and approach is the most effective way to address the complexities of the Federal organization and programs designed to enhance domestic response capabilities. The Panel is convinced that the *concept* behind the NDPO is sound, and notes with interest that the Congress has recently authorized and appropriated funds (\$6 million) for the operation of the NDPO. While that authority will give the NDPO some wherewithal to operate and to hire persons from outside the FBI, the Panel has seen no specific direction to other Federal agencies to provide personnel or other resources to the NDPO, to assist in a concerted, well-coordinated effort.

The Bremer Commission takes a more direct approach to solving the coordination

problem and recommends that the national counterterrorism coordinator participate in OMB budget decisions:

The United States does not have a single counterterrorism budget. Instead, counterterrorism programs exist in the individual budgets of 45 departments and agencies of the Federal Government. The National Coordinator for Security, Infrastructure, and Counterterrorism (currently a member of the President's staff) is responsible for ensuring that the counterterrorism programs in these departments and agencies meet the President's overall counterterrorism objectives. To discharge this responsibility, the National Coordinator established a process to set priorities, develop counterterrorism initiatives and review their funding in agency budgets. This process is an efficient means of balancing counterterrorism program requirements against other agency priorities, but it has a significant drawback. The National Coordinator has no role in the critical step when the Office of Management and Budget (OMB) decides what agency programs will be funded and at what levels. This decision is conveyed to the agencies when budget revisions are passed back to the agencies (called passbacks).

The Commission believes that whoever coordinates the national counterterrorism effort on behalf of the President should also have the authority to ensure that the President's counterterrorism objectives are reflected in agency budgets. That means the coordinator should participate with OMB in the passback of counterterrorism budget submissions, as well as in the final phase of the budget process when agencies appeal OMB's decisions

Gilmore and Bremer Commissions: Congressional Oversight

The Gilmore and Bremer Commissions also agreed that congressional coordination and oversight of counterterrorism programs needed improvement. The Gilmore Commission recommended an ad hoc Joint Special or Select Committee to coordinate congressional involvement in counterterrorism:

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

The Bremer Commission did not go as far as to recommend a joint committee but did suggest joint hearings as a first step towards congressional coordination:

...Congress should develop mechanisms for coordinated review of the President's counterterrorism policy and budget, rather than having each of the many relevant committees moving in different directions without regard to the overall strategy.

As a first step, the Commission urges Congress to consider holding joint hearings of two or more committees on counterterrorism matters. In addition, to facilitate executive-legislative discussion of

terrorism budget issues, the House and Senate Appropriations committees should each assign to senior staff responsibility for cross-appropriations review of counterterrorism programs.

Finally, the Commission notes the importance of bipartisanship both in Congress and in the executive branch when considering counterterrorism policy and funding issues.

Both the Gilmore and Bremer Commissions highlighted the need for improved information collection and dissemination between counterterrorism officials. The Gilmore Commission cited the Los Angeles area and New England as possible models information sharing and suggests additional security clearances for state and local officials:

State and local officials express the need for more “intelligence”, and for better information sharing among entities at all levels on potential terrorist threats. While the Panel is acutely aware of the need to protect classified national security information, and the sources and methods by which it may have been obtained, the Panel believes that more can and must be done to provide timely information—up, down, and laterally, at all levels of government—to those who need the information to provide effective deterrence, interdiction, protection, or response to potential threats. This may entail granting security clearances to additional officials at the state and local level. And as noted, the FBI report on Project Megiddo, and the briefings of its findings to state and local officials, is salutary.

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

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

Gilmore and Bremer Commissions: Intelligence Gathering and Sharing

The Bremer Commission provides a series of specific recommendations to improve intelligence gathering and sharing. The Commission received much criticism for recommending the CIA recruitment of terrorist informants even if they have been involved in human rights violations. However, the Commission said that the CIA had been creating an “overly risk averse” environment and needed to send a clear message that recruiting terrorists is a good thing.

There seems good reason to endorse this conclusion. The use of suspect informants is the source of most civil law enforcement activity and much of the collection of human intelligence collection. If law enforcement and intelligence agencies were denied access to such sources on legal or humanitarian grounds, this would cripple their activities and produce immense additional

human suffering. Terrorists are not usually criminals, and often have strong ideological motives. They are harder to track and subvert, and they are potentially far more dangerous. In the case of terrorists associated with the risk of CBRN attacks on the use, the threat is so great that it can literally be catastrophic. The Bremer Commission's recommendation is common sense, opposing it means trying to live in a fantasy world that makes no sense at all.

The Bremer Commission also concluded that the FBI has a "risk-averse culture" and needed to clarify the guidelines for collecting information on possible international terrorists. Among the other recommendations of the Bremer Commission was the relaxation of DOJ scrutiny for approving electronic surveillance, the need for modern computer and communications technology to keep up with terrorists, the need for more linguists, and the need for the maximum dissemination of terrorist-related information as the law allows to relevant officials. There seems to be considerable truth in these comments as well, but it is unclear that the FBI has a risk averse culture as distinguished from DOJ, and part of the problem seems to be the tacit assumption that the same procedures should be followed for all threats. There almost certainly is a strong case for treating the risk of CBRN attacks differently from lower level threats, and establishing review and authorization procedures to take more "risks" in detecting and preventing such attacks.

Gilmore and Bremer Commissions: Clarify Authority and Command and Control - Giving the Department of Defense a Lead Role

The fourth and last area of agreement between the Gilmore and Bremer Commissions was the need to clarify authority and command and control when a terrorist act occurs. The Gilmore Commission believes that the issues of "who's in charge" and how command and control is transferred from local responders to federal officials needs to be resolved. The Gilmore Commission said:

Increasingly, the Panel and its supporting staff have heard the question raised, "When an incident occurs, who's in charge?" The Panel has initially concluded that there is no single answer to the question—a determination will likely have to be made on a case-by-case basis, taking into consideration, among other factors, the nature of the incident; the perpetrator source; the actual or potential consequences immediately and over time; and the then-current capabilities for effective response at various levels. In every actual terrorist incident, non-Federal local responders will always be in charge initially, unless of course the incident occurs on a military or other Federal reservation which has its own response capability. Even in

the latter case, an incident may be of such proportions that non-Federal responders may be just as engaged, if not more so, as the Federal responders on the government enclave may be.

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

The Bremer Commission made two related recommendations about authority and command and control, one of which caused some controversy. The Commission recommended the DOD create contingency plans to take assume the lead in the case of a terrorist act so devastating that no other agency is capable of handling. The Commission said:

The Department of Defense's ability to command and control vast resources for dangerous, unstructured situations is unmatched by any other department or agency. According to current plans, DoD involvement is limited to supporting the agencies that are currently designated as having the lead in a terrorism crisis, the FBI and the Federal Emergency Management Agency (FEMA). But, in extraordinary circumstances, when a catastrophe is beyond the capabilities of local, state, and other federal agencies, or is directly related to an armed conflict overseas, the President may want to designate DoD as a lead federal agency. This may become a critical operational consideration in planning for future conflicts. Current plans and exercises do not consider this possibility.

An expanded role for the DoD in a catastrophic terrorist attack will have policy and legal implications. Other federal agencies, the states, and local communities will have major concerns. In preparing for such a contingency, there will also be internal DoD issues on resources and possible conflicts with traditional military contingency plans. These issues should be addressed beforehand.

Effective preparation also requires effective organization. The DoD is not optimally organized to respond to the wide range of missions that would likely arise from the threat of a catastrophic terrorist attack. For example, within DoD several offices, departments, Unified Commands, the Army, and the National Guard have overlapping responsibilities to plan and execute operations in case of a catastrophic terrorist attack. These operations will require an unprecedented degree of interagency coordination and communication in order to be successful.

There are neither plans for the DoD to assume a lead agency role nor exercises rehearsing this capability. Hence, these demanding tasks would have to be accomplished on an ad hoc basis by the military.

The recommendation was distorted by some to mean that the DOD should be the lead agency in all cases of terrorist acts, an assertion the Commission has denied. The Commission recognized that it is possible for a terrorist act to be so overwhelming that only the DOD would be capable responding. The Commission also recommended clarification of the legal authority of responders have in instances of catastrophic terrorism so no one hesitates or acts improperly.

The Commission said:

The Constitution permits extraordinary measures in the face of extraordinary threats. To prevent or respond to catastrophic terrorism, law enforcement and public health officials have the authority to conduct investigations and implement measures that temporarily exceed measures applicable under non-emergency conditions. These may include cordoning off of areas, vehicle searches, certain medical measures, and sweep searches through areas believed to contain weapons or terrorists.

Determining whether a particular measure is reasonable requires balancing privacy and other rights against the public interest in coping with a terrorist threat which may lead to massive casualties. Advance preparation is the best way to deal successfully with a terrorist incident without jeopardizing individuals' Constitutional rights.

The Gilmore Commission is almost certainly correct in assuming that someone must be in charge, but this could vary by type of attack and mid to high levels of attack will inevitably directly involve the President and National Security Council. Creating a peacetime Czar or Cabinet level official is only one step in resolving the problem of operational authority.

Similarly, the recommendations of the Bremer Commission seem valid when the attack involves response to a nuclear attack or a biological attack of any significance. It is far less clear that such a response is needed to high explosive or most chemical attacks. At the same time, it will be vital to ensure that biological attacks are properly characterized and that medical science shapes the response. This again illustrates the fact that extensive simulation is needed to determine how best to assign not only lead responsibility in given types attacks, but how to ensure that all proper expertise is given a proper role in leading the response.

Hart-Rudman and Bremer Commissions: Biological Pathogens, International Consensus against Terrorism, and Strengthening of Public Health Systems

The Bremer Commission also had some recommendations that were similar to those of the Hart-Rudman Commission. The three common areas were: control of biological pathogens, international consensus against terrorism, and strengthening of public health systems. As part of a greater counterproliferation effort, the Hart-Rudman Commission recommended an international ban on the creation, transfer, trade, and weaponization of biological pathogens as well as programs to deal with existing stockpiles:

The United States should seek enhanced international cooperation to combat the growing proliferation of weapons of mass destruction. This should include an effective and enforceable international ban on the

creation, transfer, trade, and weaponization of biological pathogens, whether by states or non-state actors. Also, when available and implemented with rigor, cooperative programs to deal with existing stockpiles of nuclear, biological, and chemical weapons are cost-effective and politically attractive ways to reduce the dangers of weapons and weapons material proliferation.

The Bremer Commission observed the US controls on the transfer of pathogens and related equipment is nonexistent and recommended HHS to strengthen security and Congress to create stricter controls of pathogens and related equipment:

The Secretary of Health and Human Services should strengthen physical security standards applicable to the storage, creation, and transport of pathogens in research laboratories and other certified facilities in order to protect against theft or diversion. These standards should be as rigorous as the physical protection and security measures applicable to critical nuclear materials.

The Congress should:

- Make possession of designated critical pathogens illegal for anyone who is not properly certified.
- Control domestic sale and transfer of equipment critical to the development or use of biological agents by certifying legitimate users of critical equipment and prohibiting sales of such equipment to non-certified entities.
- Require tagging of critical equipment to enable law enforcement to identify its location.

Hart-Rudman and Bremer Commissions: Strengthening the International Consensus Against Terrorism and the International Convention for the Suppression of the Financing of Terrorism:

The two commissions gave recommendations to strengthen the international consensus against terrorism. The Hart-Rudman Commission gave a broad suggestion:

The United States should also strive to deepen the international normative consensus against terrorism and state support of terrorism. It should work with others to strengthen cooperation among law enforcement agencies, intelligence services, and military forces to foil terrorist plots and deny sanctuary to terrorists by attacking their financial and logistical centers.

The Bremer Commission was more specific in deepening the international consensus against terrorism by recommending the US ratify the International Convention for the Suppression of the Financing of Terrorism:

In addition to domestic efforts, disrupting fundraising for terrorist groups requires international cooperation. A new United Nations convention, the International Convention for the Suppression of the Financing of Terrorism, provides a framework for improved cooperation. Each signing party is to enact domestic legislation to criminalize fundraising for terrorism and provide for the seizure and forfeiture of funds intended to support terrorism. The parties are to cooperate in the criminal investigation and

prosecution of terrorism fundraising, and in extraditing suspects.

...The Congress should promptly ratify the International Convention for the Suppression of the Financing of Terrorism and pass any legislation necessary for full implementation.

The final common recommendation of the Bremer and Hart-Rudman Commissions was the need to strengthen public health capabilities. The Hart-Rudman Commission gave a general recommendation to augment U.S. capabilities, while the Bremer Commission specifically recommended an international surveillance program to monitor outbreaks and terrorist experimentation with pathogens.

Different Recommendation Areas

The Hart-Rudman Commission only had one counterterrorism recommendation different from the other commissions. The Commission said the US should have specialized forces capable of dealing with threats and blackmail from terrorism and CBRN weapons.

Gilmore Commission: Threat Assessments

The Gilmore Commission focused on domestic preparedness and gave four additional recommendations. One was on threat assessments. The Commission felt that not enough attention was being given to higher-probability/lower-consequence threats and recommended more study of those threats in addition to the lower-probability/higher-consequence threats:

The Panel has indicated its concern about a preoccupation with the “worst-case scenario,” and the attendant assumption that any lesser incident can be addressed equally well by planning for the most catastrophic threat—ignoring the fact that higher-probability/lower-consequence attacks might present unique challenges of their own. As noted, this approach may not be the best means of setting budgetary priorities and allocating resources. The Panel is convinced, therefore, that more attention should be directed to assessments of the higher-probability, lower-consequence end of the potential terrorist threat spectrum—not at the expense of, but in addition to, assessments and analyses of the higher-consequence threat scenarios.

It is not really clear that this is the case in the field, and in much of the practical work being done at the agency and state/local levels. Many of the planning sessions, meetings, and simulations taking place outside the National Security area, do focus on “higher-probability/lower-consequence attacks” even when they describe them as higher level attacks. This, however, illustrates the need to plan for a spectrum of levels and means of attack, and for

neither higher-probability/lower-consequence attacks” nor the worst case.

Gilmore Commission: National Strategy for Domestic Preparedness and CBRN Terrorism Response

Another recommendation of the Gilmore Commission is the creation of a national strategy for domestic preparedness and CBRN terrorism response. The Commission is aware that the NDPO plans on developing a national strategy for domestic preparedness issues but suggests that a true national strategy must be bottom up and have presidential direction:

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

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

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

Representatives of the National Domestic Preparedness Office (NDPO)(which will be discussed in more detail below) have stated that the NDPO will develop a “national strategy” to address domestic preparedness issues. Given the fact that the responsibility for the initial and, in large measure, continuing response to *any* such incident will likely fall most heavily on the backs of state and local responders, the Panel suggests that a true national strategy must have a “bottom-up” approach—that it be developed in close consultation and collaboration with state and local officials, and the law enforcement and emergency

response communities from across the country. This Panel can help to forge that collaboration. Moreover, any such national strategy—despite its “bottom-up” structure—must have the direct leadership, guidance, and imprimatur of the President. Only that way can a strategy have a truly national tenor; but more importantly, it will contain a comprehensive, articulate expression by the nation’s chief executive of the appropriateness of and distinctions between the Federal role and missions and those at state and local levels.

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

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

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

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

In all frankness, this recommendation has only tenuous logic. It is certainly true that most of the burden of responding to low level attacks and response will fall on local and state officials, but it is not clear that they need a national strategy as much as flexible national assistance than can supplement their activity when needed. Providing a flexible federal capability to deal with bottom up demand is certainly necessary, but it is uncertain that this is a strategy in any normal sense of the term. Conversely, federal response is most needed to deal with mid and high level attacks, even if these are not the most probable near-term contingency.

This issue does, however, raise the broader issue of clearly distinguishing between risks where state and local authorities must have primary responsibility and the kind of CBRN attacks

that the federal government must deal with. One problem with much of the current approach to counterterrorism is that it assumes that levels of threat that federal, state, and local authorities have deal with for years deserve the same special attention as new and much more serious threats to the American homeland. There seems no reason that this should be the case.

Gilmore Commission: Standardization of Legal Terms

The final two recommendations by the Gilmore Commission deal with standardization. The Commission recommended codification of terms and definitions related to terrorism. The Commission cited the different definition of weapons of mass destruction by the Nunn-Lugar-Domenici Act and 18 U.S.C, Section 2332a, the definition of terrorism by the FBI and DOD, and the absence of a definition for mass casualties. There may well be a need for such action, but not at the cost of creating legislative inflexibility. Such legislation should also explicitly recognize the threats posed by proliferation and state actors, and not simply “terrorism” If necessary, it should make it clear that there are radically different levels and means of attacks and specify what differences – if any – are needed in the US response.

Gilmore Commission: National Standards for Equipment

The Commission recommended the creation of national standards for equipment used by responders to a terrorist incident. The Commission recognized that different response entities may have incompatible equipment that would greatly diminish responder capabilities. The Commission is aware of DOJ’s efforts through the National Institute of Justice to develop a list of equipment that meets certain standards, but the Commission suggested that more research and development was needed to develop effective standards for compatibility and inter-operability:

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

equipment among potential responders.

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

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

To help to reassure responders that the equipment that is being used is in fact capable of doing what it is designed to do, it is likely that an ambitious program of independent testing and evaluation will have to be undertaken. The Panel recognizes that any such program will likely have to be conducted—because of its national implications—under Federal sponsorship; and will require the addition or reallocation of significant resources. For reasons that are self-evident, local responders are insisting that testing be done with “live” agents.

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

The problem with this recommendation is that it assumes that federal, state, and local authorities already know the effects of CBRN attacks, what to stockpile to respond to them, where to put the stockpiles, and when and how to distribute them. This may be true in case of lower levels of attack, although it is brutally clear in meeting after meeting that local and state officials, and elements of federal agencies, see such stockpiles as one more way of getting more federal money to solve long-standing problems or provide new capabilities that have little to do with terrorism. There is a real risk of creating a new federal entitlements program.

The problem is very different in dealing with more lethal levels of CBRN attacks. It is not clear that federal, state, and local authorities know what to buy, where to put it, or how to ensure it can get to the user. There are certainly some cases where the need is obvious, but in many cases – particularly in the event of biological and nuclear attacks, far more work needs to be done on requirements planning.

Bremer Commission: Treatment of Former and Future States of Concern

The Bremer Commission focused on what could be improved to combat international

terrorism. The Commission's remaining recommendations were mainly related to designation of state sponsors and foreign terrorist organizations and to national counterterrorism efforts. For designations, the Commission recommended that the US keep Iran and Syria on the list of state sponsors:

Iran remains the most active state supporter of terrorism. Despite the election of reformist President Khatami in 1997, the Iranian Revolutionary Guard Corps and Ministry of Intelligence and Security have continued to be involved in the planning and execution of terrorist acts. They also provide funding, training, weapons, logistical resources, and guidance to a variety of terrorist groups. In 1999, organizations in Tehran increased support to terrorist groups opposed to the Middle East peace process, including Lebanese Hizbollah and Palestinian rejectionist groups such as the Islamic Resistance Movement (HAMAS), the Palestine Islamic Jihad (PIJ), and the Popular Front for the Liberation of Palestine-General Command (PFLP-GC). Iran continues to assassinate political dissidents at home and abroad. The Iranians responsible for terrorism abroad are often also responsible for political oppression and violence against reformers within Iran. So a firm stance against Iranian-sponsored terrorism abroad could assist the reformers.

There are indications of Iranian involvement in the 1996 Khobar Towers bombing in Saudi Arabia, in which 19 U.S. citizens were killed and more than 500 were injured. In October 1999, President Clinton officially requested cooperation from Iran in the investigation. Thus far, Iran has not responded.

International pressure in the Pan Am 103 case ultimately succeeded in getting some degree of cooperation from Libya. The U.S. Government has not sought similar multilateral action to bring pressure on Iran to cooperate in the Khobar Towers bombing investigation.

The Syrian Government still provides terrorists with safehaven, allows them to operate over a dozen terrorist training camps in the Syrian-controlled Bekaa Valley in Lebanon, and permits the Iranian Government to resupply these camps. Since its designation as a state sponsor of terrorism, Syria has expelled a few terrorist groups from Damascus, such as the Japanese Red Army, but these groups already were of marginal value to Syrian foreign policy. Meanwhile, Damascus continues to support terrorist groups opposed to the peace process. Although Syria recently made a show of "instructing" terrorists based in Damascus not to engage in certain types of attacks, it did not expel the groups or cease supporting them. This suggests Syria's determination to maintain rather than abandon terrorism.

The Bremer Commission also recommended that the US designate Afghanistan as a state sponsor and consider designating Pakistan or Greece as countries "not cooperating fully with U.S. antiterrorism efforts." On Pakistan, the Commission said:

Pakistan has cooperated on counterterrorism at times, but not consistently. In 1995, for example, Pakistan arrested and extradited to the United States Ramzi Ahmed Yousef, who masterminded the World Trade Center bombing in 1993. In December 1999, Pakistan's cooperation was vital in warding off terrorist attacks planned for the millennium. Even so, Pakistan provides safehaven, transit, and moral, political, and diplomatic support to several groups engaged in terrorism including Harakat ul-Mujahidin (HUM), which has been designated by the United States as a Foreign Terrorist Organization (FTO). HUM is responsible for kidnapping and murdering tourists in Indian-controlled Kashmir. Moreover, as part of its support for Usama bin Ladin, HUM has threatened to kill U.S. citizens.

The Commission suggested that countries designated "Not Cooperating Fully" should not

be eligible for the Department of State's Visa Waiver Program. For non-state sponsored terrorist organizations, the Commission recommended more frequent updating and inclusion of groups into the Secretary of State's designation of Foreign Terrorist Organization. The Commission also recommended that Congress review of Foreign Terrorist Organization statute to determine if changes need to be made.

Bremer Commission: Targeting Terrorist Financial Resources

For national counterterrorism efforts, the Commission recommended that the US target terrorist financial resources. The Commission suggested the creation of a joint task force of all relevant agencies that combat terrorist fundraising to develop and implement a plan to disrupt terrorist financial activities. The Commission also suggested that the Office of Foreign Assets Control in the Department of Treasury created a unit dedicated to enforcing economic sanctions against terrorist organizations. The Commission said:

Rather than relying heavily on the FTO process, the U.S. Government should take a broader approach to cutting off the flow of financial support for terrorism from within the United States. Anyone providing funds to terrorist organizations or activities should be investigated with the full vigor of the law and, where possible, prosecuted under relevant statutes, including those covering money laundering, conspiracy, tax or fraud violations. In such cases, assets may also be made subject to civil and criminal forfeiture.

In addition, the Department of the Treasury could use its Office of Foreign Assets Control (OFAC) more effectively. OFAC administers and enforces economic sanctions. For example, any U.S. financial institution holding funds belonging to a terrorist organization or one of its agents must report those assets to OFAC. Under OFAC's regulations, the transfer of such assets can be blocked. OFAC's capabilities and expertise are underutilized in part because of resource constraints.

Other government agencies, such as the Internal Revenue Service and Customs, also possess information and authority that could be used to thwart terrorist fundraising. For instance, the IRS has information on nongovernmental organizations that may be collecting donations to support terrorism, and Customs has data on large currency transactions. But there is no single entity that tracks and analyzes all the data available to the various agencies on terrorist fundraising in the United States.

These recommendation make excellent sense, provided that they are carried out under sufficient review to ensure that the selection of groups and individuals to be monitored does not become an abuse of civil liberties, or lead to surveillance of groups that are politically undesirable or who criticize the US without posing a threat of violence.

Bremer Commission: Monitoring Foreign Students

The Bremer Commission proposed that the federal government create a monitoring system of foreign students to ensure none are exploiting the US educational system for terrorist purposes. The Commission said:

While the problems of controlling America's borders are far broader than just keeping out terrorists, the Commission found this an area of special concern. For example, thousands of people from countries officially designated as state sponsors of terrorism currently study in the United States. This is not objectionable in itself as the vast majority of these students contribute to America's diversity while here and return home with no adverse impact on U.S. national security. However, experience has shown the importance of monitoring the status of foreign students. Seven years ago, investigators discovered that one of the terrorists involved in bombing the World Trade Center had entered the United States on a student visa, dropped out, and remained illegally. Today, there is still no mechanism for ensuring the same thing won't happen again.

One program holds promise as a means of addressing the issue. The Coordinated Interagency Partnership Regulating International Students (CIPRIS), a regional pilot program mandated by the 1996 Illegal Immigration Reform and Immigrant Responsibility Act (IIR/IRA) collects and makes readily available useful and current information about foreign student visa holders in the United States. For example, CIPRIS would record a foreign student's change in major from English literature to nuclear physics. The CIPRIS pilot program was implemented in 20 southern universities and is being considered for nationwide implementation after an opportunity for notice and comment. The Commission believes that CIPRIS could become a model for a nationwide program monitoring the status of foreign students.

This proposal drew much criticism from civil liberties organizations that claimed the monitoring would infringe on civil liberties and constitutional rights. In balance, however, the Bremer Commission seems correct. Studying in the US is not a right. Student visas are granted only to legitimate students for a specific course of study. Tracking students to the point of ensuring that they (a) meet the terms of their visa, and (b) there is some record of their course of study is little more than common sense.

Bremer Commission: Liability Insurance

The Bremer Commission recommended that the FBI and CIA reimburse their agents for the full cost of personal liability insurance so that agents could be more aggressive in combating terrorism and not fear lawsuits for officially sanctioned activities. Providing such insurance seems valid and providing it would not affect adequate supervision or discipline or the right to sue and seek legal redress with all of the attendant public scrutiny.

Bremer Commission: Realistic Exercises

The Commission also recommended more federal preparedness exercises and more funding for TOPOFF, the senior management exercise administered by the DOJ and FEMA. The Commission said:

In addition to DoD exercises, a realistic interagency exercise program, with full participation by all relevant federal agencies and their leaders, is essential for national preparedness to counter a catastrophic terrorist attack. In June 1995, the President established an interagency counterterrorist Exercise Subgroup and program which included preparation for a catastrophic terrorist attack. However, not all federal agencies have participated in or budgeted for these exercises.

Additionally, in September 1998, Congress funded and mandated the Department of Justice and the Federal Emergency Management Agency to conduct a counterterrorism and consequence management exercise, called TOPOFF, involving relevant federal agencies and their senior leadership, with select state and local governments participating, to evaluate the U.S. Government's preparedness for a catastrophic terrorist incident. However, sufficient funding was not provided and there is no requirement to exercise on a regular schedule.

The President should direct (1) the Exercise Subgroup, under the direction of the national coordinator for counterterrorism, to exercise annually the government's response to a catastrophic terrorism crisis, including consequence management; and (2) all relevant federal agencies to plan, budget and participate in counterterrorism and consequence management exercises coordinated by the Exercise Subgroup and ensure senior officer level participation, particularly in the annual exercises.

As has been noted earlier, it is far more important that federal, state, and local authorities understand what they really need to do and how to do it than to establish new lines of authority, fund the wrong program, and focus efficiently on the wrong set of contingencies and requirements.

General Recommendations

The US faces real and growing potential threats from state actors, their proxies, or independent extremists and terrorists. While US agencies and analysts have tendency to exaggerate the immediate threat, or the threat posted by given actors, there are many potentially hostile foreign and domestic sources of such threats, and some key threats like biological weapons involve rapidly changing technologies that will pose a steadily growing threat to the America homeland.

It is also clear from the proceeding analysis that the federal government is making major

progress in many areas, and laying the groundwork for improved cooperation with states, localities, the private sector, and the public. Indeed by the standards of many governments that face far more clear threats than the US, the US has already made significant progress in beginning to address these issues. In many cases, the US is already well ahead of its friends and allies.

At the same time, there still seems to be much that can be done. Some detailed recommendations have already been discussed in the analysis of the threat, and federal activities and spending by agency, and the recommendations of various commissions. There are, however, a number of additional recommendations that could help refine and improve the US effort..

Planning for Both Higher-Probability, Lower-Consequence and Low Probability/Catastrophic Events

The US must come firmly to grips with the fact it does not exist at the end of history and has not forged a kinder and gentler world:

- *Unchecked vulnerability is an unacceptable danger for “the world’s only superpower.”* Nature may abhor a vacuum, but enemies do not, and the evolution of more effective homeland defense is almost certainly essential to deterrence. At the same time, the very term “homeland defense” can be misleading. There are no boundaries that separate US counterproliferation and counterterrorist activity in defense of the American homeland from defense of its allies, military forces, and citizens overseas.
- *Deterrence, counterproliferation, counterterrorism, and law enforcement must be closely linked in dealing with these new threats, and it is clear that US must rethink many of its current security concepts.* Even the strongest advocates of homeland defense must recognize that a better offense may often be more effective than improved defense. Improving the offensive threat of retaliation overseas may often be the best way of defending both US interests overseas and US territory. A given investment in strengthening our allies may often be a better defense against proliferation and terrorism than investing in domestic counterterrorism programs. Hard trade-offs may have to be

made between investments in the intelligence needed to intimidate and deter foreign states and terrorist groups, and the law enforcement capabilities needed to intercept attackers once they enter the US.

- *The US cannot afford to rely on rethinking the offense as a substitute for improved defense, anymore that it can use defense as a substitute for deterrence, offense, and retaliation:* The US cannot prepare itself for the new threats posed by asymmetric warfare, foreign proliferation and terrorism, and domestic violence using new means like chemical, biological, and information warfare without much stronger programs to prevent such attacks in the US and to respond to them if they succeed. The world of the 21st Century will not be a repetition of the mutual assured destruction of the Cold War. Radical states, regimes acting under extreme pressure, terrorists, and American citizens can turn threats like chemical, biological, and nuclear weapons into grim realities in ways the US will never be able to deter with complete confidence.
- *The US must act now if it is to prepare for the future.* Developing an effective program means thinking at least 25 years into the future. It will take at least a decade for federal, state, and local authorities to develop the organization they need to deal with these threats. There are massive organizational problems that federal, state, and local authorities must solve to cooperate efficiently. The role of the federal government must be redefined in ways that are both compatible with a free society and which can preserve one when it is under attack and when attacks are successful. It will take years of exercises, tests, and training to determine what courses of action can be made to work and are most effective. Investing in such a process of change means that it must be flexible and modular enough to react to the fact no one can predict the nature of future attacks, but any meaningful improvement in capability will be so expensive that it can only be justified if it can cope with uncertainty.
- *The US must decide whether it will begin now to fund effective defenses attacks on a scale far different from any form of covert or serious attack than it has planned to deal with since the end of its efforts to provide civil defense against nuclear attack.* Marginal

changes in federal, state, and local efforts, and in the relationships between federal, state, and local agencies, can do much to cope with the threat posed by attacks using large amounts of high explosives, chemical weapons, and low-lethality biological and radiological attacks. While the level varies by state and locality, attacks involving 1,000 to 10,000 do not require radical changes in response capabilities. Nuclear and high lethality biological attacks can, however, easily produce casualties in excess of 10,000-100,000 Americans. To date, most studies and exercises indicate that existing programs and capabilities would not be adequate to deal with such attacks, and they would require far more decisive federal action and intervention than is currently feasible. There are those who argue strongly that no such threat currently exists and those who argue with equal force that they are inevitable. The present reaction of the federal government seems to be to try to improve near-term response capabilities to deal with lower levels of attack while conducting research and development into the higher levels of attack, but the policies involved remain unclear and the actions of federal agencies reflect very different perceptions of these threats.

- *The US must take a new approach to research and development and technology:* There are many areas of new technologies which must be moved off the drawing board, tested, deployed, and modified if the US is to have defensive tools that begin to match its offensive capabilities. At the same time, the US needs careful net assessments of the trends in the threat and how these impact on new approaches to defense and response. Effective planning means that the US cannot afford to mix the myth of technology with the reality. The past track record of US efforts to create and use new technologies in its defense is one of amazing eventual success. At the same time, it is one of almost universal evidence that even the best technologists cannot be trusted to create successful and deployable tools with anything like the promised effectiveness at the promised cost and time.

The development of such a complex approach to threat assessment, based on a frank admission of the vast uncertainties involved, goes against the basic grain of the American character, and forces far more demanding criteria for program justification than are normally

required. The US cannot, however, deal effectively with threats posed by state actors, their proxies, or independent extremists and terrorists unless it adopts such an approach.

Even if the US adopts such an approach, however, it will still have to concentrate its limited resources on making marginal improvements in current capabilities to deal with current threats, while adopting a research and development-driven approach to dealing with more serious and emerging threats. As a result, any US program is likely to have marginal impact, and require constant evolution for at least the next half decade.

Reacting to the Uncertain Nature of the Threat

There are many “true believers” who feel that a given threat will or will not materialize in a given form. Given the inherently uncertain nature of predictions as to who will be a threat, the means of attack they will use, and the effectiveness of the means of attack they use, it is almost certain that some of these “true believers” will prove to be right. The problem is that there is no sufficient evidence to say which threats are most important, or to predict the means of attack and level of effectiveness.

Federal programs are being forced to deal with an extremely broad spectrum of potential threats that individually have low probability, but where there is high probability that some of these threats will emerge as threats to the American homeland. As a result, each agency and department tends to threat the threat in terms of its own mission and institutional bias, and this problem cannot be resolved by central direction. Having the National Security Council, a “terrorism” czar, or an interagency forum agree on a given threat or threats will not affect the laws of probability. Uncertainty is simply uncertainty.

There is also an inherent danger in attempting to create a truly coherent program. When a truly high degree of uncertainty exists regarding the need for specific forms of federal action, enforcing a high degree of coherence from the center may actually interfere with the efficient use of resources. In many cases, individual agencies will achieve a higher capability to deal with uncertainty if they suboptimize around those marginal steps each can take to improve their existing capabilities to deal with a wide range of threats. This is particularly true in a sharply

resource-constrained environment where many potentially desirable actions will remain unfunded until a much clear pattern of threats emerges.

This is particularly true because the threats at issue involve a wide spectrum of extremely lethal biological weapons and nuclear weapons. Large amounts of high explosive, chemical weapons, and less lethal biological weapons can produce truly tragic consequences. However, the level of deterrence, defense, and response pales in terms of cost in comparison with the ability to deter, defend, and respond to the kind of attacks that could involve casualties far in excess of 10,000 Americans and billions of dollars worth of damage.

There are three further problems involved in such threat analyses that badly need to be dealt with in further US efforts to plan and execute effective programs:

- *Most of the lethality and effects data for chemical, biological, radiological, and nuclear weapons involve major uncertainties that badly need to be resolved, and the federal government is just beginning to develop effective models and simulations of such effects.* There is no lack of effects data or models per se, simply an immense lack of credibility and parametric modeling of uncertainty in a form that goes from dramatizing the problem to being useful in developing specific lessons for federal, state, and local responses. These problems have also been compounded by a natural tendency to build models to justify given policy recommendations or programs. To be blunt, agencies in the federal government, FCRCs, contractors, and NGOs are far better at using analysis to market given policies and programs than to perform analysis per se. There is a striking lack of intellectual rigor and analytic integrity in many of today's efforts that must be remedied if the US is to prioritize federal actions and funding.
- *Programs shaped around today's threats, or some prioritization based on current assessments, will not solve any of the key problems in planning and programming.* Democracies do not suddenly develop solutions they can then keep secret from their enemies. US programs take time to implement and must be publicly funded and implemented in an open society. As a result, potential attackers can adopt new methods

of attack and respond to any remaining gaps in US capability. This makes it absolutely essential to explicitly analyze the cost of defeating any given federal program over time, and the probable impact improving any US capability will have in driving attackers to use other means.

- *New methods of analysis must be developed that examine the present and future balance of offensive, defensive, and response capabilities. They must be supported by adequate net technological assessments, and analysis of countermeasures and costs to defeat all ongoing and proposed federal activities.* It is difficult enough to analyze current or near-term risks, but such analysis simply is not adequate. Effective US programs can take a decade or more to fully implement, and the technology shaping current threats is constantly changing. This is not simply a matter of basic advances like biotechnology, it is a matter of the steadily growing dissemination of the technology equipment needed to produce and deliver large amounts of high explosive, chemical weapons, and biological weapons. Much of the description of potential threats does not explicitly analyze the potential growth or changes in threat technology even when it proposes the adoption of new deterrent, defensive, and response technologies over a period of many years. There is a lack of technological net assessment that is a key not only to identifying and prioritizing effective programs, but to managing them so they counter technology growth.

The Lack of “Transparency” in Federal Programs

There is nothing unique about the lack of transparency in federal programs to deal with the threats posed by state actors, their proxies, and foreign and domestic extremists, and the use of high explosives, chemical, biological, radiological, and nuclear weapons. The US budget, and agency program and budget description often fail to describe their budgets, the nature of their programs, and measures of effectiveness in any detail. Aside from the Department of Defense, there are virtually no future year spending projections, and the Department of Defense classifies the breakouts of its future year spending projections that provide any useful description of how money is to be spent.

Far too much of the federal literature on “terrorism,” however, is threat-driven. It does not describe and justify the program, it describes the threat. There is no description of exactly what program activities are involved, or of past, current, and projected costs. There are no measures of effectiveness, or total spending and procurement are confused with such spending. As a result, it becomes extremely difficult to understand what the federal government is doing and why it should do it. Many of the descriptions that agencies do provide raise real questions about the extent to which given agencies have simply reshaped existing activities to take account of the fact the Congress is providing new incremental funding, and counter-terrorism has become fashionable.

These problems are compounded in part by the fact that OMB is required to report to the Congress, but there is no central agency charged with creating a plan, program, and budget. At the same time, they are compounded by a host of jurisdictional problems with the Congress, and the lack of a single committee or joint committee structure that could provide a cohesive degree of overview. As a result, there is a large pool of federal reporting on individual problems and issues, but little effort to appraise the overall program.

There are those who would argue that part of the reason for the lack of transparency is security. There are certainly areas like intelligence where detailed program descriptions could compromise security. There are other areas where too detailed a description of US investigative and response capabilities could aid an attacker in planning an attack. In broad terms, however, there is little reason to classify most of the information needed to allow outside analysts to fully understand the nature of federal efforts, and there are good reasons to require federal agencies to provide such data.

To put it bluntly, far too many federal activities seem to have limited substantive value, raise major uncertainties, reflect the reshaping of existing programs to obtain incremental funding, or raise questions about duplication. Furthermore, there is a tendency to imply short-term solutions can be found to long-term problems, or fund minor palliatives simply for sake of seeming to act. Few, if any, programs provide any picture of what it will cost to fully implement the activities agencies are now beginning. None seem to provide meaningful measures of

effectiveness, or any analysis of the current and future costs of “defeating” the capabilities being funded.

- *While there are sharp limits to how much coordination can be forced on a wide range of federal activities, the federal effort would almost certainly benefit from a requirement for a comprehensive annual report similar to the one the Secretary of Defense provides on the national security activities of the Department of Defense, and for including both a net assessment of the threats and US capabilities, and the future year budget implications of given federal activities as well as a description of the current budget request.*
- *Regardless of how the issue of Congressional jurisdiction is resolved, there is also a clear case for requiring the federal government to submit an annual budget justification document, and future year budget plan, that covers all related federal activities at the same time the President submits the federal budget. Such a document could be both unclassified and classified. It would thus ensure that the Executive Branch had to coordinate its programs fully as part of the budget process. It would ensure that whoever is in charge in the federal government had real review authority, and control of money is generally better than a title. It would ensure that all elements of Congress reviewed a common plan, which may be far more important than creating a single new committee. It would also allow full public review and state and local access to the overall federal plan. It is easy to talk about “reinventing government;” it would be nice to actually provide some degree of functional transparency in a critical new mission area.*

Focusing on Priorities, Programs, and Trade-offs: Creating Effective Planning, Programming, and Budgeting

The US would face serious resource allocation problems even if CBRN threats were less uncertain and ambiguous. The threat posed by covert, terrorist, or extremist use of weapons of mass destruction is only one of the new threats the US must react to. Homeland defense includes direct threats such as missile attack, and other evolving threats like information warfare. There

are other transnational threats like narcotics, organized crime, and illegal immigration that pose a serious threat to American society even if they are not military or paramilitary in character. At the same time, the US faces major problems in funding its existing future year defense program, and its civil discretionary and entitlements budget. Money is, and will remain, a critical factor, and will force hard trade-offs on all government action.

This report focuses on the threats to the American homeland posed by state actors, the use of proxies, terrorist and extremist attacks by foreign groups or individuals, and terrorist and extremist attacks by residents of the US using conventional weapons and weapons of mass destruction. Separate reports focus on the threat posed by direct attacks by foreign states using weapons like ballistic missiles, and the threat of information and economic warfare.

This focus is not intended to imply that the emerging threats to the American homeland can be neatly compartmented, or do not interact. The spectrum of threats foreign governments can pose includes all of these methods of attack. Well-organized foreign and domestic terrorist/extremist groups have the *potential* to pose a wide range of high explosive, chemical, biological, and information warfare threats. There are no rules that say foreign governments and foreign and domestic terrorist/extremist groups cannot cooperate or piggyback on each other's activities. In broad terms, however, the threats to the American homeland posed by state actors, the use of proxies, terrorist and extremist attacks by foreign groups or individuals, and terrorist and extremist attacks by residents of the US using conventional weapons and weapons of mass destruction require a different mix of responses. These responses can only be discussed in terms of practical alternatives if it is narrowed down to the point where each of the major relevant homeland defense options can be analyzed in depth.

As is the case with national missile defense, this report also deals with issues that are highly politicized. Preparing to deal with the spectrum of threats posed by foreign states and terrorists using weapons of mass destruction is currently fashionable and "politically correct." This has had major benefits in many ways. The President and high level officials have set forth clear policies for dealing with many aspects of the problem. The Congress has passed dramatic new legislation, and major changes are well underway to improve federal, state, and local

preparation to deal with the threat. There is new money available to federal agencies at a time when severe budget constraints exist on virtually every form of government spending.

Unfortunately, however, the very popularity of the issue of terrorism and weapons of mass destruction also means that there has been a rush to react to potential threats without developing a common definition of the combined threat posed by covert attacks by state actors, state use of proxies, terrorist and extremist attacks by foreign groups or individuals, and terrorist and extremist attacks by residents of the US. There is still insufficient definition of the different kinds of threat that different kinds of weapons of mass destruction pose and how these relate to threats using conventional explosives. In many cases, departments and agencies are defining the nature and intensity of the threat to meet their own internal needs and perceptions, or are acting on assumptions that imply a far better ability to predict the future than can possibly exist.

As yet, there is only limited coordination in many federal, state, and local efforts except at the organization chart level. Departments and agencies struggle for resources and influence, and there are good reasons for the resulting “feeding frenzy. Even if one ignores all federal funding for critical infrastructure protection, funding for counterterrorism has risen from \$8.3 billion in FY1998 to \$12.9 billion in FY2001, and funding for new efforts like dealing with the threat posed by weapons of mass destruction have risen from approximately \$645 million in FY1998 to \$1.6 billion in FY2001.

Under these conditions, old programs are being recast to suit new policy priorities and rhetoric, while agencies compete to create new programs and assume lead responsibility. In some ways, homeland defense has replaced the Strategic Defense Initiative as the “next best thing.” As the GAO and CBO have pointed out, the sharp rise in spending has not yet led to tight central management of the homeland defense effort, although there is a growing and steadily more effective effort to develop balanced and coordinated capabilities. There also has been little success in estimating the mid and long term budget implications of program growth and new responsibilities at the federal level, much less the state and local level. Many RDT&E efforts have been started without clear deployment and life cycle implementation plans, and there are few meaningful measures of effectiveness for federal spending.

The sharp limits on how much money and human resources can be allocated to this aspect of homeland defense will, however, soon force the US to be much more selective in choosing the programs it can continue to expand or sustain. Even today, the government needs to make every effort to coordinate its efforts and prioritize them. Regardless of partisan rhetoric, it is clear that US is not yet prepared to pay for its existing military forces and capabilities. Furthermore, there are other major transnational problems like drugs immigration, and cybercrime. There are many unrelated shortfalls in law enforcement and emergency response capabilities. For example, the US faces a major crisis in medical spending even without considering the impact of responding to chemical, nuclear, and biological attacks, and is sharply reducing the size of its emergency medical facilities and hospital intensive treatment capabilities.

It is only possible to ignore these realities at the start of a homeland defense program, at a time when planning is large threat driven and the cost of new activities is relatively limited. As long as current outlays are limited, it is all too easy to can find a credible potential threat, issue warnings, make a speech, issue an executive order, or pass a law. Any competent analyst, contractor, research firm, NGO or advisory group can find a new way to focus on potential threats and the potential merit of uncosted and poorly defined solutions. The end result is start far more activities than can be finished, fail to consider the future trade-offs that must be made to deploy effective capabilities, duplicate other efforts, or refashion existing programs under new labels.

- *Improvements in policy and strategy are no substitute for effective management programming, budgeting, and measures of the effectiveness. The practical challenge is to use more management information systems and PPB methods to tie the efforts of government together develop clear priorities, ensure that cost estimates are provided of bring programs to maturity and sustaining them, tightly manage where the money goes on an ongoing basis, ensure that the risk of countermeasures and cost to defeat is assessed on a continuing basis, find suitable measures of effectiveness, and make suitable iterative trade-offs. In fact, one recommendation of this report is that there be one central point in the federal government charged with developing a budget overview of current programs, an analysis of their future*

year costs and deployment costs, relevance to the threat, and measures of effectiveness.

Unless this transparency is ruthlessly forced upon the federal government – both in the executive branch and Congress -- no amount of organizational changes, committees, legislation, and directives will create the proper focus. The creation of lead agencies will be a bureaucratic farce, and state and local authorities will be confronted with conflicting demands, and will often have little impact on federal bureaucratic infighting.

Equally important, Congressional oversight and effective outside review and constructive criticism will be impossible. The constant misuse of security classification will create large areas of “black programs” that encourages departmental empire building and a lack of management. Programs with limited relevance will be recast as part of the homeland defense effort, and areas that really need funding will be ignored.

Effective Action Must Be Broad-Based and Sub-Optimize Efficiently

At the same time, there are limits to how much coordination is practical, and how much central direction can be applied. The federal government, individual agencies, and state and local governments will often have to sub-optimize changes to their current programs in those areas where they can do the most in the near term with the least money. While the Clinton Administration is seeking to create a cohesive federal program, and has made progress towards this end, there are no models, analytic methods, or simulations which can hope to integrate all of the elements of homeland defense into some master analysis or set of priorities based upon a common model.

The problem is not specialization and compartmentation per se. It is that it must be the result of central management and oversight, particularly given the severe limits on what any foreseeable combination of allied, federal, state, and local efforts can do. Cost constraints will be tight, trade-offs will be made whether or not they are made openly and explicitly, and the result

will be anything but leak-proof. Most important, central direction is needed to ensure that the capabilities the US creates evolve to respond to reality and not to established bureaucratic priorities.

It is also far from clear that threat and risk assessments can be used to create a set of scenarios that focus the defense effort, or which prioritize it around a select and well-defined group of scenarios. Once again, the problem is to determine the range of low probability events the US may have to react to, and what this means for deterrence, offense, defense, and response. While it is most likely that the US will have to react to a series of relatively low level events in the near term, the cumulative probability that the US may have to react to a few much more serious events over the mid to long term may well be equally high. As a result, threat and risk assessments must consider nuclear and highly lethal biological attacks.

Furthermore, there are deep conceptual problems. As has already been discussed in depth, the range of threats simply are not predictable enough for given agencies to attempt more than a constantly evolving and uncertain process of suboptimization. Put differently, departments and agencies must often do what they can to improve their capabilities at the margin, rather than seek to create building blocks in some kind of coherent homeland defense.

Such efforts may not, however, have great impact on US ability to defend against nuclear and highly lethal biological attacks. They may give the impression of defense and response capability, but the end result may not be able to cope with very high levels of attack, which may well force all levels of government to improvise radically with little warning and under intense pressure. Marginal improvements in resources may fail to deal with response requirements or be impossible to allocate efficiently within the time windows required. This is particularly true because there currently seems to be little practical understanding of what a “worst case” or high level attack would really do, and how uncertain its effects now are.

Finally, the present coordination effort often focuses either on “worst cases” or on those federal programs identified as being directly designed to defend or respond to the threat state actors, their proxies, or independent extremists and terrorists pose to the American homeland. This is almost certainly *not* the right way to will prove to create the most effective overall

program to actually improve Homeland defense. Such a program must explicitly consider the offensive, deterrent, and retaliatory capabilities of US military and intelligence agencies, and the role their activities overseas can play in creating an effective deterrent to foreign attacks on the US.

As a result, the US needs to rethink its approach to develop a program that constantly evolves, and which is based on the dilemma that it must try to manage chaos:

- *Effective homeland defense must be based on responding to the patterns of threats that actually emerge, and to shifts in the most likely contingency requirements.* It is virtually an iron law that any effort will fail that is based upon the current theories of what threats *may* emerge in a given area. Once again, a guiding principle is that there is a timeline of at least a quarter of a century of uncertain risk. No program or analysis made today can possibly be based on the correct priorities. The issue is rather how quickly and effectively programs can anticipate change and react to it.
- *The key to a successful result is that sub-optimization must be deliberate and subject to broad review, and not simply evolve by accident. Whatever the federal government does, it must involve an explicit and well-reasoned balance between:*
 - Offense and defense
 - Action overseas and in concert with our friends and allies, and measures actually taken in the US.
 - Counterproliferation and counterterrorism.
 - Defense and response.
 - Including threats in the spectrum of threats requiring special action by the federal government as part of homeland defense, and the role played by conventional law enforcement.

Managing Research and Development, Rather Than Treating CBRN As A Wish List and Slush Fund

Research and development programs receive little detailed description and the description that is provided often concentrates on the threat being dealt with, and provides little program detail. No agency provides a meaningful description of its future program, future costs, milestones, or measures of effectiveness. Cooperation with state and local agencies is often ignored, and when it is not, it tends to be discussed in anecdotal terms

There is no evidence that any department or agency has provided a technology net assessment to examine whether its programs will provide defensive capabilities that outpace advances in offensive capability. There is virtually no discussion of the risk posed by countermeasures or the cost to defeat current and planned programs. There is no discussion of the outyear costs of research and development activity or of estimated deployment schedules, measures of effectiveness, and life cycle costs. Almost without exception, there is no way to be certain to degree to which given programs in given departments or agencies are actually focused on CBRN and other counterterrorism activities, or have simply recast ongoing or desired programs to compete for such funds.

- Federal research and development efforts have a poor to dismal record of effective management. It is time to reverse this situation.

Looking Beyond CBRN: Dealing with All Medical Risks and Costs

The previous analysis indicates that there is a need for a zero-based review of the current data on the lethality of biological weapons, and for a comprehensive net technical assessment of current and future trends in biological offense and defense. Biological warfare defense and response efforts cannot, however, be separated from the need for an effective national health program.

Response measures against biological and nuclear attacks can require truly massive

increases in public health efforts and emergency services at a time when the US already faces major problems in funding medical entitlement programs and growing cost constraints are being placed on investments in medical capabilities which normally have high utilization rates. The response capabilities required to deal with large biological and nuclear “incidents” may simply be unaffordable without far more evidence that such attacks are likely, and effective treatment may simply be impossible. One grim result is that “triage” may have to be performed in ways that deliberately leave a very high number of casualties to die.

The risk of attacks on the American homeland that have massive medical consequences requires that homeland defense measures deal with two major interrelated problems in public health policy and spending.

- *There is a significant amount of medical literature -- including a recent report by the National Intelligence Council -- that indicates that the US is under significant cumulative threat of the outbreak of some disease for which current medical treatment is not adequate.* In short, the US may face a serious threat from nature as well as from foreign attackers and domestic extremists.⁴
- *US medical spending has already reached the point where it dominates much of the end use of the entitlements in the federal budget,, and where drastic efforts are being made to down-size medical spending.* These facts are largely ignored in much of the current discussion of Homeland defense, which focuses on threats and then on research and development measures that do not have a deployment cost, and which often involves response efforts so limited in estimated casualties that the list of equipment is “affordable” largely because it is assumed that the existing infrastructure can deal with the casualties and the medical impact is both treatable and involves non-infectious threats. These assumptions, however, are only valid as long as the most serious threats are defined away and the eventual need to pay for facilities and a full spectrum of response measures is ignored.

Homeland Defense and/or Law Enforcement

The US also faces major problems in defining the point at which federal intervention in some form of homeland defense program is needed, as distinguish from a reliance on normal federal, state, and local law enforcement. Many of the definitions now used for terrorism can include virtually any threat of violence by an individual or small group with a political or ideological agenda, or who is willing to attack civilians. In practice, however, most such threats are dealt with as normal law enforcement activities unless some foreign element is involved. Even in those cases where foreigners are involved, many cases are dealt with through normal law enforcement means.

It does not make sense to change these arrangements without clear cause, and the previous statistics on terrorism in the United States need to be kept in perspective in allocating law enforcement resources. According to the FBI's uniform crime statistics, there were 10 cities in the US with populations of 100,000 or more that had more than 100 murders in the first six months of 1999, and three with over 200 murders. If rapes and assaults are counted, there were 47 cities in the US with populations of 100,000 or more that had more than 1,000 "casualties" in the first six months of 1999, and nine with over 3,000.⁵

There is a reason that it now takes some 40,000 armed men and women to try to secure the greater New York metropolitan area alone. There is also a reason why law enforcement activity cannot be centered around counterterrorism or dealing with low probability covert attacks until there is a far clearer and more dangerous threat than now appears to exist. At the same time, it is inconceivable that the US could develop an effective approach to homeland defense that did attempt to make use of these resources at every level of law enforcement.

- *The task is to find the right trade-offs between reliance on normal law enforcement and specialized homeland defense activity, and between using existing resources with other primary missions and creating new dedicated homeland defense components.*

Rule of Law, Human Rights, Asymmetric Warfare, High Levels of Attack and “New Paradigms”

Homeland defense impacts heavily on legal and human rights issues. Until now, the threats to the US have been limited enough so that the US can afford to shape its response on the basis of strict observance of civil law and human rights. There is also ample emergency authority for the President, Governors, and local officials to use virtually all of the assets of government to deal with homeland defense emergencies if they arise. Even restrictions on the use of the military, such as like the Posse Comitatus Act (18 USC 1385), have so many exceptions that the problem is much more likely to be getting sufficient warning to act than any practical legal barrier to effective action.

Much of the present discussion of legal and human rights issues, however, ignores what would happen if the threat of the use of biological or nuclear weapons against the US homeland became more tangible and immediate. It also ignores the real world effects of state actors or terrorists/extremists carrying out highly lethal attacks. These effects include the problems in human rights created by the need to deal with mass triage in the face of saturated medical facilities and/or to contain a civil population with force in the event of an attack using a highly infectious agent.

Today, the US has the luxury of examining such options with attitudes shaped by the fact such attacks do not seem imminent and there are no real precedents for the kind of damage that may occur. There have been no successful attacks using weapons of mass destruction in the US, barring minor incidents, and only one partially successful major attack overseas – the Aum Shinrikyo attack in Japan. No nation or group has yet exploited the use of effective biological weapons, in spite of the fact that many nations have developed such weapons, and nuclear proliferation remains contained enough to limit the threat posed by regimes and nations that have demonstrated a high willingness to take risks as well as terrorist and extremist groups.

America’s enemies are developing a steadily more sophisticated understanding of asymmetric warfare and America’s vulnerabilities. If major unconventional attacks occur and

succeed anywhere in the world in the years to come, such attacks might well become a new norm for asymmetric warfare. America's enemies might then respond by rapidly developing such capabilities to attack the US, and such shifts could occur relatively quickly and with little strategic warning. With luck, such a world will never happen. Reliance on luck, however, is scarcely a reliable criterion for planning. It is quite clear, however, that the US and its allies may face a very different future/

- *US intelligence efforts and law enforcement must both reorganize to deal with the risk of a "paradigm" shift in the willingness and ability to use weapons of mass destruction in unconventional attacks on the US homeland, and be given the proper legislation and regulations.* Many states are now involved in a process of proliferation that will change their capabilities to carry out such attacks. Advances in manufacturing, petrochemicals, and the biological science are making it steadily easier for both states and non-state actors to build lethal chemical and biological weapons. The technology and components to develop every aspect of nuclear weapons other than weapons grade uranium and plutonium are becoming steadily more available.

The Need for Central Coordination and Management

: There is broad agreement that some central office is needed to coordinate the federal effort, to ensure proper program and budget review, to coordinate auditing of capability, and to coordinate emergency response capability. There is also broad agreement that such a coordinator needs sufficient rank and authority to speak for the President on these issues, and to ensure that agency budget submissions must include adequate programs and funding. Some have proposed an independent office similar to the Y2K program, some a new form of drug Czar, and some a cabinet level officer.

- *These issues, however, need far more careful study.* Similar arguments are being made about providing a coordinator to deal with critical infrastructure attacks and all of homeland defense. At the same time, many of the prevention and response skills

involved are highly specialized and duplicate the activity needed to respond to many other forms of emergency – accidents, weather, etc. At this point in time, what really seems to be needed is a Presidential Task Force to review the broad need to deal with all of the emerging threats to the American homeland, and to draft recommendations and a PDD for the next President.

Table of Contents

HOMELAND DEFENSE: FEDERAL POLICY AND PROGRAMS TO DEAL WITH THE THREAT OF ATTACKS WITH WEAPONS OF MASS DESTRUCTION.....I

Rough Draft for Commenti

REVISION: JULY 16, 2000.....i

US GOVERNMENT EFFORTS TO CREATE A HOMELAND DEFENSE CAPABILITY 1

KEY PRESIDENTIAL DECISION DIRECTIVES AND LEGISLATION AFFECTING THE FEDERAL RESPONSE 1

CHANGES IN THE STRUCTURE OF THE FEDERAL EFFORT..... 4

THE GROWTH OF THE FEDERAL EFFORT..... 5

The FY2000 Program..... 6

The FY2001 Program..... 7

THE DETAILS OF THE FEDERAL EFFORT..... 8

The Changing Patterns in Federal Spending..... 9

Planning and Programming the Overall Federal Effort 11

Antiterrorism, Counterterrorism, and Core Spending..... 20

Antiterrorism..... 20

Counterterrorism 21

“Core Spending” on Terrorism..... 22

Spending on Preparedness for Attacks Using Weapons of Mass Destruction 26

WMD Antiterrorism Activities..... 27

WMD Counterterrorism..... 28

R&D for Defense Against WMD 28

FEDERAL EFFORTS BY DEPARTMENT AND AGENCY 33

DEPARTMENT OF AGRICULTURE..... 40

National Animal Health Emergency Program..... 40

CENTRAL INTELLIGENCE AGENCY 41

DEPARTMENT OF COMMERCE..... 42

DEPARTMENT OF DEFENSE 42

Domestic Preparedness Program 44

Chemical and Biological Defense Program 47

WMD Civil Support Teams..... 50

Joint Task Force for Civil Support..... 51

Foreign Emergency Support Team 51

Office of the Secretary of Defense..... 51

US Military Services and Joint Chiefs of Staff..... 52

Possible FY2000 Budget 53

DEPARTMENT OF ENERGY **53**

Office of Nonproliferation and National Security..... 54

Office of Emergency Management 54

Office of Defense Programs..... 54

Office of Emergency Response..... 55

Nuclear Emergency Search Team..... 55

Radiological Assistance Program..... 55

The Nuclear Safeguards, Security, and Emergency Operations Program..... 55

Research and Development 56

Total Program Spending 56

ENVIRONMENTAL PROTECTION AGENCY..... **57**

Office of Solid Waste and Emergency Response 58

On-Scene Coordinator (OSCs)..... 58

Current Budget 58

FEDERAL EMERGENCY MANAGEMENT AGENCY..... **59**

Response and Recovery Directorate 59

Preparedness, Training, and Exercises Directorate 60

United States Fire Administration 60

National Fire Academy and Emergency Management Institute..... 60

GENERAL SERVICES ADMINISTRATION..... **62**

DEPARTMENT OF HEALTH AND HUMAN SERVICES **63**

HOLOCAUST MEMORIAL MUSEUM **68**

DEPARTMENT OF THE INTERIOR **68**

DEPARTMENT OF JUSTICE AND FEDERAL BUREAU OF INVESTIGATION..... **69**

National Domestic Preparedness Office (NDPO)..... 70

Office for State and Local Domestic Preparedness Support (OSLDPS) 73

State Domestic Preparedness Equipment Program 73

Metropolitan Fire and Emergency Medical Services Training Program 74

OSLDPS Technical Assistance Activities..... 75

State Domestic Preparedness Equipment Program Needs Assessment and Strategy Development Initiative..... 76

TOPOFF Exercises..... 78

National Domestic Preparedness Consortium..... 78

Awareness of National Security Issues and Response Program (ANSIR)..... 79

National Institute of Justice..... 80

Total Department of Justice and FBI Funding 80

NATIONAL SECURITY COMMUNITY..... 81

NUCLEAR REGULATORY COMMISSION 82

SMITHSONIAN 83

DEPARTMENT OF STATE 83

Embassy Protection..... 84

Coordinator for Counterterrorism..... 85

 Foreign Emergency Support Teams (FEST) 85

 Technical Support Working Group..... 85

Bureau of Consular Affairs..... 86

Bureau of Diplomatic Security..... 86

Anti-Terrorism Assistance (ATA) Program 86

Total State Department Funding..... 87

DEPARTMENT OF TRANSPORTATION..... 87

DEPARTMENT OF TREASURY..... 89

US AID (NOW STATE DEPARTMENT) 90

DEPARTMENT OF VETERANS AFFAIRS 91

FEDERAL AND STATE/LOCAL COOPERATION 92

LIMITS TO COOPERATION..... 92

WEST NILE OUTBREAK..... 93

THE LESSONS FROM “JOINTNESS” 95

HOW OTHER NATIONS DEAL WITH THESE THREATS..... 98

LEADERSHIP AND MANAGEMENT..... 100

POLICIES AND STRATEGIES..... 101

CLAIMED RELIANCE ON CRIMINAL PROSECUTION AS THE MAJOR RESPONSE AND DETERRENT 102

OVERSIGHT, PLANNING, PROGRAMMING, AND BUDGETING 102

RESOURCE ALLOCATIONS ARE TARGETED AT LIKELY THREATS, NOT VULNERABILITIES: LIMITED CONCERN WITH WMD THREATS 103

LEARNING FROM FOREIGN COUNTRIES 104

COMMISSION RECOMMENDATIONS..... 105

Comparison of Major Recommendations 105

EVALUATING MAJOR RECOMMENDATIONS 106

Gilmore and Bremer Commissions: Executive Coordination and Management..... 107

Gilmore and Bremer Commissions: Congressional Oversight..... 108

Gilmore and Bremer Commissions: Intelligence Gathering and Sharing 109

Gilmore and Bremer Commissions: Clarify Authority and Command and Control - Giving the Department of Defense a Lead Role 110

Hart-Rudman and Bremer Commissions: Biological Pathogens, International Consensus against Terrorism, and Strengthening of Public Health Systems 112

Hart-Rudman and Bremer Commissions: Strengthening the International Consensus Against Terrorism and the International Convention for the Suppression of the Financing of Terrorism: 113

DIFFERENT RECOMMENDATION AREAS **114**

Gilmore Commission: Threat Assessments..... 114

Gilmore Commission: National Strategy for Domestic Preparedness and CBRN Terrorism Response 114

Gilmore Commission: Standardization of Legal Terms 117

Gilmore Commission: National Standards for Equipment 117

Bremer Commission: Treatment of Former and Future States of Concern..... 118

Bremer Commission: Targeting Terrorist Financial Resources..... 120

Bremer Commission: Monitoring Foreign Students..... 120

Bremer Commission: Liability Insurance..... 121

Bremer Commission: Realistic Exercises 121

GENERAL RECOMMENDATIONS..... **122**

PLANNING FOR BOTH HIGHER-PROBABILITY, LOWER-CONSEQUENCE AND LOW PROBABILITY/CATASTROPHIC EVENTS..... **123**

REACTING TO THE UNCERTAIN NATURE OF THE THREAT..... **126**

THE LACK OF “TRANSPARENCY” IN FEDERAL PROGRAMS..... **128**

FOCUSING ON PRIORITIES, PROGRAMS, AND TRADE-OFFS: CREATING EFFECTIVE PLANNING, PROGRAMMING, AND BUDGETING **130**

EFFECTIVE ACTION MUST BE BROAD-BASED AND SUB-OPTIMIZE EFFICIENTLY **134**

MANAGING RESEARCH AND DEVELOPMENT, RATHER THAN TREATING CBRN AS A WISH LIST AND SLUSH FUND..... **137**

LOOKING BEYOND CBRN: **137**

DEALING WITH ALL MEDICAL RISKS AND COSTS **137**

HOMELAND DEFENSE AND/OR LAW ENFORCEMENT **139**

RULE OF LAW, HUMAN RIGHTS, ASYMMETRIC WARFARE, HIGH LEVELS OF ATTACK AND “NEW PARADIGMS” **140**

List of Charts, Tables, and Figures

Table Thirteen	15
OMB Estimate of Total Federal Spending on Terrorism (As of 6/2000).....	15
Chart Ten.....	16
Federal Spending on Terrorism, WMD, and CIP by Category: FY1998-FY2001	16
Chart Eleven	17
Distribution of Federal Spending on Terrorism, WMD, and CIP by Category: FY2001.....	17
Chart Twelve	18
Federal Spending on Terrorism, WMD, and CIP by Agency: FY1998-FY2001 – Part One	18
Chart Twelve	19
Federal Spending on Terrorism, WMD, and CIP by Agency: FY1998-FY2001 – Part Two.....	19
Chart Thirteen.....	23
Federal Spending on Terrorism and WMD by Category: FY1998-FY2001	23
Chart Fourteen.....	24
Core Federal Spending on Terrorism and WMD by Activity: FY1998-FY2001:	24
Chart Fifteen.....	25
Distribution of Core Federal Spending on Terrorism and WMD by Activity: FY2001.....	25
Chart Sixteen	30
Federal Spending on WMD Preparedness by Activity: FY1998-FY20001	30

Chart Seventeen..... 31

Federal Spending on WMD by Agency: FY1998-FY2001 – Part One..... 31

Chart Seventeen..... 32

Federal Spending on WMD by Agency: FY1998-FY2001 – Part Two..... 32

Table Fourteen..... 34

OMB Estimate of Federal Spending on Terrorism by Agency (As of 6/2000) 34

Table Fifteen..... 40

Department of Agriculture Spending for Combating Terrorism and WMD Preparedness 40

Table Sixteen..... 42

Department of Commerce Spending for Combating Terrorism and WMD Preparedness 42

Table Seventeen:..... 45

First Responders Trained Through Domestic Preparedness Program (from program’s inception in
fiscal year 1997 through fiscal year 1999) 45

Table Eighteen..... 56

Department of Energy Spending for Combating Terrorism and WMD Preparedness..... 56

Table Nineteen..... 58

Department of Energy Spending for Combating Terrorism and WMD Preparedness..... 58

Table Twenty..... 62

Federal Emergency Management Agency Spending for Combating Terrorism and WMD

Preparedness 62

Table Twenty-One 62

General Services Administration Spending for Combating Terrorism and WMD Preparedness. 62

Table Twenty-Two 67

Department of Health and Human Services Spending for Combating Terrorism and WMD
Preparedness 67

Table Twenty-Three 68

Holocaust Memorial Museum Spending for Combating Terrorism and WMD Preparedness 68

Table Twenty-Four 68

Department of the Interior Spending for Combating Terrorism and WMD Preparedness 68

Table Twenty-Five..... 81

Department of Justice Spending for Combating Terrorism and WMD Preparedness..... 81

Table Twenty-Six 82

National Security Community, including the Department of Defense, Spending for Combating
Terrorism and WMD Preparedness..... 82

Table Twenty-Seven 83

Nuclear Regulatory Commission Spending for Combating Terrorism and WMD Preparedness. 83

Table Twenty-Eight 83

Smithsonian Spending for Combating Terrorism and WMD Preparedness 83

Table Twenty-Nine 87

Department of State Spending for Combating Terrorism and WMD Preparedness 87

Table Thirty 88

Department of Transportation Spending for Combating Terrorism and WMD Preparedness 88

Table Thirty-One 89

Department of Treasury Spending for Combating Terrorism and WMD Preparedness 89

Table Thirty-Two..... 90

US AID Spending for Combating Terrorism and WMD Preparedness..... 90

Table Thirty-Four 91

Department of Veterans Affairs Spending for Combating Terrorism and WMD Preparedness... 91

Table Thirty-Five..... 106

Comparison of Commission Recommendations 106

US Government Efforts to Create a Homeland Defense Capability

The US has followed the same basic principles in dealing with terrorism since the 1970s: Make no concessions to terrorists, pressure state sponsors of terrorism, and apply the rule of law to terrorists as criminals. This U.S. policy on terrorism became formalized in 1986, when the Reagan administration's issued National Security Decision Directive 207 (NSDD 207).

This shift to a more formal policy came as the result of the findings of the 1985 Vice President's Task Force on Terrorism, which highlighted the need for improved, centralized interagency coordination of the significant federal assets to respond to terrorist incidents. NSDD 207 reaffirmed the lead agency responsibilities of past policy. The State Department was responsible for international terrorism policy, procedures, and programs, and the FBI was responsible for dealing with domestic terrorist acts while acting through the Department of Justice.

The US response to the potential threats from covert attacks by state actors, their proxies, or independent extremists and terrorists has, however, changed significantly since the mid-1990s. The next major change in policy came in the National Defense Authorization Act for Fiscal Year 1994, Public Law No.103-160, Section 1703 (50 USC 1522). This law mandated the coordination and integration of all Department of Defense chemical and biological (CB) defense programs. As part of this coordination and integration, the Secretary of Defense was directed to submit an assessment and a description of plans to improve readiness to survive, fight and win in a nuclear, biological and chemical (NBC) contaminated environment. Since that time, 50 USC 1522 has provided the essential authority to ensure the elimination of unnecessarily redundant programs, focusing funds on DoD and program priorities, and enhancing readiness.

Key Presidential Decision Directives and Legislation Affecting the Federal Response

The bombing of the federal building in Oklahoma City led to the issuance of Presidential

Decision Directive 39 (PDD-39) in June 1995. PDD-39 built on the previous directive and contained three key elements of a national strategy for combating terrorism: (1) reduce vulnerabilities to terrorist attacks and prevent and deter terrorist acts before they occur; (2) respond to terrorist acts that do occur—crisis management—and apprehend and punish terrorists; and (3) manage the consequences of terrorist acts, including restoring capabilities to protect public health and safety and essential government services and providing emergency relief. This directive also further elaborates on agencies' roles and responsibilities and some specific measures to be taken regarding each element of the strategy.⁶

These policies have since been further developed by two key Presidential Decision Directives, PDD-62 and PDD-63.

- PDD-62 reaffirmed the basic principles of PDD-39, but clarified and reinforced the specific missions of the US agencies charged with defeating and defending against terrorism, and created a new and more systematic federal approach to fighting the emerging threat posed by weapons of mass destruction (WMD). This includes programs to deter terrorist incidents involving chemical, biological, radiological, and nuclear weapons, and to manage the consequences if such incidents should occur.
- PDD-63 called for a national effort to assure the security of critical infrastructure. It covers both critical infrastructure protection and cyber crime, and the security of both government and private sector infrastructure to ensure national security, national economic security, and public health and safety.

As a result of PDD-39 and PDD-62, the federal response to domestic incidents is now divided into crisis management, led respectively by the FBI, and consequence management led by FEMA. The GAO reports that,⁷

Two Presidential Decisions Directives—number 39 issued in June 1995 and number 62 issued in May 1998—define U.S. policy to combat terrorism. These presidential directives and implementing guidance divide the federal response to terrorist attacks into two categories—crisis management and consequence management. Crisis management includes efforts to stop a terrorist attack, arrest terrorists, and gather evidence for criminal prosecution. Consequence management includes efforts to provide medical treatment and emergency services, evacuate people from dangerous areas, and restore government services. The presidential directives also organize federal efforts to combat terrorism along a lead agency concept. The

Department of Justice, through the Federal Bureau of Investigation (FBI), is the lead federal agency for crisis management of domestic terrorist incidents. For managing the consequences of domestic terrorist incidents, state and local authorities are primarily responsible. The Federal Emergency Management Agency (FEMA) is the lead federal agency for consequence management if state or local authorities request federal assistance.

New legislation has also shaped US policy. “The Defense Against Weapons of Mass Destruction Act,” contained in the National Defense Authorization Act for Fiscal Year 1997 (title XIV of P.L. 104-201, Sept. 23, 1996), established the Nunn-Lugar-Domenici Domestic Preparedness Program. This act made the Department of Defense the lead federal agency for implementing the program, and is to work in cooperation with the FBI, the Department of Energy, the Environmental Protection Agency, the Department of Health and Human Services, and the Federal Emergency Management Agency.⁸

The US gave significantly higher priority to the full range of threats posed by weapons of mass destruction. On June 8, 1998, the President forwarded to Congress a fiscal year 1999 budget amendment that included a proposal to (1) build for the first time civilian stockpile of antidotes and vaccines to respond to a large-scale biological or chemical attack, (2) improve the public health surveillance system to detect biological or chemical agents rapidly and analyze resulting disease outbreaks, (3) provide specialized equipment and training to states and localities for responding to a biological or chemical incident, and (4) expand the National Institutes of Health's research into vaccines and therapies.

The Omnibus Consolidated and Emergency Supplemental Appropriations Act (P.L. 105- 277) included \$51 million for the Centers for Disease Control and Prevention to begin developing a pharmaceutical and vaccine stockpile for civilian populations. The act also required that HHS submit an operating plan to the House and Senate Committees on Appropriations before obligating the funds. The fiscal year 2000 request for HHS' bioterrorism initiative is \$230 million, including \$52 million for the Centers for Disease Control and Prevention to continue procurement of a national stockpile.

Important legislation is also pending. On April 6, 2000, H.R. 4210 was introduced to the House Committee on Transportation and Infrastructure, Subcommittee on Oversight,

Investigations, and Emergency Management. The bill would create the Office of Terrorism Preparedness within the Executive Office of the President. Duties of the Office would include: establishing, overseeing, and coordinating federal policies and priorities for state and local preparedness; publishing a Domestic Terrorism Preparedness Plan and an annual strategy for achieving the plan; reviewing state and local preparedness and creating voluntary minimum standards.

It is unclear, however, that this legislation will be enacted. The GAO has stated that the Office would have overlapping duties with the DOJ's National Domestic Preparedness Office, which is administered by the FBI:⁹

As currently proposed in the bill, the Office may overlap with some functions to be performed by the existing National Domestic Preparedness Office. The Attorney General established this office within the Department of Justice to be responsible for interagency leadership and coordination of federal efforts to provide assistance for state and local governments to prepare for terrorist incidents involving weapons of mass destruction. As an example of potential duplication, the National Domestic Preparedness Office recently issued a "blueprint" for federal assistance, which is analogous to the new Office of Terrorism Preparedness function to prepare a national plan and strategy.

In addition, the bill would limit the scope of the new Office of Terrorism Preparedness to incidents involving weapons of mass destruction. According to intelligence and law enforcement officials, terrorists are least likely to use these types of weapons. The Subcommittee may want to consider authorizing the Office of Terrorism Preparedness to assist state and local governments to prepare for both weapons of mass destruction and the more likely threat of conventional explosives.

Changes in the Structure of the Federal Effort

The number of federal players involved in combating the threats posed by state actors, their proxies, or independent extremists and terrorists has increased substantially since PD-39 was issued in June 1995. The GAO has reported that the number of players now involves more than 40 federal agencies, bureaus, and offices in combating terrorism. For example, Department of Agriculture representatives now attend counterterrorism crisis response exercise planning functions. The U.S. Army's Director of Military Support has created a new office to implement the Nunn-Lugar-Domenici Domestic Preparedness Program, which has a new mission of training U.S. cities' emergency response personnel to deal with terrorist incidents using chemical and biological WMD. It and plans to create another office to integrate another new player-the National Guard and Reserve-into the terrorism consequence management area.

Similarly, the National Guard and Reserve has established 10 WMD Civil Support Teams, formerly known as Rapid Assessment and Initial Detection (RAID) teams, throughout the country and will have a total of 27 teams by early 2001.¹⁰ The U.S. Marine Corps has established the Chemical Biological Incident Response Force. Further, the Department of Energy has redesigned its long-standing Nuclear Emergency Search Team into various Joint Technical Operations Teams and other teams. At least one Department of Energy laboratory is offering consequence management services for chemical and biological as well as nuclear incidents. And the Public Health Service is in the process of establishing 120 Metropolitan Medical Strike Teams throughout the country in addition to 3 deployable "national asset" National Medical Response Teams and existing Disaster Medical Assistance Teams. There are many more examples of new players in the terrorism arena.

The Growth of the Federal Effort

These rapid changes in the way the Federal government deals with terrorism have been accompanied by an even more rapid growth in federal spending which has created major problems in tracking and assessing the Federal effort to deal with terrorism. The reporting on the key programs contributing to homeland defense is currently a definitional and statistical nightmare, and while the federal effort reflects steadily improving coordination, there are still bureaucratic rivalries, duplicative programs, and differing priorities.

What is clear, is that major increases are taking place in the federal budget. The GAO reported in 1997 that seven key federal agencies spent more than an estimated \$6.5 billion on federal efforts to combat terrorism, excluding classified programs and activities in FY 1997. Some key agencies' spending on terrorism-related programs had increased dramatically. For example, FBI terrorism-related funding and staff-level authorizations tripled between FY1995 and FY1997, and Federal Aviation Administration spending to combat terrorism also tripled.¹¹

Office of Management and Budget (OMB) reporting to the Congress on enacted and requested terrorism-related funding for fiscal years 1998 and 1999, stated that more than 17 agencies then had classified and unclassified programs. These agencies were authorized a total of

\$6.5 billion for fiscal year 1998, and \$6.7 billion for fiscal year 1999. OMB's figures are lower than the GAO's were for fiscal year 1997, but different definitions and interpretations of how to attribute terrorism-related spending in broader accounts can cause a difference of billions of dollars.¹² For example, the OMB) later reported that actual spending in 1998 totaled \$7.658 billion consisting of \$5.871 billion for combating terrorism, \$.645 billion for combating weapons of mass destruction and \$1.142 billion for critical infrastructure protection.¹³

The FY2000 Program

The White House issued a more detailed "guesstimate" as to the size federal spending in submitting its FY2000 budget request. President Clinton's FY 2000 requested budget for counterterrorism:¹⁴

In his FY00 budget request, President Clinton will propose \$10 billion to address "terrorism and terrorist-emerging tools" including nearly \$1.4 billion in defense against chemical and biological terrorism. A further \$1.46 billion will be requested for critical infrastructure protection, \$231 million for nonproliferation and transnational antiterrorism efforts, and \$230 million for bioterrorism programs at the Department of Health and Human Services.

The White House also provided the following breakdown of how the FY2000 program was allocated to different activities:¹⁵

- *Funding for Domestic Preparedness and Critical Infrastructure Protection:* The President's Fiscal Year 2000 budget includes requests for \$2.849 billion for critical infrastructure protection, computer security, and domestic preparedness against a weapons of mass destruction attack. The budget request also proposed \$7.162 billion for conventional counter-terrorism security programs.
- *Domestic Preparedness against Weapons of Mass Destruction:* In May 1999 the President proposed adding \$300 million for a new weapons of mass destruction domestic preparedness program. As a result, the 1999 enacted level was \$1.281 billion. The President's FY 2000 funding request for countering the threat of terrorist use of weapons of mass destruction continues and expands the program to \$1.385 billion. The FY 2000 request included increases of \$30 million above the previous level for research into new vaccines and medicines, an additional \$15 million to fund Public Health Surveillance to detect an attack, and an additional \$13 million to create new metropolitan medical response teams. Highlights of the FY 2000 budget included:
 - \$52 million to continue procurement of a national stockpile of specialized medicines to protect the civilian population.
 - \$611 million for training and equipping emergency personnel in U.S. cities, planning and exercising for weapons of mass destruction contingencies and strengthening public health infrastructure.
 - \$206 million to protect U.S. government facilities, \$381 million for research and development, including pathogen genome sequencing, vaccines, new therapies, detection and diagnosis,

decontamination, and disposition of nuclear material.

- *Critical Infrastructure Protection and Computer Security:* The President's FY 2000 request included \$1.464 billion for protection of critical infrastructure and computer security. This represented a 40% increase in the two budget years since the President created the Critical Infrastructure Protection Commission. The highlights of this program included:
 - Critical Infrastructure Applied Research Initiative (\$500 million).
 - Intrusion and Detection Systems: In addition to ongoing Department of Defense funding, \$2 million will be spent to design and evaluate a similar system for other Federal agencies.
 - Information Sharing and Analysis Centers (ISACs): As part of the public-private partnership, we will provide \$8 million to support the initial establishment of ISACs.
- *Cyber Corps:* This program addresses the shortage of highly skilled computer science expertise in the government and enable agencies to recruit a cadre of experts to respond to attacks on computer networks. It will use existing personnel flexibilities, scholarship and financial assistance programs, and \$3 million to examine new scholarship programs to retrain, retain and recruit computer science students.
- *Counter-terrorism Security:* In addition to the programs above, the President's FY 2000 budget request for all anti-terrorism and counter-terrorism programs was \$8.547 billion, a 12% increase over the FY 1999 enacted level and an 18% increase over FY1998.
- The President also requested a supplemental appropriation in FY 1999 of \$2.064 billion after the Africa bombings. This included \$1.4 billion to provide additional security measures to diplomatic and consular facilities and rebuild the two embassies destroyed in Dar es Salaam and Nairobi.

The FY2001 Program

An OMB estimate of FY2001 federal spending on counterterrorism indicates that spending will total \$9.3 billion for FY 2001, a 43% increase. Within these amounts, WMD preparedness spending has increased from \$645 million in FY1998 to \$1.55 billion in FY2001, a 141% increase.¹⁶ . According to the GAO, however, the requested FY 2001 budget for terrorism as of April 6, 2000 was \$11.117 billion. \$7.538 billion was for combating terrorism, \$1.552 billion for combating WMD, and \$2.027 for critical infrastructure protection.¹⁷

In addition to reporting on the increase in the number of programs, we have testified twice on the rapid increase in federal funding to combat terrorism. The Office of Management and Budget (OMB) reported 1998 actual spending at \$7.658 billion consisting of \$5.871 billion for combating terrorism, \$.645 billion for combating weapons of mass destruction and \$1.142 billion for critical infrastructure protection. The President's budget request for fiscal year 2001 totals \$11.117 billion consisting of \$7.538 billion for combating terrorism, \$1.552 billion for combating weapons of mass destruction and \$2.027 billion for critical infrastructure protection. As proposed in the President's budget request, total funding would increase about 45 percent from 1998 to 2001, with component increases of about 28 percent for combating terrorism, about 140 percent for combating weapons of mass destruction, and about 77 percent for critical infrastructure protection. As noted in our earlier work, funding has increased dramatically at the Departments of Health and Human Services, Justice, and at the FBI.

Part of the problem in estimating federal expenditures is that they are subject to constant change. For example, the President requested an additional \$300 million for counterterrorism, on May 17, 2000,. The Department of Justice will receive an additional \$89 million, the Department of Treasury \$87 million, and other agencies will receive \$159 million to fund extra personnel, equipment, joint operations, and infrastructure improvements.¹⁸ The White House described these new program initiatives are follows:

President Clinton announced a plan today to invest an additional \$300 million in critical programs to strengthen the Nation's counterterrorism efforts.

The funding would enhance the Federal government's work to deter and detect terrorist activity, applying lessons learned from the counterterrorism effort undertaken during Millennium celebration events. The request proposes \$89 million for the Department of Justice and \$87 million for the Department of the Treasury to fund extra personnel, new equipment, and additional joint operations and infrastructure improvements. An additional \$159 million is proposed for other agencies to support these efforts.

Highlights of the initiative include:

- Increasing the number of Joint Terrorism Task Forces located throughout the United States. The Task Forces were established to integrate the resources and expertise of the law enforcement authorities of the Federal Bureau of Investigation (FBI), the Immigration and Naturalization Service (INS), the U.S. Customs Service, ATF, Secret Service and state and local law enforcement.
- Improving monitoring on the northern border with secure communications equipment and advanced monitoring equipment, including high resolution day and night camera technology.
- Expanding INS forensic capabilities at the government's federal crime lab dedicated to the forensic examination of potentially fraudulent travel documents.
- Supporting the establishment of a new interagency National Terrorist Asset Tracking Center to analyze the financing of terrorist organizations and expand the Office of Foreign Asset Control at the Department of the Treasury.
- Increasing the number of Department of Justice prosecutors and legal staff to support the prosecution of terrorists.
- Increasing the Department of the Treasury's Counterterrorism Fund that was established to cover costs associated with efforts to counter, investigate or prosecute domestic or international terrorism.

Today's request builds on activities already being undertaken. In FY 2000, reprogramming funds the majority of the package. A fully offset FY 2001 budget amendment will be submitted to Congress.

The Details of the Federal Effort

The most accurate detailed estimate of the federal efforts is the work done by OMB in response to a requirement in Section 1051 of the Fiscal Year 1998 National Defense Authorization Act (P.L.105-85, which requires the Administration to provide information on Executive branch funding efforts to combat terrorism. Subsequent legislation (Section 1403 of

P.L.105-261) requires an annex to this report that shows spending on domestic preparedness.

Table Thirteen, and Charts Ten to Twelve, show the patterns in total federal spending on the threats posed by state actors, their proxies, or independent extremists and terrorists. According to the data in this table, the total funding for all forms of federal action dealing with terrorism rose from \$8.3 billion in FY1998 to \$12.893 billion in FY2000. This is a rise of 55%. The total funding designed specifically to deal with the threat from WMD rose from \$645 million in FY1998 to \$1.554,96 million in FY2000, a rise of 240%. The rise in critical infrastructure protection was from \$1.142 million to \$2,027.25 million, a rise of 78%. These figures reveal an extremely rapid rate of growth in new program areas.

The Changing Patterns in Federal Spending

A review of Table Thirteen, and Charts Ten to Twelve, also reveals the following more detailed patterns in federal spending during FY1998-FY2001:

- The federal effort is broadly distributed among 23 major Federal departments and agencies. The largest efforts are carried out in the national security area, which includes the Department of Defense and intelligence agencies, and which received slightly over 51% of the total funding programmed for FY2001. The second largest recipient has been the State Department, largely because of the high cost of improving physical security at US embassies.
- The “civil” effort reflects a similar rise in spending on physical protection, which is a key reason for the rise in spending by agencies like the Department of Energy, GSA, Transportation and Energy. There has, however, been an important increase in funding for law enforcement and the funding for the Department of Justice rose by nearly 50% during FY1998-FY2000.
- Most federal spending on terrorism is not directly related to either the threat posed by weapons of mass destruction (14%) or to critical infrastructure protection (18%). Spending on other activities totaled 68% in the FY2001 budget request.

- The main increases in the overall federal effort to combat terrorism took place in funding improved physical protection for government facilities and employees (\$2.9 billion to \$4.3 billion), in preparing for and responding to terrorist acts (\$418 million to \$947 million), and in research and development (\$403 million to \$813 million.)
- In contrast, law enforcement – the traditional focus of the federal effort – rose from \$2.7 billion to \$3.0 billion. This latter rise was still quite significant, but law enforcement spending dropped from 41% of all spending in FY1998 to 32% in FY2001.
- The rise in spending to directly counter the threat of the use of WMD spending, in contrast, did not involve major increases in spending on physical protection for either government or the national populace. It did lead to a near doubling of law enforcement spending, and massive increases in spending on preparing for and responding to WMD terrorism (\$155 million to \$633 million), and on research and development (\$240 million to \$590 million.)
- The growth in the CIP effort was more broadly distributed by category, although the outreach each to the private sector trebled (\$103 million to \$328 million), and federal efforts in education and intrusion monitoring and response more than trebled.

It is important to note that these totals include all federal spending and not simply efforts to react to the threat posed to the US homeland. As a result, they give a somewhat misleading view of how the US is attempting to defend against the threat posed by state actors, their proxies, or independent extremists and terrorists. For example, CIP or critical infrastructure protection is often excluded from the analysis of US counter-terrorism efforts and includes different threats such as information warfare. It is also discussed separately, in depth, in a different section of this report.

At the same time, any effort to break out federal spending into neat categories presents major problems in categorization. While spending on efforts to directly deal with the threat of state actors, their proxies, or independent extremists and terrorists using weapons of mass

destruction is only a relatively small portion of total federal spending, much of the spending in other areas improves the quality of law enforcement and offers some protection against the use of such weapons. There are also broad categories of federal spending, like spending on national health care, the offensive and deterrent capabilities of the Department of Defense, and the civil emergency capabilities of agencies like FEMA which have a major impact both in countering terrorism and in consequence management.

Planning and Programming the Overall Federal Effort

This latter point is particularly important because it reflects the serious real-world limits on how efficiently the federal government can hope to be in allocating resources. The initial increases in funding produced a near feeding frenzy as departments and agencies competed for major new sources of funding. As the GAO noted in a 1998 report,¹⁹

....more money is being spent to combat terrorism without any assurance of whether it is focused on the right programs or in the right amounts.... key interagency management functions were not clearly required or performed. For example, neither the National Security Council nor the Office of Management and Budget (OMB) was required to regularly collect, aggregate, and review funding and spending data relative to combating terrorism on a crosscutting, government-wide basis. Further, neither agency had established funding priorities for terrorism-related programs within or across agencies' individual budgets or ensured that individual agencies' stated requirements had been validated against threat and risk criteria before budget requests were submitted to the Congress. Because government-wide priorities have not been established and funding requirements have not necessarily been validated based on an analytically sound assessment of the threat and risk of terrorist attack, there is no basis to have a reasonable assurance that funds are being spent on the right programs in the right amounts and that unnecessary program and funding duplication, overlap, misallocation, fragmentation, and gaps have not occurred.

The Federal government has since made major efforts to improve its coordination, planning, programming, budgeting, and coordination efforts. The National Defense Authorization Act for Fiscal Year 1998 (P.L. 105-85, Nov. 18, 1997) required OMB to establish a reporting system for executive agencies on the budgeting and expenditure of funds for programs and activities to combat terrorism. OMB is also to collect the information and the President is to report the results to the Congress annually, including information on the programs and activities, priorities, and duplication of efforts in implementing the programs.²⁰ OMB made its first report in 1998, and the reports that have followed reflect a steadily improving effort to ensure the coordination of efforts within and between federal agencies.

The Clinton Administration has made other efforts to develop an integrated federal approach to dealing with the threat posed by state actors, their proxies, or independent extremists and terrorists. As part of this effort, the Administration has developed more specific guidance for Federal Agencies in two documents: A “Five Year Interagency Counter-Terrorism Plan,” and a “National Plan for Infrastructure Systems Protection.”

The Administration also has tasked the National Security Council (NSC) with leading the interagency working groups involved with terrorism, the threat from weapons of mass destruction, and critical infrastructure protection, and with ensuring that the policies are properly prioritized and executed in Agency programs and budget. An annual review by the NSC is intended to ensure that agencies structure their activities efficiently and effectively and to develop a comprehensive and crosscutting national program.

There are obvious limits to what these efforts can accomplish. While it is easy to talk about creating a coordinated federal plan, and efficiently programming resources accordingly, the sheer scale of the current federal effort, its rapid recent growth, and agency efforts to compete for new resources make such efforts largely impossible. This becomes all too clear in the more detailed analyses of agency and departmental efforts that follows, and the problem is further complicated by the problem of determining with proper federal interface with state and local governments, and the private and civil sectors. For example, response capabilities for given types of attack differ so much by urban area that it becomes extremely difficult for agencies to develop a common approach that can react to these differences.

Both the Gilmore Commission and GAO have found that serious problems still exist in the coordination effort, and that the federal government still has a long way to go in developing a well-coordinated and effective program, and it is far from clear that it can do so until the nature of future threats is far clearer than it is today. The GAO testified in June 2000 that,²¹

One of the major deficiencies in federal efforts to combat terrorism is the lack of linkage between the terrorist threat, a national strategy, and agency resources. Much of the federal efforts to combat terrorism have been based upon vulnerabilities rather than an analysis of credible threats. For example, agencies have used and are still using improbable “worst case scenarios” to plan and develop programs. While there has been a major effort to develop a national strategy, to date the strategy does not include a clear desired outcome to be achieved. Resources to combat terrorism have increased in terms of both budgets and

programs. These increased resources have not been clearly linked to a threat analysis and we have found cases where some agency initiatives appear at odds with the judgments of the intelligence community.

This situation also creates the potential for agencies to develop their own programs without adequate coordination, leaving the potential for gaps and/or duplication. Efforts to track and coordinate federal spending across agencies have started, but they have only begun to tackle the important task of prioritizing programs.

We have recommended, and the executive branch has agreed to, conducting threat and risk assessments to improve federal efforts to combat terrorism. Specifically, such assessments could be an important step to develop a national strategy and to target resources. The federal government cannot prepare for CBRN incidents on its own. Several improvements are also warranted in intergovernmental relations between federal, state and local governments. For example, we found that federal agencies developed some of their assistance programs without coordinating them with existing state and local emergency management structures.

In addition, the multitude of federal assistance programs has led to confusion on the part of state and local officials. One step to improve coordination and reduce confusion has been the creation of the National Domestic Preparedness Office within the Department of Justice to provide "one stop shopping" to state and local officials in need of assistance. This office has recently prepared a draft plan on how it will provide assistance.

Another intergovernmental issue requiring resolution is the matter of command and control at the site of a terrorist incident. Roles of the federal government versus the state and local governments need to be further clarified to prevent confusion. The federal government is making some progress in addressing these command and control issues through exercises. Federal exercises, in contrast to earlier years, are now practicing crisis and consequence management simultaneously and including state and local participation.

Finally, the Gilmore Panel report found many of the same problems that we have been reporting on, such as the need for (1) more rigorous analyses of the threat, (2) better management of federal programs, (3) improvements in coordination with state and local officials, and (4) a national strategy to combat terrorism. In addition, the report raises some interesting points for Congress to consider in the future as it oversees federal programs to combat terrorism.

Three are deeper conceptual problems that go far beyond these criticisms. As has already been discussed in depth, the range of threats simply are not predictable enough for given agencies to attempt more than a constantly evolving and uncertain process of suboptimization. Put differently, departments and agencies must often do what they can to improve their capabilities at the margin, rather than seek to create building blocks in some kind of coherent homeland defense.

Such efforts may not, however, have great impact on US ability to defend against nuclear and highly lethal biological attacks. They may give the impression of defense and response capability, but the end result may not be able to cope with very high levels of attack, which may well force all levels of government to improvise radically with little warning and under intense

pressure. Marginal improvements in resources may fail to deal with response requirements or be impossible to allocate efficiently within the time windows required. This is particularly true because there currently seems to be little practical understanding of what a “worst case” or high level attack would really do, and how uncertain its effects now are.

Finally, the present coordination effort only focuses on those federal programs identified as being directly designed to defend or respond to the threat state actors, their proxies, or independent extremists and terrorists pose to the American homeland. This is almost certainly *not* the right way to will prove to create the most effective overall program to actually improve Homeland defense. Such a program must explicitly consider the offensive, deterrent, and retaliatory capabilities of US military and intelligence agencies, and the role their activities overseas can play in creating an effective deterrent to foreign attacks on the US.

Table ThirteenOMB Estimate of Total Federal Spending on Terrorism (As of 6/2000)

(Government Spending for Combating Terrorism, WMD and Critical Infrastructure Protection in Current \$US Billions)

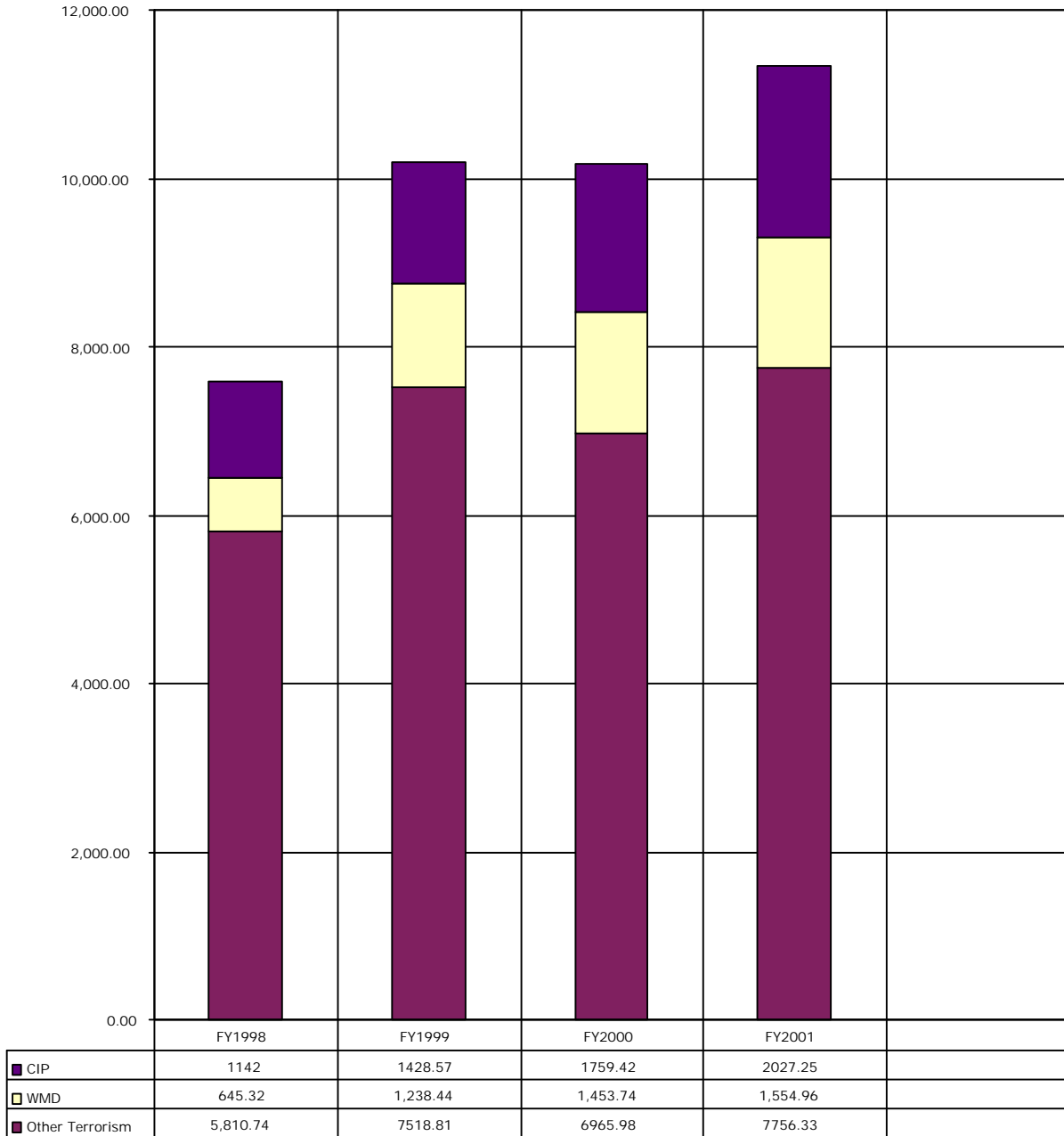
	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Federal Government</i>	<i>8,303.40</i>	<i>11,424.26</i>	<i>11,632.88</i>	<i>12,893.50</i>
<i>Combat Terrorism</i>	<i>6,516.08</i>	<i>8,757.25</i>	<i>8,419.72</i>	<i>9,311.29</i>
Law Enforcement and Investigative Activities	2,654.72	2,686.77	2,820.04	3,025.51
Physical Security of Government Facilities and Employees	2,893.72	4,356.44	3,637.49	4,259.24
Physical Security of National Populace	146.66	256.83	249.86	266.76
Preparing for and Responding to Terrorist Acts	417.84	930.21	984.41	947.00
Research and Development	403.14	527.01	727.91	812.79
<i>WMD Preparedness</i>	<i>645.32</i>	<i>1,238.44</i>	<i>1,453.74</i>	<i>1,554.96</i>
Law Enforcement and Investigative Activities	71.82	102.30	93.77	142.53
Physical Security of Government	175.09	199.35	200.58	185.41
Physical Security of National Populace	3.39	3.83	3.61	3.62
Preparing for and Responding to WMD Terrorism	155.26	564.20	618.74	633.48
Research and Development	239.75	368.76	537.04	589.92
<i>Critical Infrastructure Protection</i>	<i>1,142.00</i>	<i>1,428.57</i>	<i>1,759.42</i>	<i>2,027.25</i>
Federal Infrastructure Protection	1,038.79	1,278.91	1,584.26	1,699.03
Education and Training	37.54	48.50	79.45	105.00
Intrusion Monitoring and Response	127.63	186.27	213.37	249.27
Legislative Initiatives and Legal Issues	0.12	0.20	0.20	0.23
Multiple Program Areas	242.45	282.72	397.21	369.05
Reconstitution	26.19	30.18	16.29	5.64
System Protection	533.32	631.13	710.23	740.69
Threat/Vulnerability/Risk Assessments	71.56	99.92	167.51	229.15
CIP Assistance/Outreach to Private Sector	103.21	149.66	175.16	328.22
Education and Training	1.14	1.60	1.60	2.50
Intrusion Monitoring and Response	3.75	5.20	4.70	6.62
Legislative Initiatives and Legal Issues	1.58	2.60	2.60	3.60
Multiple Program Areas	37.99	70.78	61.14	133.92
Public Awareness/Outreach	0.00	0.00	2.30	3.10
Reconstitution	0.00	0.00	0.00	2.13
System Protection	37.31	43.15	57.05	72.14
Threat/Vulnerability/Risk Assessments	21.44	26.33	45.78	104.14

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Chart Ten

Federal Spending on Terrorism, WMD, and CIP by Category: FY1998-FY2001
(Current \$US Millions)

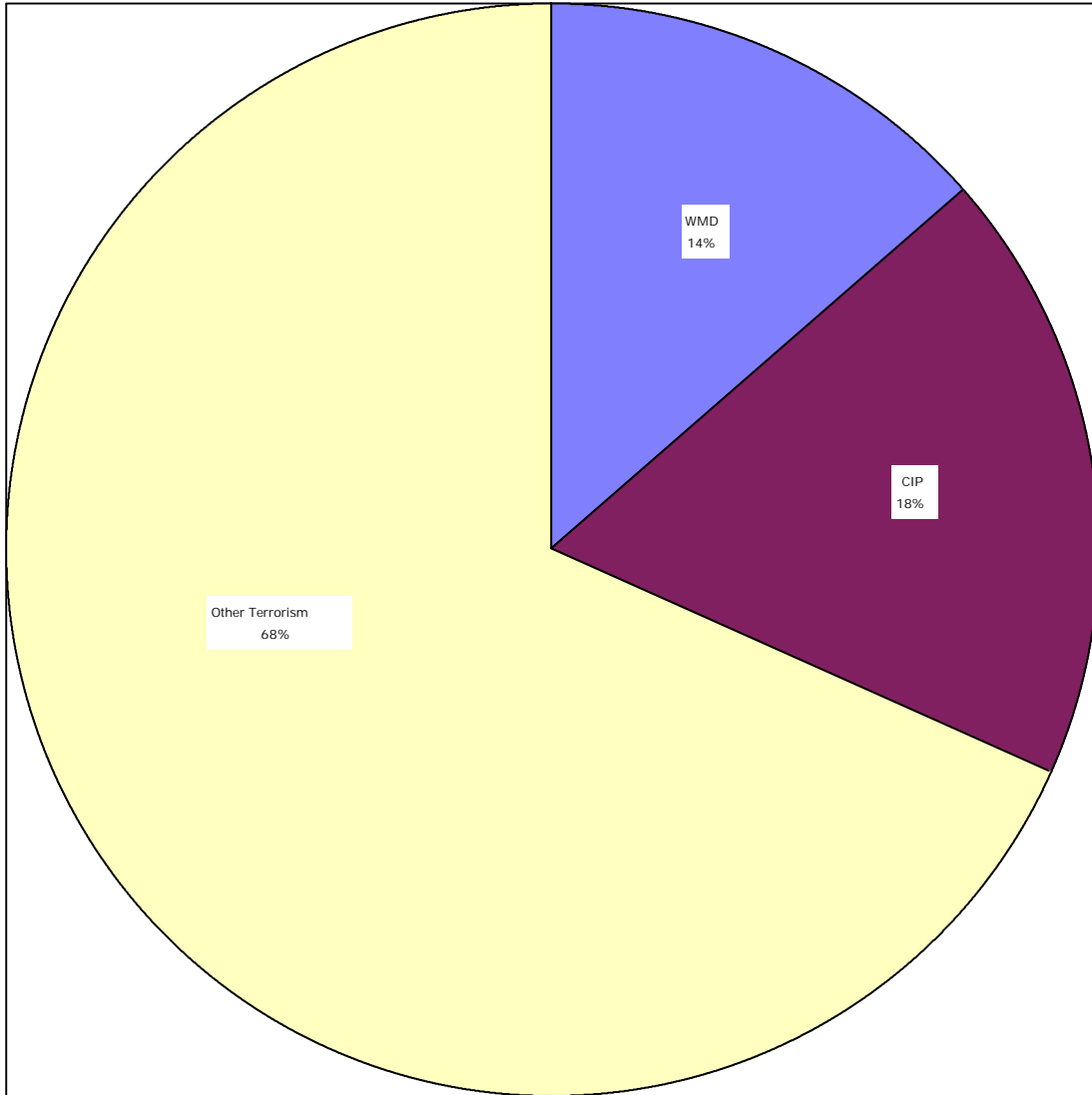


Source: Adapted by Anthony H. Cordesman from data provided by ACDA on April 1, 1999. Belarus and Kazakhstan report zero in every category.

Chart Eleven

Distribution of Federal Spending on Terrorism, WMD, and CIP by Category: FY2001

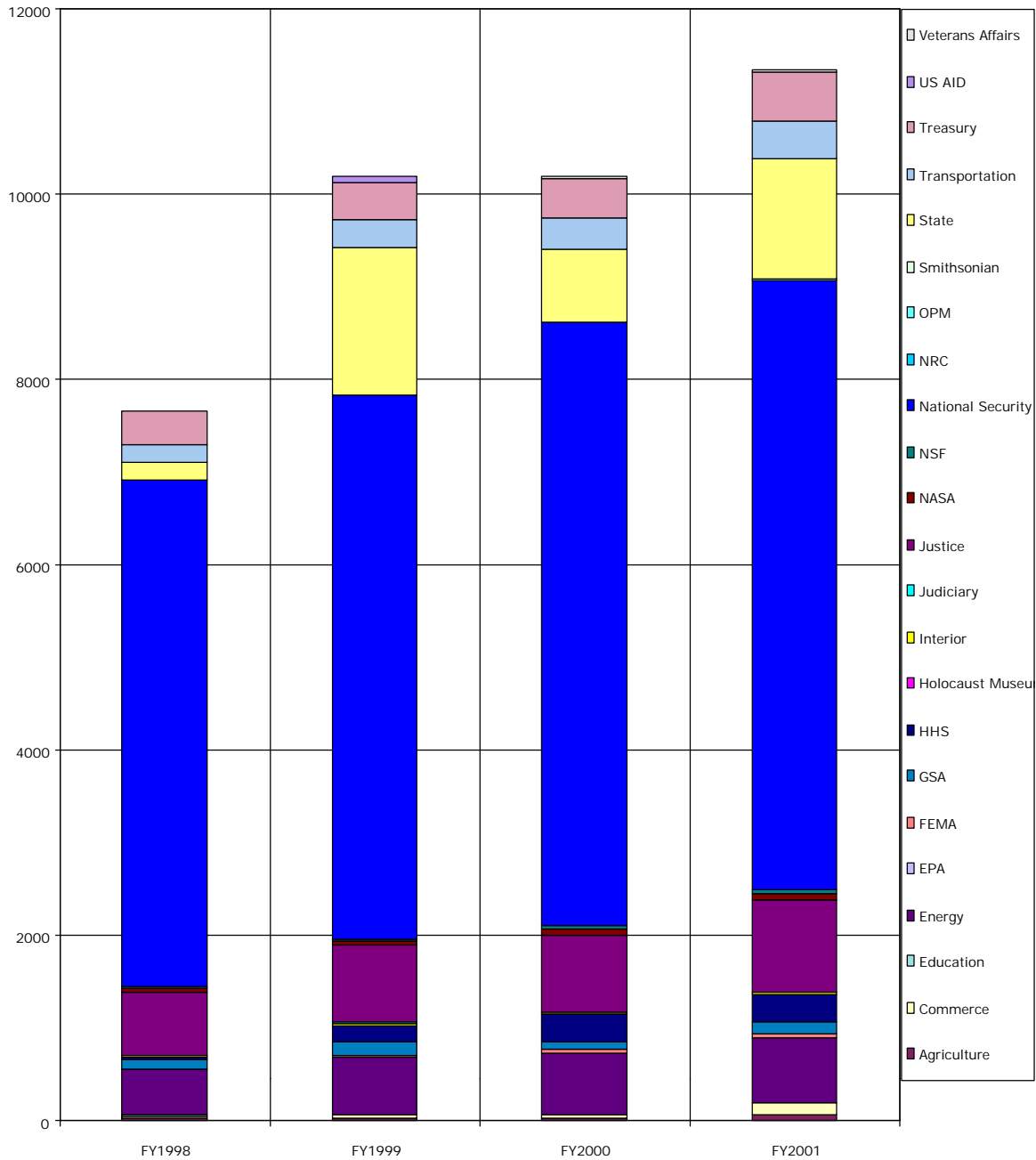
(Current \$US Millions)



Source: Adapted by Anthony H. Cordesman from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000.

Chart Twelve

Federal Spending on Terrorism, WMD, and CIP by Agency: FY1998-FY2001 – Part One
(Current \$US Millions)



Source: Adapted by Anthony H. Cordesman from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000.

Chart TwelveFederal Spending on Terrorism, WMD, and CIP by Agency: FY1998-FY2001 – Part Two
(Current \$US Millions)

<u>FY2001</u>	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	
Agriculture	10.90	12.92	14.84	59.17
Commerce	38.89	53.66	40.15	125.70
Education	3.59	4.45	5.23	2.51
Energy	500.48	614.65	669.59	708.83
EPA	2.12	2.24	2.08	5.50
FEMA	5.92	17.61	31.57	35.99
GSA	89.6	136.5	92.8	132.36
HHS	37.75	187.51	299.67	292.97
Holocaust Museum	0.00	2.00	0.00	0.00
Interior	12.21	15.61	12.31	11.49
Judiciary	7.00	8.00	10.60	11.20
Justice	672.7	848.08	826.04	994.76
NASA	41.00	43.00	66.00	61.00
NSF	19.15	21.42	26.65	43.85
National Security	5470.68	5867.73	6520.11	6582.97
NRC	3.48	3.41	3.21	3.49
OPM	0.00	0.00	2.00	7.00
Smithsonian	0.00	0.00	0.00	0.05
State	186.00	1579.00	791.00	1312.00
Transportation	189.63	295.66	327.89	397.49
Treasury	364.27	416.90	424.21	527.24
US AID	5.68	54.89	5.83	5.01
Veterans Affairs	0.01	0.04	17.33	17.39

Source: Adapted by Anthony H. Cordesman from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000.

Antiterrorism, Counterterrorism, and Core Spending

Chart Thirteen shows the patterns in federal expenditures, less expenditures on CIP. OMB reports that these expenditures are broadly divided into anti-terrorism spending, which includes protection against terrorism and management of the consequences of an attack, and methods to counter terrorism that include efforts to preempt and prosecute terrorism.

OMB also reports that there is an ongoing debate of what priority should be given to each group of activities, but the distinctions between such federal activities are often artificial and it is obvious from the budget presentations of different departments and agencies that the US is still seeking to find what balance is needed. Much of the spending in both categories, however, does not go to Homeland defense per se.

Antiterrorism

In the case of “antiterrorism,” the US has spent massive sums on force protection in recent years, and this includes embassy security and the protection of US troops overseas. According to an OMB estimate, spending in this area grew by 47% from FY1998-2001, largely because of need to improve the protection of embassies. The Clinton Administration requested \$4,295 million for such activities in FY2001, or roughly 55% of all of the money dedicated to anti-terrorism spending. The US National Security community accounts for 51% of the federal funding in “anti-terrorism,” largely because of force protection efforts.

Federal anti-terrorism efforts involve very little broadly based spending on the protection of the national populace and infrastructure. Funds to improve the physical security of the national populace and infrastructure facilities in the US have increased by 80% since FY1998, but accounted for only 3% of the FY2001 request for anti-terrorism funding. Most of this spending has gone to defend largely against conventional attacks, and does not enhance protection against the use of weapons of mass destruction in ways that would attack from beyond a relatively limited security perimeter of selected federal facilities. According to OMB, most of this money has gone to one narrow area, aviation security and in the form of increased inspections and training assistance to security companies.

Law enforcement and investigation activities directed at anti-terrorism include criminal investigations and intelligence assessments by a wide range of agencies. The Bureau of Alcohol, Tobacco, and Firearms funds activities related to trafficking in illegal firearms, the recovery of explosives, and tracing projects. GSA investigates building security. Justice and Treasury concentrate on terrorism-related criminal investigations, and the FAA, GSA, Coast Guard, intelligence community, and NRC conduct defensive intelligence assessments in their areas of responsibility. The Clinton Administration has proposed a \$112 million rise in spending in FY2001 in this category, a 6% rise over FY2000.

Counterterrorism

Federal spending on “counterterrorism” is dominated by law enforcement and investigative activities, which use over 70 percent of total spending. The effort to preempt and prosecute terrorists seeks to meet the goals set forth in PDD-62 relating to the apprehension and prosecution of terrorists. The Clinton Administration has sought to increase this aspect of the FY2001 budget request by \$235 million, of which \$148 million would go to the Justice and Treasury Departments to detect and deter terrorist activity. An additional \$87 million would go to the national security agencies.

The effort to prepare and respond to terrorist acts is dominated by spending by the FBI and national security agencies, which are allocated nearly 80 percent of the FY2001 request. The FBI effort includes investigations and operations and training, forensics, and criminal justice activities. A substantial amount of this funding, however, goes to aid foreign countries or deal with terrorist attacks on Americans overseas. For example, the Administration is seeking to fund a crisis response or FEST aircraft to transport teams to terrorist incidents to assist host nations in managing or resolving a crisis. This area of federal funding also includes Treasury activities in planning and securing protective activities.

Research and development funding for counterterrorism accounts for 80% of all research and development funding, and is conducted by the national security agencies, FBI, and Department of Energy. Much of this funding goes for research to prevent or respond to the use of

weapons of mass destruction, and most recent increases in this category have been dominated by funding for such research.

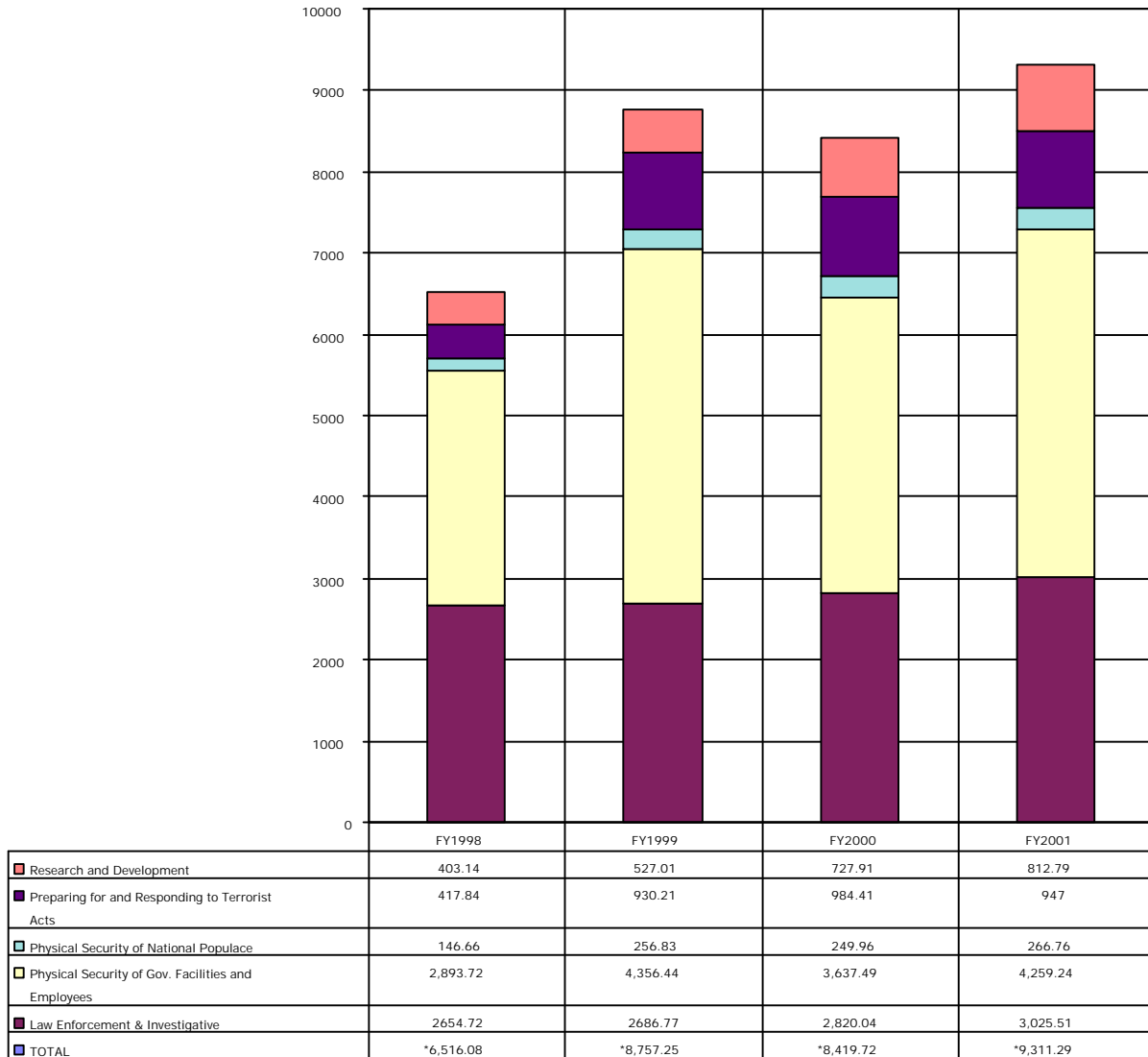
“Core Spending” on Terrorism

Much of the activity in both anti-terrorism and counter-terrorism affects world-wide federal activities. Accordingly, Charts Fourteen and Fifteen provide a different breakout of the patterns in total federal spending on terrorism. They eliminate spending on activities like critical infrastructure protection and show only the core federal spending on threat state actors, their proxies, or independent extremists and terrorists. It must be stressed that such a categorization is highly artificial, but it seems to provide a somewhat more accurate picture of the trends in federal spending designed to directly deter, defend, and/or respond to direct attacks on the American Homeland..

The total expenditures in these charts are much lower than those in the previous tables and charts. The total for FY2001 is only 58 percent of the total for CIP, WMD, and other terrorism, and 70 of the total for WMD, and other terrorism. At the same time, they are still considerable. “Core spending” increased from \$4,267.68 million in FY1998 to \$6,607.02 million in FY2001, or by 55 percent. This involved a 77% increase in spending to deal with weapons of mass destruction, and a more than 100% increase in related research and development activity. They also involved a 14% increase in other law enforcement and investigation activities, a 126% increase in preparations and response to terrorist acts – almost all of which has gone to protection against attacks using weapons of mass destruction -- and a more than 80% increase in efforts to improve the physical security of the populace.

Chart Thirteen

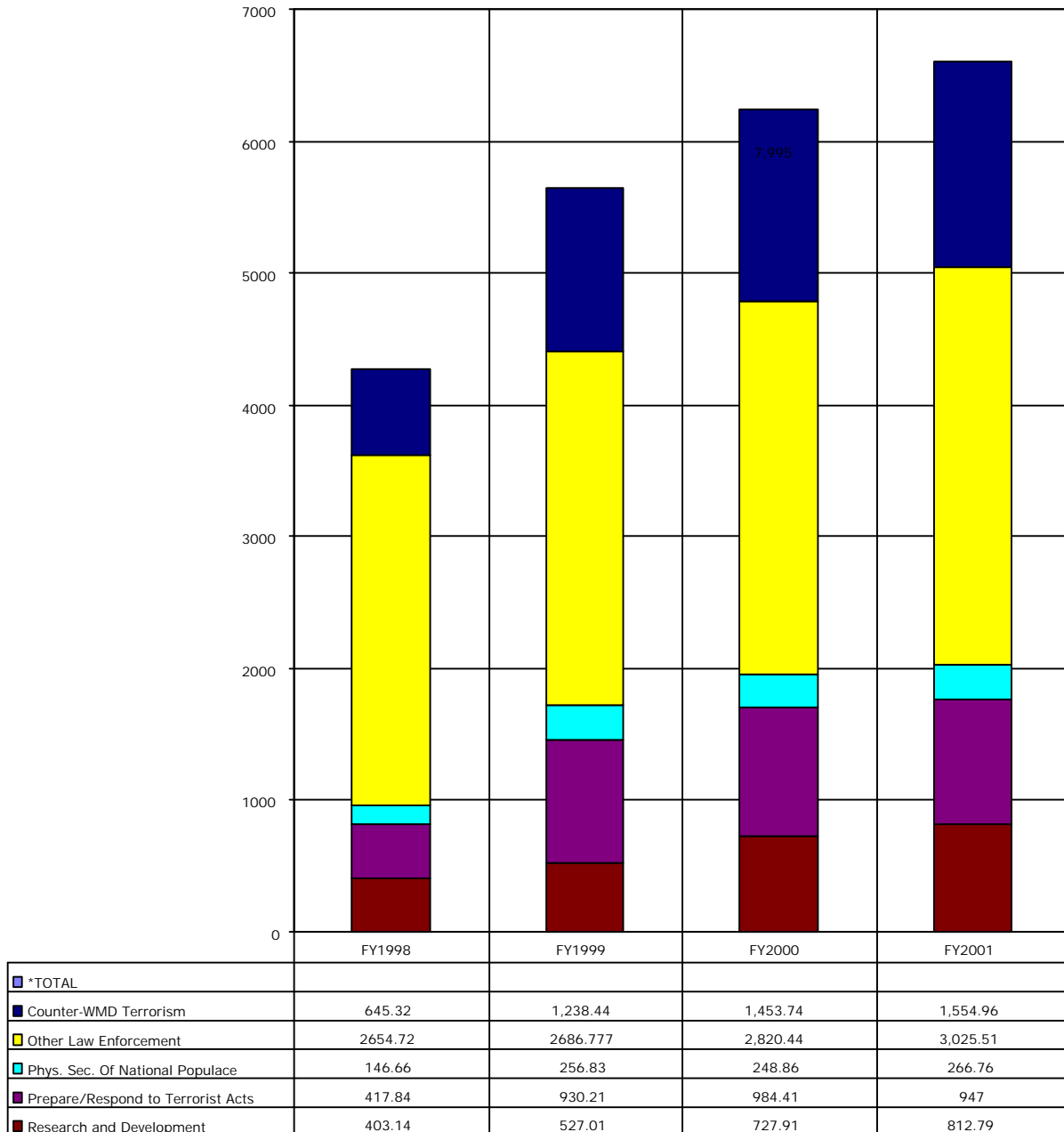
Federal Spending on Terrorism and WMD by Category: FY1998-FY2001
(Current \$US Millions)



Source: Adapted by Anthony H. Cordesman from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000..

Chart Fourteen

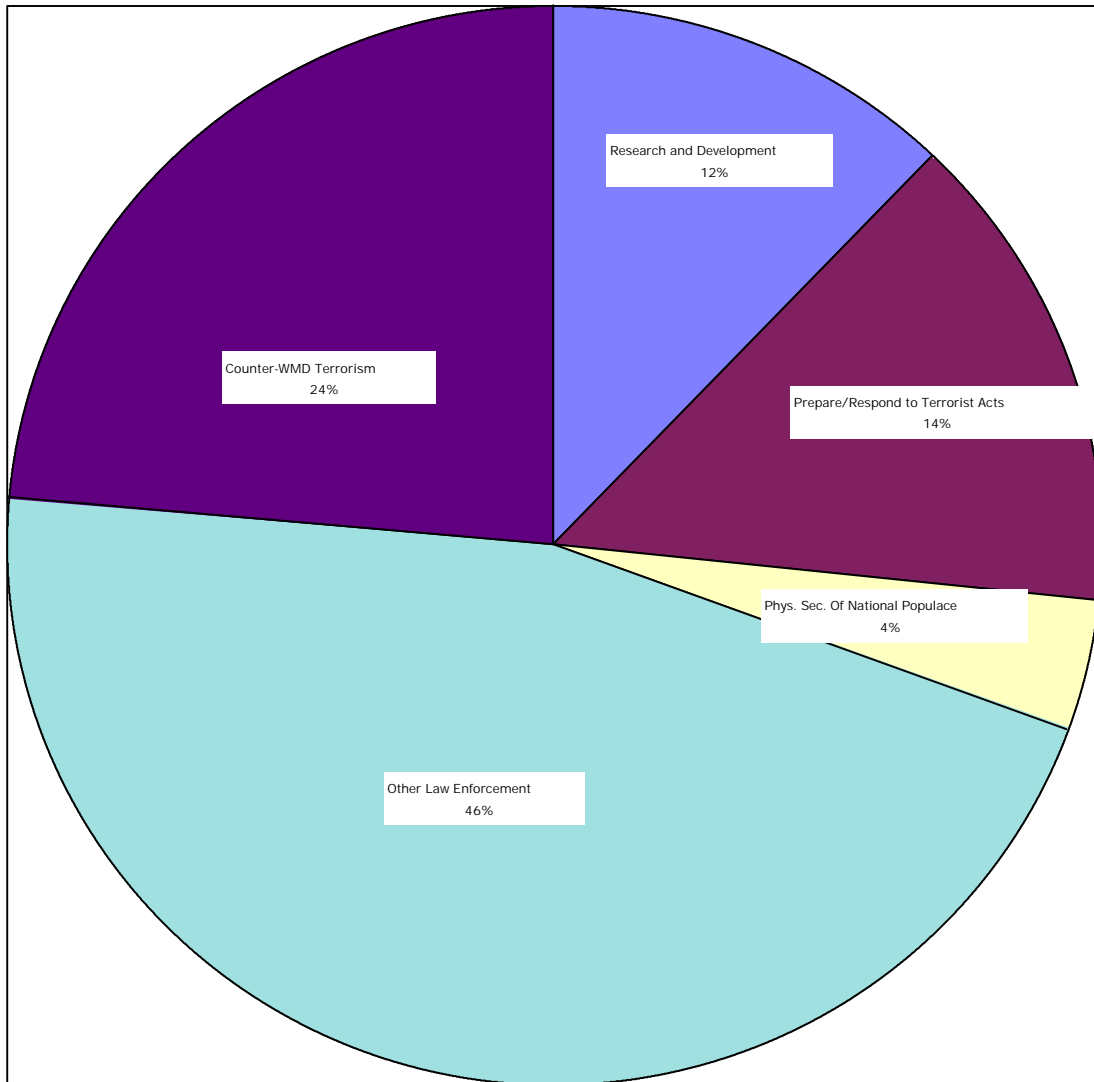
Core Federal Spending on Terrorism and WMD by Activity: FY1998-FY2001:
(Current \$US Millions)



Source: Adapted by Anthony H. Cordesman from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000.

Chart Fifteen

Distribution of Core Federal Spending on Terrorism and WMD by Activity: FY2001
(Current \$US Millions)



Source: Adapted by Anthony H. Cordesman from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000.

Spending on Preparedness for Attacks Using Weapons of Mass Destruction

Only a relatively small number of federal programs are dedicated specifically to dealing with the threat that state actors, their proxies, or independent extremists and terrorists pose to the US Homeland, and these programs often apply at least indirectly to the protection of US forces overseas and America's friends and allies. The size and nature of these programs is shown in Charts Sixteen and Seventeen. Total Federal expenditures have grown from \$645.32 million in FY1998 to a request for \$1,554.96 in FY2001, or by a factor of 2.4. In the process, they have grown from eight percent of total federal terrorism and CIP spending in FY1998 to 14% percent in FY2001.

As Chart Seventeen shows, most of the money is allocated to the Department of Defense and intelligence community (National Security) and Department of Energy – both of which have special expertise in these areas. Their combined budgets have risen from a total of \$456 million in FY1998 to \$831 million in FY2001. HHS has seen a massive increase in such funding -- \$15.9 million in FY1998 to \$265.37 million in FY2001 -- because of the threat of biological warfare. The same is true for the Department of Agriculture, which has gone from \$5.2 million to \$39.8 million. State has seen its budget increase from \$23 million to \$72 million.

The budget of the Department of Justice has more than doubled from \$100.8 million in FY1998 to \$255 million in FY2001. Treasury has increased from \$18 million to \$26 million, FEMA from \$5.92 to \$35 million, and Commerce from \$11.9 to 20.2 million.

WMD programs seek to deter incidents involving the use of massive conventional bombs and chemical, biological, radiological, and nuclear weapons and manage the consequences if they are used. Most spending goes to anti-terrorism efforts, and roughly 90% is devoted to defensive efforts. This spending responds to PPD-62 and the need to enhance domestic preparedness. The FBI is the lead agency for crisis management where there is a credible threat of a WMD incident. FEMA is the lead agency for consequence management, when the incident or threat has subsided and the key priority is to restore order and deliver emergency assistance. Other agencies contribute according to their mission. Energy deals with radiological issues, HHS

with medical impacts, etc. The Department of Defense provides support and has established a joint task force for support to civil authorities and to coordinate federal, state, and local authorities as part of its new Joint Forces Command.

These expenditures also, however, cover foreign incidents. The State Department has responsibility for consequence management and for initial US coordination of such action through the Foreign Emergency Support Team (FEST). The Department of Defense plays a major role in both domestic and foreign related activities because of its long experience with WMD.

WMD Antiterrorism Activities

The main activity in WMD anti-terrorism is preparing for and responding to WMD terrorism. Spending increased from \$89 million in FY1998 to \$566 million in FY2000, after PDD created a new requirement for a concerted effort to improve domestic preparedness. It also assigned Justice, FEMA, HHS, and Defense responsibility as lead agencies for WMD crisis management, consequence management, medical response, and training for state and local authorities, and established a new interagency working group to deal with these issues. The are four major initiatives underway as part of this effort.:

- *Federal assistance to state and local authorities:* The federal government provides training, equipment, planning and technical expertise. Funding is planned to increase by 15% in FY2001 and shift emphasis from training to equipment grants as the first groups of the 120 largest cities in the UJS complete training and begin to procure specialized equipment.
- *Medical defense:* Activity includes public health surveillance of people and the nation's food supply, development of a stockpile of vaccines and therapeutics, and other planning for the medical aspects of an WMD incident. An 8% increase in funding is planned for public health infrastructure for FY2001, and includes a more active program for epidemiological capacity to improve detection and the reporting of outbreaks and for food supply protection. The role of the Department of Agriculture is enhanced to strengthen its ability to identify and protect against terrorist attacks aimed at crops or livestock.
- *Federal special response:* A large-scale WMD incident would overwhelm the response capabilities of state and local authorities. Federal response units will be needed from a variety of agencies, each with a specific expertise and mission. The Department of Energy provides nuclear response teams. The EPA provides HAZMAT management teams. HHS provides medical response teams. The FBI provides forensic response teams, and DoD provides explosive ordnance disposal teams. Funding doubled between FY1998 and FY1999, but then dropped slightly in FY2000 after the start up cost of the DoD WMD Civil Support Teams were paid for.

- *Federal contingency planning and exercises:* These prepare federal agencies and departments to respond to terrorist incidents. There has only been modest program growth since FY1999.

The US also has three smaller mission areas: Physical security of government, physical security of the national populace, and law enforcement and investigation. The FY2001 request for all three programs is \$259 million. Much of this spending goes to protecting government facilities with WMD-relative materials.

WMD Counterterrorism

Most WMD counterterrorism resources go to the national security community and they fall into two main categories. The first is law enforcement and investigation. It totals \$73 million in FY2001, and spending has increased by 40% since FY1998. The second is preparing for and responding to terrorist acts, which totals \$67 million in FY2001. Some of this activity is classified, but it also includes Department of Commerce implementation activities for the Chemical Weapons Convention, accounts for most of the increase over FY2001. The other funding in this area is far participation in joint task forces and planning WMD counterterrorism activities.

R&D for Defense Against WMD

At this point in time, most federal spending on WMD concentrates on research and development. The Clinton Administration has determined that this is the highest priority area for spending. It proposed a 50% increase (\$129 million) in FY1999, and a 30% increase (\$111 million) in FY2001. This spending has strong congressional support, and is focused on dealing with three main scientific and technological challenges:

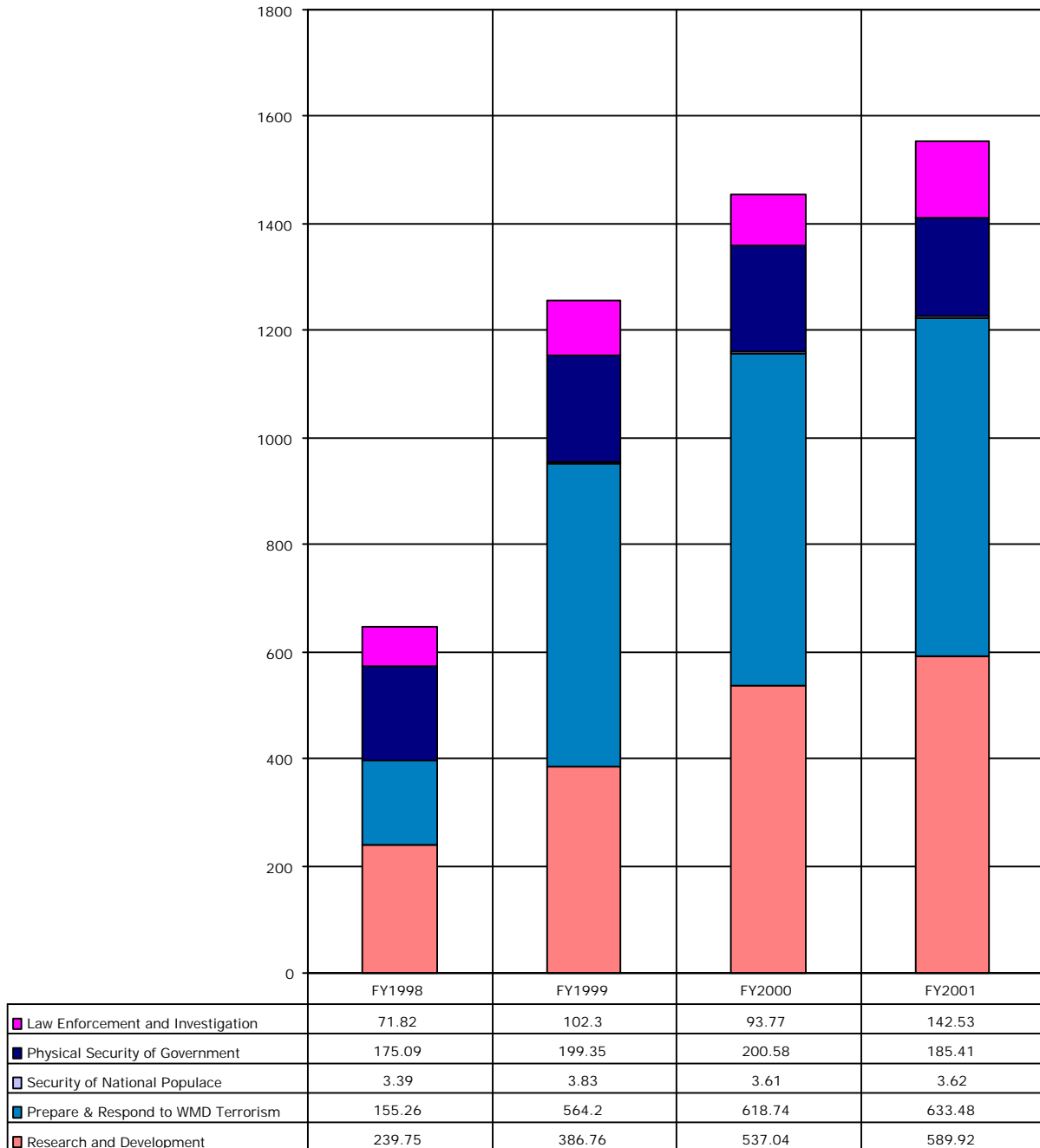
- Preventing or forestalling the release of a WMD payload.
- Detecting and responding to a threatened or actual release.
- Managing the health, environmental, and law enforcement consequences of such an incident.

These efforts require an exceptional degree of interagency coordination, which is the responsibility of the White House Office of Science and Technology Policy, and which chairs an interagency working group to determine vulnerabilities and shortfalls in the US effort to mitigate

or respond to WMD, determines R&D objectives, coordinate agency R&D activities, and identify new requirements. The Clinton Administration has sought to enhance the links between researcher and customers for their R&D products, such as the agencies responsible for meeting first responder and technical needs.

Chart Sixteen

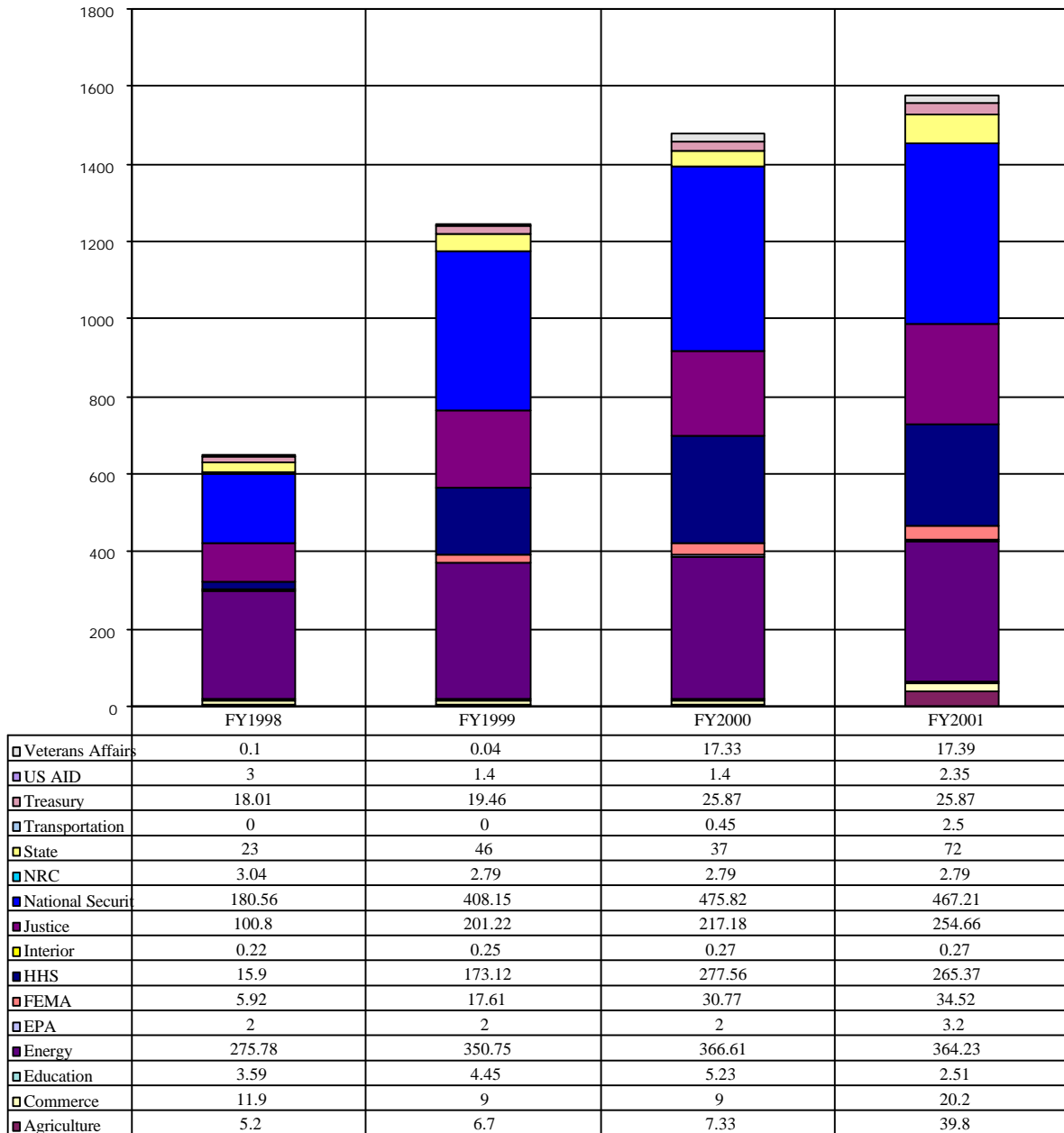
Federal Spending on WMD Preparedness by Activity: FY1998-FY2001
(Current \$US Millions)



Source: Adapted by Anthony H. Cordesman from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000.

Chart Seventeen

Federal Spending on WMD by Agency: FY1998-FY2001 – Part One
(Current \$US Millions)



Source: Adapted by Anthony H. Cordesman from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

Chart SeventeenFederal Spending on WMD by Agency: FY1998-FY2001 – Part Two

(Current \$US Millions)

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
Agriculture	5.20	6.70	7.33	39.80
Commerce	11.90	9.00	9.00	20.20
Education	3.59	4.45	5.23	2.51
Energy	275.78	350.75	366.61	364.23
EPA	2.00	2.00	2.00	3.20
FEMA	5.92	17.61	30.77	34.52
HHS	15.90	173.12	277.56	265.37
Interior	0.22	0.25	0.27	0.27
Justice	100.80	201.22	217.18	254.66
National Security	180.56	408.15	475.82	467.21
NRC	3.04	2.79	2.79	2.79
State	23.00	46.00	37.00	72.00
Transportation	0.00	0.00	0.45	2.50
Treasury	18.01	19.46	25.87	25.87
US AID	3.00	1.40	1.40	2.35
Veterans Affairs	0.10	0.04	17.33	17.39

Source: Adapted by Anthony H. Cordesman from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

Federal Efforts by Department and Agency

Federal departments and agencies generally do a poor job in providing unclassified reporting on any aspect of their counterterrorism programs. Many fail to provide any details on their activities. Of those who do report, many discuss the threat but only provide a vague description of their actual programs, and no detailed description of the money being spent. No agency provides a meaningful description of its future program, future costs, milestones, or measures of effectiveness. Cooperation with state and local agencies is often ignored, and when it is not, it tends to be discussed in anecdotal terms.

Research and development programs receive little detailed description and the description that is provided often concentrates on the threat being dealt with, and agencies provide little program detail. There is no evidence that any department or agency has provided a technology net assessment to examine whether its programs will provide defensive capabilities that outpace advances in offensive capability. There is virtually no discussion of the risk posed by countermeasures or the cost to defeat current and planned programs. There is no discussion of the outyear costs of research and development activity or of estimated deployment schedules, measures of effectiveness, and life cycle costs. Almost without exception, there is no way to be certain to degree to which given programs in given departments or agencies are actually focused on CBRN and other counterterrorism activities, or have simply recast ongoing or desired programs to compete for such funds.

The OMB reports in response to the National Defense Authorization Act do, however, provide an overview of some department and agency activity, and considerably more insight into agency spending. They do not cut across individual agency efforts to the point where, for example, it is possible to determine whether there is anything approaching a coherent program to deal with biological warfare. Yet, they do provide considerable detail on key activities within each agency.

The most recent OMD data are shown in Table Fourteen. It is important to note three

things about these data. First, they do not include expenditures on critical infrastructure protection, although some of these expenditures deal with the protection of physical infrastructure, rather than information systems, and would help homeland defense in the event of a CBRN attack. Second, there is no way to determine how much spending deals with domestic threats per se versus threats to US interests abroad. *Finally, the data on “WMD Preparedness” programs is included in the totals for the programs to combat terrorism, and is not additive to the figures shown for “Combat Terrorism.”*

Table Fourteen

OMB Estimate of Federal Spending on Terrorism by Agency (As of 6/2000)

(Government Spending for Combating Terrorism, WMD and Critical Infrastructure Protection in Current \$US Billions)

Department of Agriculture	16.10	19.62	22.17	98.97
<i>Combat Terrorism</i>	10.20	11.70	12.33	41.28
Physical Security of Government Facilities and Employees	5.00	5.00	5.00	1.48
Preparing for and Responding to Terrorist Acts	0.00	0.00	0.63	10.60
Research and Development	5.20	6.70	6.70	29.20
WMD Preparedness	5.20	6.70	7.33	39.80
Preparing for and Responding to WMD Terrorism	0.00	0.00	0.63	10.60
Federal Planning and Exercises	0.00	0.00	0.00	0.26
Other Planning and Assistance to State/Local	0.00	0.00	0.00	4.48
Public Health Infrastructure/Surveillance	0.00	0.00	0.63	5.87
Research and Development	5.20	6.70	6.70	29.20
Basic Research, incl. Gene Sequencing	0.00	0.00	0.00	10.00
Other	5.20	6.70	6.70	19.20
*OMB Highlighted Programs WMD/CIP				
Research and Development	-	-	-	10.00
Laboratory Infrastructure Improvements	-	-	-	19.00
National Animal Health Emergency Program	-	-	-	5.90
Department of Commerce	50.79	62.66	49.15	145.90
<i>Combat Terrorism</i>	29.54	31.85	22.40	33.60
Law Enforcement and Investigative Activities	5.80	3.90	3.90	15.10
Physical Security of Government Facilities and Employees	11.64	17.45	8.00	8.00
Research and Development	12.10	10.50	10.50	10.50
<i>WMD Preparedness</i>	11.90	9.00	9.00	20.20
Law Enforcement and Investigative Activities	1.90	0.00	0.00	11.20
Research and Development	10.00	9.00	9.00	9.00
Basic Research, incl. Gene Sequencing	10.00	9.00	9.00	9.00

*OMB Highlighted Programs				
WMD Programs				
Bureau of Export Administration	-	-	-	11.20
Department of Energy	776.26	965.40	1,035.90	1,073.06
<i>Combat Terrorism</i>	498.98	611.05	647.61	663.53
Law Enforcement and Investigative	0.94	0.94	0.94	0.94
Physical Security of Government Facilities and Employees	389.00	449.85	468.22	471.05
Preparing for and Responding to Terrorist Acts	84.38	84.80	94.35	97.74
Research and Development	24.66	75.46	84.10	93.80
<i>WMD Preparedness</i>	275.78	350.75	366.31	364.23
Physical Security of Government	186.50	192.25	189.62	174.45
Preparing for and Responding to WMD Terrorism	84.38	84.80	94.35	97.74
Equipment for First Responders	2.10	1.40	8.00	9.55
Federal Planning/Exercises	2.58	3.05	3.05	3.40
First Responder Training and Exercises	0.20	0.20	3.85	4.08
Other	0.50	1.16	1.45	1.45
Special Response Units	79.00	79.00	78.00	79.31
Research and Development	22.90	73.70	82.34	92.04
Basic Research, incl. Gene Sequencing	3.00	4.80	11.00	14.00
Detection/Diagnostics	14.50	16.50	21.00	22.50
Modeling, Simulation, Systems Analyses	3.60	2.00	6.74	6.74
Other	0.00	47.60	40.40	45.60
Personal/Environment Decontamination	1.80	2.80	3.20	3.20
*OMB Highlighted Programs				
WMD Programs				
Nuclear Emergency Search Team	-	-	-	44.00
Technology Development and Applications	-	-	-	25.00
Radiological Assistance Program	-	-	-	4.00
Research and Development	-	-	-	92.00
Nuclear Safeguards, Security and Emergency Operations	-	-	25.00	N/A
Environmental Protection Agency	4.12	4.24	4.08	8.70
<i>Combat Terrorism</i>	2.00	2.00	2.00	3.20
Preparing for and Responding to Terrorist Acts	2.00	2.00	2.00	3.20
<i>WMD Preparedness</i>	2.00	2.00	2.00	3.20
Preparing for and Responding to WMD Terrorism	2.00	2.00	2.00	3.20
Special Response Units	2.00	2.00	2.00	3.20
*OMB Highlighted Programs				
WMD Programs				
WMD Coordinator, Equipment and Training	-	-	-	3.20
Federal Emergency Management Agency	11.84	35.22	62.34	70.51
<i>Combat Terrorism</i>	5.92	17.61	30.77	34.52
Physical Security of Government Facilities and Employees	1.46	1.96	2.13	2.13
Preparing for and Responding to Terrorist Acts	4.45	15.64	28.64	32.39
<i>WMD Preparedness</i>	5.92	17.61	30.77	34.52
Physical Security of Government	1.46	1.96	2.13	2.13
Preparing for and Responding to WMD Terrorism	4.45	15.64	28.64	32.39
Federal Planning/Exercises	0.92	3.02	4.50	4.95
First Responder Training and Exercises	2.76	8.31	14.56	13.96
Other	0.00	0.00	0.08	0.08
Other Planning and Assistance to State/Locals	0.76	4.31	9.50	9.50
Special Response Units	0.00	0.00	0.00	3.90

*OMB Highlighted Programs				
WMD Programs				
Assistance to State and Local Authorities	-	-	-	24.00
Urban Search and Rescue Teams	-	-	-	4.00
General Services Administration	89.60	136.50	92.80	132.36
<i>Combat Terrorism</i>	89.60	133.50	92.80	116.96
Law Enforcement and Investigative Activities	13.90	15.30	15.10	15.39
Physical Security of Government Facilities and Employees	72.90	115.30	74.90	99.41
Preparing for and Responding to Terrorist Acts	2.80	2.90	2.80	2.16
Department of Health and Human Services	53.65	360.63	577.23	558.34
<i>Combat Terrorism</i>	15.90	173.12	277.56	265.37
Preparing for and Responding to Terrorist Acts	0.00	138.25	165.60	173.63
Research and Development	15.90	34.87	111.96	91.74
<i>WMD Preparedness</i>	15.90	173.12	277.56	265.37
Preparing for and Responding to WMD Terrorism	0.00	138.25	165.60	173.63
Medical Responder Training Exercises	0.00	3.00	1.00	2.00
Other	0.00	2.00	3.10	10.60
Other Planning and Assistance to State/Locals	0.00	16.25	16.50	17.43
Public Health Infrastructure/Surveillance	0.00	62.00	88.00	85.50
Special Response Units	0.00	4.00	5.00	6.10
Stockpile of Vaccines and Therapeutics	0.00	51.00	52.00	52.00
Research and Developments	15.90	34.87	111.96	91.74
Basic Research, incl. Gene Sequencing	13.00	17.23	21.76	21.76
Detection/Diagnostics	0.00	5.68	5.68	8.28
Other	0.00	1.85	31.72	0.00
Personal/Collective Protection	0.00	0.00	0.00	1.20
Therapeutics/Treatments	0.00	3.98	4.35	4.35
Vaccines	2.90	6.13	48.45	56.15
*OMB Highlighted Programs				
WMD Programs				
Strengthening the Public Health Surveillance System for WMD	-	-	-	87.00
National Pharmaceutical Stockpile Program	-	-	-	52.00
Metropolitan Medical Response Systems and WMD Preparedness	-	-	-	30.00
Research and Development	-	-	-	92.00
Holocaust Memorial Museum	0.00	2.00	0.00	0.00
<i>Combat Terrorism</i>	0.00	2.00	0.00	0.00
Physical Security of Government Facilities and Employees	0.00	2.00	0.00	0.00
Department of the Interior	12.43	15.86	12.58	11.76
<i>Combat Terrorism</i>	10.92	14.01	9.66	9.66
Law Enforcement and Investigative Activities	0.17	0.20	0.22	0.22
Physical Security of Government Facilities and Employees	10.71	13.77	9.40	9.40
Preparing for and Responding to Terrorist Acts	0.05	0.05	0.05	0.05
WMD Preparedness	0.22	0.25	0.27	0.27
Law Enforcement and Investigative Activities	0.17	0.20	0.22	0.22
Preparing for and Responding to WMD Terrorism	0.05	0.05	0.05	0.05
Other	0.05	0.05	0.05	0.05

Judiciary	7.00	8.00	10.60	11.20
<i>Combat Terrorism</i>	7.00	8.00	10.60	11.20
Physical Security of Government Facilities and Employees	7.00	8.00	10.60	11.20
Department of Justice	773.50	1,049.30	1,043.22	1,249.42
<i>Combat Terrorism</i>	647.09	793.99	782.02	949.25
Law Enforcement and Investigative Activities	346.90	328.91	346.24	409.53
Physical Security of Government Facilities and Employees	84.29	105.08	117.12	171.22
Physical Security of National Populace	29.00	41.76	31.67	30.79
Preparing for and Responding to Terrorist Acts	159.90	301.37	250.12	307.26
Research and Development	27.00	16.87	36.88	30.45
<i>WMD Preparedness</i>	100.80	201.22	217.18	254.66
Law Enforcement and Investigative Activities	43.00	39.74	39.74	43.24
Physical Security of National Populace	1.00	1.44	1.22	1.23
Preparing for and Responding to WMD Terrorism	41.80	147.35	143.54	189.25
Equipment for First Responders	12.00	95.00	85.00	88.00
First Responder Training and Exercises	10.00	26.47	38.45	73.45
Other	1.80	2.00	2.20	2.80
Other Planning and Assistance to State/Locals	18.00	23.88	17.89	25.00
Research and Development	15.00	12.69	32.69	20.94
Detection/Diagnostics	3.00	2.69	2.69	3.94
Personal/Collective Protection	12.00	10.00	30.00	17.00
*OMB Highlighted Programs				
WMD Programs				
Equipment Grants for First Responders	-	-	-	78.00
Domestic Preparedness Training	-	-	-	31.00
Hazardous Devices School	-	-	-	4.60
Center for Domestic Preparedness at Fort McClellan	-	-	-	15.00
Technology and Standards Development	-	-	-	17.00
National Security	5,651.24	6,275.88	6,995.93	7,050.18
<i>Combat Terrorism</i>	4,496.12	4,682.51	5,117.17	5,124.06
Law Enforcement and Investigative Activities	2,042.33	2,067.79	2,213.24	2,213.52
Physical Security of Government Facilities and Employees	2,075.47	2,036.47	2,122.75	2,173.85
Physical Security of National Populace	0.15	0.04	0.15	0.15
Preparing for and Responding to Terrorist Acts	104.20	256.18	358.58	233.84
Research and Development	270.98	322.03	422.45	502.71
<i>WMD Preparedness</i>	180.56	408.15	475.82	467.21
Law Enforcement and Investigative Activities	7.10	20.96	20.41	19.47
Preparing for and Responding to WMD Terrorism	2.71	156.39	161.50	100.74
First Responder Training and Exercises	0.05	49.90	32.10	10.20
Other Planning and Assistance to State/Locals	0.00	15.60	8.50	10.30
Special Response Units	2.66	90.89	120.90	80.24
Research and Development	170.75	230.80	293.90	347.00
Basic Research, incl. Gene Sequencing	44.50	0.00	6.25	37.50
Detection/Diagnostics	0.25	34.10	48.45	62.30
Modeling, Simulation, Systems Analyses	0.00	8.60	10.00	10.00
Other	126.00	140.00	161.50	141.00
Personal/Collective Protection	0.00	0.00	0.00	10.00
Personal/Environmental Decontamination	0.00	6.50	17.10	21.00
Therapeutics/Treatments	0.00	12.00	16.50	22.20
Vaccines	0.00	29.60	34.10	43.00

*OMB Highlighted Programs				
WMD Programs				
Terrorism Consequence Management Response Units	-	-	-	80.00
Coordination of Civil Support	-	-	-	5.00
Research and Development	-	-	-	340.00
Airlift for Counterterrorism Response	-	-	73.00	N/A
Nuclear Regulatory Commission	6.52	6.20	6.00	6.28
<i>Combat Terrorism</i>				
Law Enforcement and Investigative Activities	3.48	3.21	3.21	3.24
Physical Security of Government Facilities and Employees	0.65	0.40	0.40	0.40
Physical Security of National Populace	0.42	0.40	0.40	0.40
Physical Security of National Populace	2.39	2.39	2.39	2.39
Preparing for and Responding to Terrorist Acts	0.02	0.02	0.02	0.05
<i>WMD Preparedness</i>				
Law Enforcement and Investigative Activities	3.04	2.79	2.79	2.79
Physical Security of National Populace	0.65	0.40	0.40	0.40
Physical Security of National Populace	2.39	2.39	2.39	2.39
Smithsonian	0.00	0.00	0.00	0.05
<i>Combat Terrorism</i>				
Physical Security of Government Facilities and Employees	0.00	0.00	0.00	0.05
Physical Security of Government Facilities and Employees	0.00	0.00	0.00	0.05
Department of State	209.00	1,625.00	828.00	1,384.00
<i>Combat Terrorism</i>				
Law Enforcement and Investigative Activities	186.00	1579.00	791.00	1312.00
Physical Security of Government Facilities and Employees	27.00	53.00	46.00	80.00
Physical Security of Government Facilities and Employees	151.00	1512.00	727.00	1224.00
Preparing for and Responding to Terrorist Acts	6.00	6.00	6.00	6.00
Research and Development	2.00	8.00	2.00	2.00
<i>WMD Preparedness</i>				
Law Enforcement and Investigative Activities	23.00	46.00	37.00	72.00
Preparing for and Responding to WMD Terrorism	19.00	41.00	33.00	68.00
Special Response Units	4.00	4.00	4.00	4.00
Special Response Units	4.00	4.00	4.00	4.00
Research and Development	0.00	1.00	0.00	0.00
Other	0.00	1.00	0.00	0.00
*OMB Highlighted Programs				
WMD Programs				
Embassy Security	-	-	-	1200.00
Anti-Terrorism Assistance Program	-	-	-	64.00
Terrorism Interdiction Program	-	-	-	4.00
Department of Transportation	189.63	295.66	328.34	399.99
<i>Combat Terrorism</i>				
Law Enforcement and Investigative Activities	169.30	270.78	277.21	298.15
Physical Security of Government Facilities and Employees	3.90	4.21	4.48	4.68
Physical Security of Government Facilities and Employees	17.86	18.16	19.54	20.94
Physical Security of National Populace	99.78	193.58	199.08	216.50
Preparing for and Responding to Terrorist Acts	3.16	3.04	3.52	6.03
Research and Development	44.60	51.79	50.60	49.65
<i>WMD Preparedness</i>				
Preparing for and Responding to WMD Terrorism	0.00	0.00	0.45	2.50
Equipment for First Responders	0.00	0.00	0.00	2.50
Equipment for First Responders	0.00	0.00	0.00	2.50
Research and Development	0.00	0.00	0.45	0.00
Detection/Diagnostics	0.00	0.00	0.45	0.00
*OMB Highlighted Programs WMD/CIP				

National Airspace System Modernization	-	-	-	49.90
Aviation Security	-	-	-	312.00
Protection of Critical Coast Guard Systems	-	-	-	3.30
Transportation Infrastructure Assurance Research and Development	-	-	-	3.40
Information Sharing and Threat Dissemination	-	-	-	1.00
Global Positioning System Protection	-	-	-	0.15
Department of Treasury	382.28	436.36	450.08	553.11
<i>Combat Terrorism</i>	341.36	368.01	348.00	440.21
Law Enforcement and Investigative Activities	213.13	212.13	189.53	285.73
Physical Security of Government Facilities and Employees	64.30	67.51	68.46	63.46
Physical Security of National Populace	15.34	19.06	16.58	16.58
Preparing for and Responding to Terrorist Acts	47.89	68.52	70.70	71.70
Research and Development	0.70	0.79	2.73	2.74
<i>WMD Preparedness</i>	18.01	19.46	25.87	25.87
Physical Security of Government Facilities and Employees	5.14	5.14	8.84	8.84
Preparing for and Responding to WMD Terrorism	12.88	14.32	17.03	17.03
Equipment for First Responders	0.99	2.02	2.23	2.23
Other	0.35	0.73	0.20	0.20
Special Response Units	11.53	11.57	14.60	14.60
*OMB Highlighted Programs				
WMD Programs				
Air Security Protective Operations	-	-	-	16.00
CIP Programs				
Research and Development	-	-	-	4.00
Public Key Infrastructure	-	-	-	7.00
US AID	8.68	56.29	7.23	7.36
Combat Terrorism	5.68	54.89	5.83	5.01
Physical Security of Government Facilities and Employees	2.68	3.49	3.98	2.66
Preparing for and Responding to Terrorist Acts	3.00	51.40	1.40	2.35
<i>WMD Preparedness</i>	3.00	1.40	1.40	2.35
Preparing for and Responding to WMD Terrorism	3.00	1.40	1.40	2.35
First Responder Training and Exercises	0.30	1.40	1.40	2.35
Other	2.70	0.00	0.00	0.00
Department of Veterans Affairs	0.01	0.04	17.33	17.39
<i>Combat Terrorism</i>	0.01	0.04	0.00	0.00
Preparing for and Responding to Terrorist Acts	0.01	0.00	0.00	0.00
*OMB Highlighted Programs				
WMD Programs				
Stockpiling Pharmaceuticals	-	-	-	N/A
Training Medical Personnel	-	-	-	N/A

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Department of Agriculture

The Department of Agriculture plays a critical role in preparing for biological attacks on US agriculture, and in dealing with the impact of fallout and secondary effects from a nuclear attack. USDA is requesting \$10 million for FY 2001 for new research and development into techniques to rapidly identify pathogens and toxins and to discover the geographic origin of the pathogens.²²

National Animal Health Emergency Program

The FY 2001 request also includes \$5.9 million APHIS's National Animal Health Emergency Program. The program is designed for APHIS to train personnel to respond to animal disease outbreaks that threaten the agriculture economy. APHIS is planning to develop training for WMD terrorism, including decontamination of CB agents. The funding will also go towards an awareness campaign to recognize foreign animal diseases; to develop an animal pathogen genetic library; to develop veterinary investigative tools; to update bioterrorism response plans; and towards the National Emergency Management Operations Center. The National Emergency Management Center provides leadership for national plant and animal health emergencies.²³

The following chart on USDA counterterrorism spending adapted from the 2000 OMB counterterrorism funding report shows a very large increase in the funds requested for FY 2001 compared to previous appropriations. The \$41.28 million requested is 235% above FY 2000 levels. 96% of the requested funds will go towards WMD preparedness.²⁴

Table Fifteen

Department of Agriculture Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	10.20	11.70	12.33	41.28
Physical Security of Government Facilities and Employees	5.00	5.00	5.00	1.48
Preparing for and Responding to Terrorist Acts	0.00	0.00	0.63	10.60
Research and Development	5.20	6.70	6.70	29.20

<i>WMD Preparedness</i>	5.20	6.70	7.33	39.80
Preparing for and Responding to WMD Terrorism	0.00	0.00	0.63	10.60
Federal Planning and Exercises	0.00	0.00	0.00	0.26
Other Planning and Assistance to State/Local	0.00	0.00	0.00	4.48
Public Health Infrastructure/Surveillance	0.00	0.00	0.63	5.87
Research and Development	5.20	6.70	6.70	29.20
Basic Research, incl. Gene Sequencing	0.00	0.00	0.00	10.00
Other	5.20	6.70	6.70	19.20
<i>*OMB Highlighted Programs WMD</i>				
Research and Development	-	-	-	10.00
National Animal Health Emergency Program	-	-	-	5.90

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Central Intelligence Agency

OMD does not report on CIA activity except as part of the broader category of "National Security. The Center for Nonproliferation at the Monterey Institute of International Studies described the counterterrorism efforts of the CIA as follows:²⁵

The Directorate of Central Intelligence's mission is to gather timely intelligence on terrorist groups abroad in order to prevent and prepare for terrorist attacks.

Interagency Intelligence Committee on Terrorism

More than 40 federal agencies, bureaus, and offices are members of this committee. The Committee shares information between agencies on activities of terrorist groups and countries sponsoring terrorism in order to assess terrorist threats. Another element of this project is the detailing of staff between organizations, including representatives of many intelligence agencies to the Counterterrorist Center.

Counterterrorist Center

This center is a hub for interagency intelligence sharing to further efforts to combat terrorism. The center has representatives from all major facets of the intelligence community, as listed below. According to a speech by President Clinton in 1995, "an FBI official serves as the deputy director of the Counterterrorist Center."

The agencies contributing to the Counterterrorist Center are as follows: Federal Bureau of Investigation, National Security Agency, Defense Intelligence Agency, Bureau of Intelligence and Research of the State Department, and the Central Intelligence Agency.

Department of Commerce

The Department of Commerce plays a major role in export and import control and in enforcing some aspects of arms control. The DOC's Bureau of Export Administration requested \$11.2 million for FY 2001 to strengthen import and export controls on WMD materials and to implement Chemical Weapons Convention inspections. Below is a chart adapted from the 2000 OMB counterterrorism funding report.²⁶ FY 2001 requested funding for WMD preparedness includes an increase of \$11.2 million towards WMD preparedness.

Table Sixteen

Department of Commerce Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	29.54	31.85	22.40	33.60
Law Enforcement and Investigative Activities	5.80	3.90	3.90	15.10
Physical Security of Government Facilities and Employees	11.64	17.45	8.00	8.00
Research and Development	12.10	10.50	10.50	10.50
<i>WMD Preparedness</i>	11.90	9.00	9.00	20.20
Law Enforcement and Investigative Activities	1.90	0.00	0.00	11.20
Research and Development	10.00	9.00	9.00	9.00
Basic Research, incl. Gene Sequencing	10.00	9.00	9.00	9.00
*OMB Highlighted Programs				
Bureau of Export Administration	-	-	-	11.20

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Department of Defense

OMB does not provide specific figures for the Department of Defense, which is included as part of the OMB totals for "National Security." The Department does, however, play a critical role in defending the US against foreign attacks, in intelligence, in counterterrorism, and in responding to CBRN attacks. The Secretary of Defense announced the Defense Counterproliferation Initiative in 1993 to combat the CBRN threat. This Initiative calls for developing capabilities that will allow the US to defeat an enemy using CBRN weapons, and the Secretary of Defense has described the CBRN threat as the single greatest and most complex

challenge currently facing the DOD.

The GAO has reported as follows on the progress DOD has made in implementing the Initiative:²⁷

The U. S. National Military Strategy states that the continued proliferation of weapons of mass destruction, particularly chemical and biological weapons, has made their use by an adversary increasingly likely in both a major theater war and smaller scale contingencies. These weapons are capable of causing mass casualties, and their threat or use can disrupt the planning and conduct of military operations. DOD believes effective deterrence against the use of these weapons depends on a range of nuclear and conventional response capabilities, as well as active and passive defenses and supporting command, control, communications, and intelligence. DOD estimates that for fiscal year 2001 it will invest over \$7.3 billion on the research, development, and acquisition of such conventional response capabilities, with about \$5.3 billion of that investment on missile defense. Although an unclassified estimate is unavailable, additional funding is spent to provide intelligence support for counterproliferation.

To help ensure that DOD's counterproliferation policy objectives are met and that implementation of the Counterproliferation Initiative is integrated and focused, the Secretary of Defense, in 1996, established the Counterproliferation Council composed of senior DOD civilian and military officials. The Council is to monitor departmental progress on developing the strategy, doctrine, and force planning necessary to effectively execute its counterproliferation objectives. In 1997, DOD's Quadrennial Defense Review report stated that a key challenge the Department must meet to ensure it is prepared for the NBC threat is to institutionalize—integrate or make permanent—counterproliferation as an organizing principle in every facet of military activity.

To review activities and programs related to countering proliferation threats within the Departments of Defense and Energy and the U.S. intelligence community, in 1993 the Congress established the Counterproliferation Program Review Committee. The Committee's charter includes addressing shortfalls in existing and programmed capabilities to counter the proliferation of NBC weapons of mass destruction and their delivery systems; identifying and eliminating undesirable redundancies or uncoordinated efforts; and establishing priorities for programs and funding. Since 1995, the Committee has submitted an annual report to the Congress detailing its findings and recommendations.

DOD is taking steps to make the nuclear, biological, and chemical threat a matter of routine consideration within its activities and functions, such as training and field exercises and the acquisition of weapon systems and equipment. Since the 1993 Defense Counterproliferation Initiative was announced, DOD has given greater emphasis to this threat in policy and planning documents, and the Joint Staff has made considerable effort to determine and prioritize the counterproliferation requirements of the unified commands. The services, particularly the Air Force, have increased the importance placed on counterproliferation requirements in their acquisition programs, training, and doctrine. Regional unified commands have incorporated counterproliferation concepts, equipment, and tasks into their planning and military exercises.

...While DOD has taken positive steps, it can do more to integrate and focus its response to the growing threat posed by the proliferation of nuclear, biological, and chemical weapons. DOD does not have an overarching joint counterproliferation doctrine document to provide a centralized picture of how DOD should respond in a nuclear, biological, and chemical environment across the spectrum of military operations. Such a document, which was recently approved for development, will help ensure that counterproliferation is being satisfactorily integrated in the entire body of joint doctrine. DOD also has not taken sufficient action to provide reasonable assurance that its weapon systems and equipment can survive and operate in a biological and chemical environment. Additionally, studies by DOD and a congressionally

mandated commission indicate that DOD's organization structure may be too diffused to effectively manage and integrate the Department's counterproliferation mission.

DOD has not developed key strategy documents and management plans to aid in directing and managing its counterproliferation initiatives. Internal DOD reviews have identified the need for a comprehensive strategy for countering the proliferation of weapons of mass destruction and a military strategy for integrating offensive and defensive capabilities. There is also no management plan to guide, oversee, and integrate department-wide initiatives, which would include a reporting and evaluation process with performance measures to allow for a continual assessment of the Department's progress in achieving goals and objectives.

DOD primarily coordinates its counterproliferation activities with the Department of Energy and the intelligence community through the Counterproliferation Program Review Committee. DOD, Energy, and intelligence agency officials generally expressed satisfaction with the exchange of information that the Committee had provided about ongoing programs among the agencies. However, the Committee has taken little action to identify and eliminate undesirable redundancies among research and development programs, one of the primary reasons the Congress established it. The Committee does not have a process to facilitate such determinations and provide a basis to make decisions on eliminating undesired redundancies.

This report includes recommendations that the Secretary of Defense (1) develop strategies, a management plan, and performance measures to help guide and manage the implementation of DOD's counterproliferation actions; (2) include in the next Quadrennial Defense Review an examination of the Department's organization for counterproliferation; (3) take steps to help ensure that the nuclear, biological, and chemical threat is being given sufficient attention in military doctrine and in the design and development of weapon systems and equipment; and (4) devise and implement a mechanism to help identify and eliminate undesirable redundancies among counterproliferation programs.

Domestic Preparedness Program

The Defense Against Weapons of Mass Destruction Act of 1996, also known as the Nunn-Lugar-Domenici Act, designated the DOD as the lead agency for domestic preparedness for responding to and managing the consequences of a WMD attack. DOD established the Domestic Preparedness Program to train local and state first responders for a CBRN attack. The Army's Soldier and Biological Chemical Command is the organization within the DOD that administers the Domestic Preparedness Program.²⁸ Total funding for the program during fiscal years 1997-99 was \$66.9 million. Funding for fiscal year 2000 is \$12.6 million. The funding request for FY2001 is \$31 million.²⁹

A March 2000, GAO report summarized the program as follows:³⁰

Defense developed the Domestic Preparedness Program to build on the existing knowledge and capabilities of those who would first deal with a WMD incident locally: fire, law enforcement, hazardous materials, and medical personnel. Defense planned to provide personnel in the 120 largest U.S. cities (based on city population) with training and expert advice regarding emergency responses to the use or threatened use of weapons of mass destruction or related materials. Defense targeted cities for the training because it wanted

to deal with a single government entity that could choose the most appropriate personnel to be trained and to receive training equipment. Defense trains city personnel, who then provide similar instruction to their emergency responder communities.

The training is generally a week long and comprises six separate courses--emergency responder awareness, emergency responder operations, technician-hazardous materials, technician-emergency medical services, technician-hospital provider, and incident command. The awareness and operations courses, each 4-hour segments, generally train responders in how to recognize a WMD incident and how to protect themselves and their communities during such incidents. The technician courses vary in length from 8 to 16 hours and are primarily for individuals in those specialties. The incident command course, 8 hours in length, focuses on the management of an incident and includes an exercise during which participants role-play their responses.

As of September 30, 1999, Defense had completed training in 67 cities and trained approximately 19,000 individuals. This includes only those individuals directly trained by Defense instructors...

The GAO also provided the following table on the output of these training efforts:

Table Seventeen:

First Responders Trained Through Domestic Preparedness Program (from program's inception in fiscal year 1997 through fiscal year 1999)

Responder community	Number trained
Firefighter	5,100
Law enforcement	4,300
Emergency medical services	1,600
Hospital provider	2,800
Military	850
Other ^b	4,350
Total	19,000

The program will cover the 120 largest cities in the US based on 1990 Census data, and each city can request \$300,000 of equipment that is loaned from the DOD for 5 years. Training will be completed in the 120 largest cities by mid-2001.

The Domestic Preparedness Program has been an example that critics like the GAO have

cited in arguing for better federal integration of terrorism programs. DOJ administers the Metropolitan Firefighters program and FEMA administers WMD courses at its National Fire Academy and Emergency Management Institute in Maryland. The problem is the potential for and actual overlap in first responders' training among the DOD, DOJ, and FEMA programs. Furthermore, another complaint is that it is inefficient for responders in each city to attend three programs from three departments when an integrated program would save time and resources. The Administration has proposed to transfer the program to DOJ on October 1, 2000, however, and DOJ will complete DOD's commitments to the 120 cities.³¹

The GAO has made the following comments,³²

Federal training programs on weapons of mass destruction are not well coordinated, resulting in inefficiencies in the federal effort and concerns in the first responder communities. The Departments of Defense and Justice and the Federal Emergency Management Agency are providing similar awareness courses as part of their train-the-trainer programs. Defense and Justice plan to deliver their programs to individuals in the same 120 cities, and Justice also plans to train individuals in 135 additional jurisdictions. Through September 1999, Defense had trained individuals in 67 cities, and through mid-November 1999 Justice had trained individuals in 95 cities and metropolitan areas. Training from both agencies' programs was provided to individuals in 16 common cities. State and local officials and representatives of various responder organizations expressed concerns about duplication and overlap among the two federal training programs, courses offered by the Consortium, and other courses such as hazardous materials and other specialized training that first responders are required to complete. Some officials said that the number of federal organizations involved in weapons of mass destruction training creates confusion about which federal organization is in charge of that training. Officials were concerned that the Defense and Justice programs offered to cities and counties had bypassed the states' emergency management and training structures. As a result, some responders, such as state police, had been missed. And some officials were concerned that the Defense and Justice programs will not train responders in smaller communities. They pointed out the potential to reach responders in smaller communities through the use of state and local training organizations and the use of training tools such as video transmission of instructional materials to existing facilities at firehouses and National Guard armories. The responders' concerns are consistent with the conclusions reached by a forum of over 200 state and local responders in August 1998 and a June 1999 Justice report. Common themes included the need for a single focal point for information about federal programs, a centrally coordinated and standardized national training program to ensure an effective and integrated response and to minimize redundancy in training programs, and the need to incorporate training related to terrorist incidents involving weapons of mass destruction into existing training delivery mechanisms for the emergency responder communities.

Efforts are under way to improve the federal government's role in weapons of mass destruction training, but more actions are needed to eliminate duplicative training and improve the efficiency of the Defense and Justice programs. Although Defense plans to transfer its Domestic Preparedness Program to Justice on October 1, 2000, and Justice was to provide Congress with a comprehensive plan for the transfer no later than December 15, 1999, that plan had not been issued as of March 1, 2000. According to Justice officials, Justice will complete Domestic Preparedness training in the 120 cities to honor Defense's commitments to those cities. It also still plans to deliver its Metropolitan Firefighters program to individuals in 255 cities and counties. Thus, in the near term, some cities will receive similar awareness courses under both programs. Justice officials said that in the longer term, they will assess the need to continue the Domestic

Preparedness Program beyond the 120 cities based on a number of factors, including comprehensive needs assessments to be completed by the states and inputs from the first responder communities. In response to requests from the first responder community, Justice has established the interagency National Domestic Preparedness Office. The Office, recently funded under the Consolidated Appropriation Act for Fiscal Year 2000, is just getting organized. According to its draft action plan, it will provide an interagency forum for coordinating federal weapons of mass destruction assistance to state and local emergency responders. The Office has identified an ambitious list of tasks directed at many of the training concerns expressed by first responders.

To improve the efficiency of federal programs, we are recommending that the Secretary of Defense and the Attorney General eliminate duplicative training in the same metropolitan areas. We are also recommending that if the Department of Justice provides Domestic Preparedness Program training in more than the currently planned 120 cities, it integrate the program with the Metropolitan Firefighters Program to capitalize on the strengths of each program and eliminate duplication and overlap.

Chemical and Biological Defense Program

After the Persian Gulf War, protection against chemical and biological weapons became a high priority. Congress passed the National Defense Authorization Act for Fiscal Year 1994, which directed the Secretary of Defense to improve the DOD's chemical and biological defense programs. DOD integrated all programs into what is now the Chemical and Biological Defense Program headed by the Deputy Assistant to the Secretary of Defense for Chemical and Biological Defense. This has led to a steady increase in many expenditures. For example, the chemical agents and munitions destruction, defense category of Defense-wide Procurement Appropriations Account has increased \$24 million from \$979 million for the 2000 FYDP to \$1,004 million for the 2001 FYDP.³³

The Deputy Assistant to the Secretary of Defense is responsible for planning, programming, budgeting, coordination of medical and non-medical defenses, and overseeing management. The Deputy Assistance Secretary is also the Executive Secretary of the Steering Committee which is comprised of Directors of the Defense Threat Reduction Agency, Defense Research and Engineering, representatives of the joint Chiefs of Staff, the Assistant Secretary of Defense for Strategy and Threat Reduction, the Assistant Secretary for Health Affairs, and top officials responsible for chemical and biological defense.³⁴

The Chemical and Biological Defense Program is divided into three non-medical defensive capabilities: contamination avoidance, protection, and decontamination. Contamination avoidance is detecting and avoiding contaminated areas, and decontamination is the restoration

of fighting ability after a CB attack. The research agencies of the Chemical and Biological Defense Program include the Soldier and Biological Chemical Command, the Joint Program Office for Biological Defense, and the Defense Advanced Research Projects Agency. GAO testimony provides a brief description of these research agencies:³⁵

- The Soldier and Biological Chemical Command is organized around two integrated business areas, one of which is research, development, and acquisition. Nearly half of its research, development, and acquisition funding supports the Chemical and Biological Defense Program. The Command is engaged in the full range of research and development encompassing both biological and chemical systems. Its business areas include chemical detection, biological detection, decontamination, protection, and supporting science and technology.
- The Joint Program Office for Biological Defense manages the biological warfare agent detection program. The office monitors emerging technologies for advanced development, demonstration, and upgrades of fielded biological detection systems.
- The Defense Advanced Research Projects Agency's Biological Warfare Defense Program is an applied research program established under the authority of the National Defense Authorization Act for Fiscal Year 1997 (P.L. 104-201, as amended) to fund revolutionary new approaches to biological warfare defense. The Biological Warfare Defense Program pursues high-risk, high-potential technologies from the demonstration of technical feasibility through the development of prototype systems.

The Department of Defense (DoD) Chemical and Biological Defense Program (CBDP) continues to implement congressional direction to improve jointness and reflects an integrated DoD developed program. The FY 1999-2000 program funds the highest priority counterproliferation initiatives. During the past year, the Department reviewed its capabilities to protect against the asymmetric threats from chemical and biological weapons. As a result of the review, funding was identified to enhance and accelerate high-payoff technologies and advanced CB defense systems.

The FY2000- 2001 President's Budget Submission includes \$380 million in increased research and development funding for biological warfare defense and vaccines over the FY 2000-05 Future Years Defense Program (FYDP), as well as additional FY 1999 Emergency Supplemental funding to procure CB defense equipment for the Guard and Reserves to support the Consequence Management mission.

Moreover, the Department continues to procure new CB defense equipment, due in large measure to the May 1997 Report of the Quadrennial Defense Review (QDR) recommendation to increase planned spending on counterproliferation by \$1 billion over the FY 1999- 2003 program

period, of which \$732 million was allocated for chemical and biological defense efforts. The DoD CBDP invests in technologies to provide improved capabilities that have minimal adverse impact on warfighting potential.

For FY 2000, the program's appropriation was \$791 million, \$410 million for R&D and \$381 million for procurement.³⁶

The GAO has repeatedly criticized the CBDP for not following the 1993 Government Performance and Results Act. The Results Act directs agencies to focus on program outcomes and performance rather than on program resources and activities. GAO criticized the CBDP in August 1999 and again in May 2000:³⁷

Congressional reports and administrative guidance indicate that DOD programs such as the Chemical and Biological Defense Program should follow the Results Act's outcome-oriented principles, including the establishment of general goals; quantifiable, measurable, outcome oriented performance goals; and related measures. Moreover, research organizations such as the Research Roundtable, the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine have concluded that both applied and basic research programs supported by the federal government could be evaluated meaningfully in accordance with the Results Act framework.

DOD's Chemical and Biological Defense Program in general, and its R&D activities in particular, have not incorporated key Results Act principles. Program goals are vague and unmeasurable and the performance measures emphasize activities rather than impacts. In the absence of explicit and measurable goals, it is difficult to assess the impact of the Program on warfighters' ability to survive, fight, and win in a chemical and biological environment.

Chemical and Biological Defense Program research and development organizations have incorporated Results Act principles inconsistently. Only one of three DOD organizations that engage in R&D activities in support of the Chemical and Biological Defense Program has adopted the Results Act planning and evaluation tools. The remaining two cited either the utilization of equivalent planning tools or the unique challenges of evaluating research and development activities as reasons for not adopting the Results Act processes.

Our August 1999 report recommended that the Secretary of Defense direct that actions be taken to develop a performance plan for the Chemical and Biological Defense Program based on the outcome-oriented management principles embodied in the Results Act. DOD concurred with the recommendation and agreed to develop a full detailed and coordinated plan for inclusion in its next DOD Chemical and Biological Defense Program Annual Report to Congress. Nevertheless, the next Report to Congress in March 2000 did not contain a plan containing the elements outlined in our recommendation. In the March 2000 Report to Congress, DOD established a new set of program goals and stated specific technology and systems goals will be included in a performance plan to be completed during calendar year 2000 and included in the next annual report to Congress.

The GAO also recommends that CBDP be coordinated with the other non-medical chemical and

biological research programs:³⁸

Each of the federally funded programs conducting non-medical research and development on threats from chemical and biological agents has its own mission objective. However, we found many similarities among these programs in terms of the research and development activities they engage in, the threats they intend to address, the types of capabilities they seek to develop, the technologies they pursue in developing those capabilities, and the organizations they use to conduct the work. For example, these programs conduct a similar range of research and development activities, such as evaluating the feasibility or showing the practical utility of a technology. With regard to threat, two of the programs (those in the Department of Defense and Defense Advanced Research Projects Agency) focus on threats to the military, and the other two (those in the Department of Energy and the Technical Support Working Group) focus on threats to civilians. However, the military and civilian user communities are concerned about many of the same chemical and biological substances (such as nerve agents) and possible perpetrators (such as foreign terrorists). In addition, we found that these programs are seeking to develop many of the same capabilities, such as detection and identification of biological agents. Furthermore, the types of technologies (such as mass spectroscopy) they pursue to achieve those capabilities may overlap. Finally, these programs may contract with the same groups of laboratories to perform research and development work.

Although the four programs we examined currently use both formal and informal mechanisms for coordination, we found several problems that may hamper their coordination efforts. First, participation in formal and informal coordination mechanisms is inconsistent. For instance, several of these mechanisms do not include representatives of the civilian user community. Second, program officials cited a lack of comprehensive information on which chemical and biological threats to the civilian population are the most important and on what capabilities for addressing these threats are most needed. Third, several programs do not formally incorporate existing information on chemical and biological threats or needed capabilities in deciding what research and development projects to fund. Having and using detailed information on civilian chemical and biological threats and the capabilities needed to respond to those threats would enable coordination mechanisms to better assess whether inefficient duplication or critical research gaps exist, and if so, what changes should be made in federal research and development programs.

WMD Civil Support Teams

The WMD Civil Support Teams represent the first military responders and have a goal of reaching a WMD scene within four hours. 10 teams have already been established and a total of 27 teams will be deployed by early 2001. WMD Civil Support Teams were formerly known as National Guard Rapid Assessment and Initial Detection Teams. The teams help local and state responders assess the situation, provide technical and medical advice, define requirements, and expedite the use of state and federal support. A team is comprised of seven cells: command and control, reconnaissance, medical support, security, logistics, air liaison, and communications.³⁹ Each team has 22 members, and the governors of the states they are deployed have command and control of the team.⁴⁰

Joint Task Force for Civil Support

The DOD established the Joint Task Force for Civil Support to coordinate the department's WMD consequence management support to local and state officials. The task force is based in Norfolk, VA, and is led by a National Guard brigadier general. The task force has no standing forces but can mobilize quickly at FEMA's request of assistance. The task force also has operational command and control of WMD Civil Support Teams if the teams are federalized.⁴¹ \$5 million has been requested for FY 2001 for the Joint Task Force.

Foreign Emergency Support Team

The DOD provides the aircraft for the interagency Foreign Emergency Support Team (FEST). FEST assists with the management of terrorist attacks in foreign countries. The DOD needs funding to replace the 38-year-old aircraft. \$73 million was appropriated in the FY Supplemental.⁴²

Office of the Secretary of Defense

According to the Nunn-Lugar-Domenici Act, the Secretary of Defense leads the Emergency Response Assistance Program to train first responders. To carry out the program, the Secretary of Defense must consult with the Director of FEMA, the Secretary of Energy, and the heads of any other federal, State and local agencies with expertise and responsibilities in the area of emergency response. The Office of the Secretary of Defense directs the following efforts:

- *Special Operations/Low-Intensity Conflict (SO/LIC)*: Has overall policy and resource oversight for domestic preparedness. Maintains the Counterterror Technical Support Program (CTTS) which is a fast-track R&D program for multi-agency and international aspects of terrorism.
- *Defense Threat Reduction Agency*: Manages and coordinates the extensive technical expertise on chemical and biological defense within the Defense Department. Also involved in counterproliferation, Cooperative Threat Reduction activities, and special weapons technology.
- *Director of Military Support (DOMS)*: Located under the Secretary of the Army, within the office of the Assistant Secretary for Installations, Logistics, and Environment, this office serves as the central point for the coordination of military support to civilian authorities.
- *Reserve Component Consequence Management Program Integration Office*. The Reserve Component Consequence Management Program Integration Office has been established under the command of the Director of Military Support in order to integrate Reserve and Guard components into the national

domestic preparedness strategy. This office will coordinate identification, training, equipping, and exercise of Reservists and Guard components.

US Military Services and Joint Chiefs of Staff

While they are not always part of the CBRN budget, the US military services play a broad role in deterring, defending, and responding to CBRN incidents:

- *Special Operations Command*: Special Mission Units are manned, equipped, and trained to deal with transnational threats, including WMD. Includes members from Army Delta Force, Navy SEAL Team 6, Air Force Special Tactics Squadron 1. Also can include the Army's 75th Ranger Regiment and the 160th Special Operations Regiment. The Special Mission Units are under the command of the Joint Special Operations Command (JSOC) at Fort Bragg, North Carolina.
- *Central Command*: Central Command's area of responsibility extends to the Middle East and much of Africa. Within this area, this command must assure the security of Americans and their property abroad from acts of terrorism. Central Command acts as the military's forward deployed eyes, ears, and arms to counter acts of terrorism within its area of responsibility.
- *United States Army Medical Research Institute of Infectious Diseases (USAMRIID)* Conducts research to develop technologies, procedures, and training programs for medical defense against biological warfare threats and naturally occurring infectious diseases. The lead medical research laboratory for the U.S. Biological Defense Research Program and the only biological containment laboratory in the DOD capable of studying infectious diseases.
- *Technical Escort Unit (TEU)*: Army unit that handles, dismantles, and disposes of chemical and biological weapons and munitions. Based at Aberdeen Proving Ground, Maryland.
- *Soldier and Biological Chemical Command (SBCCOM)*: Formerly Chemical and Biological Defense Command. SBCCOM has responsibility for training development and city training visits. The organization has established a chemical-biological hotline for expert assistance in an emergency, as well as a non-emergency helpline.
- *Navy Medical Research Institute*: Conducts research, development, tests, and evaluations for the Navy and Marine Corps, on infectious diseases, casualty care, and provides biomedical research capabilities to support field laboratories and hospitals.
- *Air Force*: For FY1999 the House appropriated \$120,500,000 for: the provision of crisis response aviation support for critical national security, law enforcement and emergency response agencies This money is provided with the understanding that the President of the United States shall submit to the Congress by March 15, 1999, an interagency agreement for the utilization of Department of Defense assets to support the crisis response requirements of the Federal Bureau of Investigation and the Federal Emergency Management Agency.
- *Chemical/Biological Incident Response Force (CBIRF)*: A Marine Corps unit that is developing the capacity to identify chemical and biological agents, "assess downwind hazards, conduct advanced lifesaving support, and decontaminate patients." Provide communications and enhance transportation capability. In FY97, \$10,000,000 dollars was allocated by DOD for equipment to support CBIRF
- *National Guard*: The Reserve Component Consequence Management Program Integration Office has

been established under the command of the Director of Military Support in order to integrate Reserve and Guard components into the national domestic preparedness strategy. This office will coordinate training, equipping, and exercising of Reservists and Guard components.

- *Rapid Assessment and Initial Detection (RAID) Teams.* There are 22 member teams in 10 States. The RAID teams act in support of first responders at the request of the State or federal government. They are on alert to respond to a suspected or actual WMD attack, assess the situation, provide advice to the local incident commander, and facilitate the arrival of requested DOD equipment, services, and people in the after-effects of an event.
- *Military Reserves:* Reservists, like the Guard, will be utilized to train first responders in their community and be mobilized in the event of an attack. The DOD plans to establish 170 reconnaissance and decontamination teams, drawn mostly from existing chemical companies, to train and be equipped to support the rapid response teams. The Reserve Component Consequence Management Program Integration Office has been established under the command of the Director of Military Support in order to integrate Reserve and Guard components into the national domestic preparedness strategy. This office will coordinate training, equipping, and exercising of Reservists and Guard components.

Possible FY2000 Budget

The Center for Nonproliferation, Monterey Institute of International Studies outlined in its 1999 report the various counterterrorism efforts of the DOD:⁴³

Provides transportation for support teams to the site of terrorist activity. Provides training for first responders at the State and local levels. To date, nearly 10,000 first responders in 30 cities have received training. In FY97, total spending for unclassified terrorism-related programs totaled approximately \$3,671,100,000. For FY99 the House has appropriated \$50,000,000:

to initiate and expand activities of the Department of Defense to prevent, prepare for, and respond to a terrorist attack in the United States involving weapons of mass destruction:

of which \$35,000,000 is to be transferred as follows:

\$4,000,000 to National Guard Personnel (Army)

\$1,000,000 to National Guard Personnel (Air Force)

\$2,000,000 to Operation and Maintenance (Army)

\$20,000,000 to Operation and Maintenance (Army National Guard)

\$8,000,000 to Procurement (Defense-Wide)

of which \$15,000,000 is for: Research, Development, Test and Evaluation (Army) to develop and support a long term, sustainable Weapons of Mass Destruction emergency preparedness training program

Department of Energy

The Department of Energy plays a broad range of roles in defense against CBRN

attacks. It provides first responder training through established programs like the FBI's Hazardous Device School and loans pager-sized radiation detection instruments to FBI accredited bomb technicians.⁴⁴ The DOE also maintains the Radiological Assistance Program (RAP) which provides 24 hour access to personnel and equipment for radiological emergencies. It maintains the Radiation Emergency Assistance Center/Training Site (REAC/TS) which provides around-the-clock direct and consultative assistance in the area of human health effects of radiological hazards. The program also trains Emergency Medical Technicians, physicians, and nurses. This program works closely with DOD's Domestic Preparedness Program. Another element of DOE's anti-terror effort is the Atmospheric Release Advisory Capability (ARAC) which does computer-based predictive monitoring for tracking atmospheric dispersions of radiation and hazardous materials. Total FY97 Department of Energy spending for unclassified terrorism-related programs totaled approximately \$1,420,000,000.⁴⁵

There are a number of other important activities:

Office of Nonproliferation and National Security

This office coordinates DOE activities in nonproliferation, nuclear safeguards and security, and emergency management.

Office of Emergency Management

This office acts as single point of contact for all DOE emergency management and threat assessment-related activities. Operates the Headquarters Emergency Operations Center (EOC), Communications Center, and Departmental emergency communications network. "Ensures a viable technical response is in place for any type of radiological or nuclear accident or incident including radiological releases, U.S. nuclear weapons accidents, or a malevolent event involving an improvised nuclear device or radiological dispersal device."

Office of Defense Programs

The Office of Defense Programs ensures the safety, reliability, and performance of nuclear weapons without underground nuclear testing.

Office of Emergency Response

This office is tasked with developing the ability to immediately respond to radiological accidents or incidents anywhere in the world. Directs seven emergency response capabilities, including Nuclear Emergency Search Teams.

Nuclear Emergency Search Team

DOE also provides the Nuclear Emergency Search Team (NEST). NEST helps resolve nuclear and radiological terrorist attacks. NEST is comprised of: an advisory team to the Lead Federal Agency, search teams that can also train and equip local and state responders, and joint technical operations teams that work with explosive ordnance disposal teams to neutralize a nuclear or radiological device. The FY 2001 budget request for NEST is \$44 million.⁴⁶

Its staff consists of engineers, scientists, and other technical specialists from DOE's national laboratories and other contractors. It is deployable within 4 hours of notification with specially trained teams and equipment to assist the FBI in handling nuclear or radiological threats. NEST assets include intelligence, communications, search, assessment, access, diagnostics, disablement, operations, containment/damage limitations, logistics, and health physics capabilities.

Radiological Assistance Program

Another program is the Radiological Assistance Program. The program is responsible for coordinating local bomb squad responder plans with national response plans. The program divides the country into eight regions, and each region has a Regional Coordinating Office, a Federal Response Coordinator, and at least three response teams.⁴⁷

The Nuclear Safeguards, Security, and Emergency Operations Program

The Nuclear Safeguards, Security, and Emergency Operations program is the primary DOE program to protect sensitive nuclear materials and assets. The Office of Security and Emergency Operations administers the program in a process involving updating threat assessments, security policy and implementation, and consequence management plans. Included

in the Security and Emergency Operations program is a technology development and applications program. The technology program has the responsibility of deploying security systems at DOE sites and for DOE security forces. The security systems defend against a variety of weapons, including explosives and chemical attacks. The FY 2001 requested budget includes \$25 million for the technology program.⁴⁸

Research and Development

DOE is requesting \$92 million for FY 2001 for research and development. The research into chemical, materials, and biological sciences helps DOE develop defenses against CB attacks. DOE's Chemical and Biological Nonproliferation Program (CBNP) plays an active part in combating the threat of CB weapons. The OMB states, "The strategy of the CBNP relies on close linkages between technology development and systems analysis and integration to systematically and comprehensively address the domestic chemical and biological terrorism threat."⁴⁹ CBNP's funding has grown from \$17 million in FY 1997 to a projected \$63 million in FY 2001.⁵⁰

Total Program Spending

The following chart on DOE counterterrorism spending adapted from the 2000 OMB counterterrorism funding report shows no significant increase in funding since FY 1999. The requested FY 2001 budget is \$663.53 million.⁵¹

Table Eighteen

Department of Energy Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	498.98	611.05	647.61	663.53
Law Enforcement and Investigative	0.94	0.94	0.94	0.94
Physical Security of Government Facilities and Employees	389.00	449.85	468.22	471.05
Preparing for and Responding to Terrorist Acts	84.38	84.80	94.35	97.74
Research and Development	24.66	75.46	84.10	93.80
<i>WMD Preparedness</i>	275.78	350.75	366.31	364.23
Physical Security of Government	186.50	192.25	189.62	174.45
Preparing for and Responding to WMD Terrorism	84.38	84.80	94.35	97.74
Equipment for First Responders	2.10	1.40	8.00	9.55
Federal Planning/Exercises	2.58	3.05	3.05	3.40

First Responder Training and Exercises	0.20	0.20	3.85	4.08
Other	0.50	1.16	1.45	1.45
Special Response Units	79.00	79.00	78.00	79.31
Research and Development	22.90	73.70	82.34	92.04
Basic Research, incl. Gene Sequencing	3.00	4.80	11.00	14.00
Detection/Diagnostics	14.50	16.50	21.00	22.50
Modeling, Simulation, Systems Analyses	3.60	2.00	6.74	6.74
Other	0.00	47.60	40.40	45.60
Personal/Environment Decontamination	1.80	2.80	3.20	3.20
*OMB Highlighted Programs				
Nuclear Emergency Search Team	-	-	-	44.00
Technology Development and Applications	-	-	-	25.00
Radiological Assistance Program	-	-	-	4.00
Research and Development	-	-	-	92.00
Nuclear Safeguards, Security and Emergency Operations	-	-	25.00	N/A

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Environmental Protection Agency

EPA has several counterterrorism functions. These include:⁵²

- Responsibility over preparation and response to emergencies with oil, hazardous substances, and certain radiological materials.
- Assist in the Domestic Preparedness Program on hazmat identification and with environmental cleanup.
- Develop community response plans to deal with accidental or deliberate releases of hazardous substances and participate in the first responder training program.

The EPA's preparedness and response activities are exercised under the authority of the National Oil and Hazardous Substances Pollution Contingency Plan (NCP) and the Radiological Response Program. The EPA also provides technical assistance, response coordination and management, and resource assistance to local and state responders under the National Response System (NRS). The NRS is the federal government's mechanism for emergency response to releases of hazardous contaminants that threaten human health or the environment.⁵³

Presidential Decision Directive 63 named the EPA lead agency for the Water Supply Sector. PDD 39 directed the EPA to assist the FBI with hazard and threat assessment in a

terrorist attack and to assist FEMA with decontamination and cleanup. The directives allow the EPA to participate in both crisis and consequence management phases of a terrorist attack.⁵⁴ The EPA also contributes to the DOD's Domestic Preparedness Program and provides hazardous materials (HAZMAT) training to areas not served by the Domestic Preparedness Program.⁵⁵

Office of Solid Waste and Emergency Response

Chemical Emergency Preparedness and Prevention Office (CEPPO) is the primary office within the Office of Solid Waste and Emergency Response that coordinates preparedness and prevention of chemical accidents and oil spills. It is responsible for the overall management and coordination of EPA's activities involving accident prevention, preparedness, and response for natural and manmade disasters. It also oversees the EPA's Counter-Terrorism Planning Preparedness Program and the National Security Emergency Preparedness Program.

On-Scene Coordinator (OSCs)

The Federal On-Scene Coordinator is the primary official under the National Response System. The EPA has approximately 215 OSCs for inland zones and the U.S. Coast Guard provides OSCs for coastal zones. OSCs are activated by the National Response Center, a first alert center for CBRN substances released into the environment. An OSC is the point of contact between federal and local officials and has the authority to manage all response efforts at the incident scene. An OSC can call upon the Environment Response Team (ERT), the Radiological Emergency Response Team (RERT), and the U.S. Coast Guard National Strike Force (NSF).⁵⁶ The FY 2001 budget request for these activities is \$3.2 million.⁵⁷

Current Budget

The following chart on EPA counterterrorism spending adapted from the 2000 OMB counterterrorism funding report shows there has been no change in funding from FY 1998 to FY 2001 requested. All EPA counterterrorism funding has gone towards WMD preparedness.⁵⁸

Table Nineteen

Department of Energy Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	2.00	2.00	2.00	3.20
Preparing for and Responding to Terrorist Acts	2.00	2.00	2.00	3.20
<i>WMD Preparedness</i>	2.00	2.00	2.00	3.20
Preparing for and Responding to WMD Terrorism	2.00	2.00	2.00	3.20
Special Response Units	2.00	2.00	2.00	3.20
*OMB Highlighted Programs				
WMD Coordinator, Equipment and Training	-	-	-	3.20

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Federal Emergency Management Agency

Presidential Decision Directives 39 and 62 designated FEMA the lead federal consequence management agency if state and local officials request federal assistance.⁵⁹ Initially, the FBI maintains command until the Attorney General transfers the lead agency role to FEMA.⁶⁰ FEMA's FY 2001 requested budget for WMD preparedness is \$34.52 million. \$4 million will go towards the new Urban Search and Rescue Teams. Six teams will be created and these teams will operate in a CBRN contaminated environment. \$24 million will go towards local and state assistance.⁶¹ The Center for Nonproliferation, Monterey Institute of International Studies has summarize FEMA's counterterrorism efforts as follows:⁶²

- The Federal Emergency Management Agency (FEMA) acts in support of the FBI in Washington, DC, and on the scene of the crisis until the Attorney General transfers the lead to FEMA.
- Though state and local officials bear primary responsibility for consequence management, FEMA is in charge of the federal aspects of consequence management to a terrorist act. Consequence management includes protecting public health and safety and providing emergency relief to state governments, businesses, and individuals.
- Chairs the Senior Interagency Coordination Group for consequence management policy issues and initiatives (includes representatives from DOD, DOJ, DOE, HHS, DOT, Agriculture, EPA, and General Services Administration).

Response and Recovery Directorate

Manages the Rapid Response Information System (RRIS) to inventory physical assets and equipment available to state and local officials and provides a database of chemical and

biological agents and safety precautions.

Preparedness, Training, and Exercises Directorate

This office trains emergency managers, firefighters, and elected officials in consequence management through the Emergency Management Institute and the National Fire Academy at the National Emergency Training Center in Emmitsburg, MD. Conducts exercises in WMD terrorism consequence management through the Comprehensive Exercise Program (CEP). These exercises provide the opportunity to investigate the capability of the Federal Response Plan to effectively deal with consequence management and test the ability of different levels of response to interact.

United States Fire Administration

Provides training to firefighters and other first responders through the National Fire Academy in conjunction with the Preparedness, Training, and Exercises Directorate.

National Fire Academy and Emergency Management Institute

FEMA's Emergency Management Institute and National Fire Academy have both instituted new courses in first responder training. FEMA provides WMD and first responder training at its National Fire Academy and its Emergency Management Institute in Emmitsburg, Maryland. The Academy and Institute also provide materials to local and state officials to themselves train responders. Some of these courses are train the trainer courses. About 71,000 individuals have participated in the Academy's training from October 1, 1997, through September 30, 1999.⁶³ A March, 2000, GAO report provides a program description:⁶⁴

- FEMA provides WMD training to first responders through its National Fire Academy and its Emergency Management Institute. These organizations offer training at their combined residence campus in Emmitsburg, Maryland, and provide course materials to individuals for self-study or to
- state and local training organizations for their use. In addition, they offer courses that were not developed specifically for dealing with WMD incidents but would assist first responders with those incidents.
- The Fire Academy offers six courses to prepare first responders to manage the consequences of a terrorist WMD incident. It provides the training at its campus and also provides training materials for use by individuals and state and local training organizations. One course, its 6-day incident

management course, is offered on campus and to state and local training organizations for their use. The other five courses are offered off campus using Academy-developed materials. These courses train individuals in emergency response to terrorism through (1) a self-paced, self-study course; (2) a basic concepts course, the same 16-hour course offered by Justice in its Metropolitan Firefighters program;¹⁵ (3) a 2-day more advanced course for the first on-scene supervisor; (4) a 2-day more advanced course for the first on-scene emergency medical services personnel; and (5) a 2-day more advanced course for the first on-scene hazardous materials personnel. Many of these are train-the-trainer courses. About 71,000 students have participated in the Fire Academy's offerings from October 1, 1997, through September 30, 1999. This includes students trained by Academy instructors and by student instructors.

- The Emergency Management Institute also offers several courses related to the use of WMD. It offers a 5-day course, integrated emergency management consequences of terrorism, on campus. Off campus, it offers a 1-day course, senior officials workshop on terrorism, and a series of courses involving specific WMD scenarios, such as an anthrax incident, to aid senior officials to respond to and manage a WMD event.

Both organizations offer courses on and off campus that are not specifically WMD related but that can help first responders deal with WMD incidents. For example, the Institute has a 5½-day radiological emergency response operations course that provides training on response and management of radiological incidents.

Funding for FEMA's first responder training totaled \$4 million in fiscal year 1998 and \$3.6 million in fiscal year 1999 and is projected at about \$6.4 million in fiscal year 2000. Included are small, antiterrorism training grants that FEMA makes available to the states, either directly or through its Fire Academy. FEMA's direct grants totaled about \$1.2 million in fiscal years 1998 and 1999, or about \$23,000 per state. The states can use these grants for a variety of purposes. For example, officials we met with in North Carolina and Virginia said that they have used FEMA grant money to help fund training in their community college and fire academy systems. The Academy's grants totaled about \$2 million in fiscal year 1998 and \$4 million in fiscal year 1999 and are budgeted for \$4 million for fiscal year 2000. The states have to apply for the grants and can use the funds to pay for instructor travel, training equipment, and the use of facilities.

The Academy's and Institute's programs have been examples that critics like the GAO have cited in arguing for better federal integration of terrorism programs. DOD administers the Domestic Preparedness Program and DOJ administers the Metropolitan Firefighters program. The problem is the potential for and actual overlap in first responders' training among the DOJ, DOD, and FEMA programs. Furthermore, critics argue it is inefficient for responders in each city to attend three programs from three departments when an integrated program would save time and resources. However, DOJ and FEMA focus on slightly different populations. DOJ concentrates on the large metropolitan areas while FEMA makes its training available throughout the United States.⁶⁵

The following chart on FEMA counterterrorism spending adapted from the 2000 OMB counterterrorism funding report shows tremendous increases in funding from FY 1998 to FY 2001 requested. Funding has increased over 480% to \$34.52 million, and all of the money goes towards WMD preparedness.⁶⁶

Table TwentyFederal Emergency Management Agency Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	5.92	17.61	30.77	34.52
Physical Security of Government Facilities and Employees	1.46	1.96	2.13	2.13
Preparing for and Responding to Terrorist Acts	4.45	15.64	28.64	32.39
<i>WMD Preparedness</i>	5.92	17.61	30.77	34.52
Physical Security of Government	1.46	1.96	2.13	2.13
Preparing for and Responding to WMD Terrorism	4.45	15.64	28.64	32.39
Federal Planning/Exercises	0.92	3.02	4.50	4.95
First Responder Training and Exercises	2.76	8.31	14.56	13.96
Other	0.00	0.00	0.08	0.08
Other Planning and Assistance to State/Locals	0.76	4.31	9.50	9.50
Special Response Units	0.00	0.00	0.00	3.90
*OMB Highlighted Programs				
Assistance to State and Local Authorities	-	-	-	24.00
Urban Search and Rescue Teams	-	-	-	4.00

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

General Services Administration

Most GSA money is spent on the physical protection of federal facilities. The following chart on GSA counterterrorism spending report shows that no money is being spent specifically on CBRN threats.⁶⁷

Table Twenty-OneGeneral Services Administration Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	89.60	133.50	92.80	116.96
Law Enforcement and Investigative Activities	13.90	15.30	15.10	15.39
Physical Security of Government Facilities and Employees	72.90	115.30	74.90	99.41
Preparing for and Responding to Terrorist Acts	2.80	2.90	2.80	2.16

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Department of Health and Human Services

HHS plays a critical role in responding to biological attacks. Presidential Decision Directive 62 designated the HHS as the lead Federal agency for medical emergency responses arising from WMD incidents. HHS is also in charge of public health and medical consequence management of WMD attacks as mandated by Emergency Support Function 8 of the Federal Response Plan. Twelve agencies support the HHS in consequence management.⁶⁸ These include

- *Centers for Disease Control (CDC)*: The federal agency responsible for protecting the public health of the country through prevention and control of diseases and other preventable conditions and responding to public health emergencies. The CDC also works with national and international agencies to eradicate or control communicable diseases and other preventable conditions.
- *Office of Emergency Preparedness*: Coordinate the health and medical response of the Federal government, in support of state and local governments, in the aftermath of terrorist acts involving chemical or biological agents. \$2,500,000 appropriated for the Office of Emergency Preparedness in the FY99 Omnibus bill for a national medical disaster system.
- *Metropolitan Medical Strike Teams (MMST)*: Provide initial on-site response and safe patient transportation to hospital emergency rooms, provide medical and mental health care to victims and will move victims to other regions should local health care resources be overrun during a terrorist attack. Prototypes of the MMST were established in Washington, DC and in Atlanta, GA during the 1996 Summer Olympic Games. Approximately twenty-five cities have been chosen to begin development of the teams.
- *National Institutes of Health (NIH)*: Federal focal point for biomedical research, including extensive vaccine research. \$10,000,000 appropriated in the FY99 Omnibus bill for vaccine research and development in support of bioterrorism preparedness.

Metropolitan Medical Response Systems

HHS is also responsible for aiding local authorities in dealing with the impact of a biological attack. Congress passed the Defense Against Weapons of Mass Destruction Act of 1996, also known as the Nunn-Lugar-Domenici Act, after the Oklahoma City bombing. The Act authorized funds for the DOD to help the Secretary of HHS establish a program to enhance local medical response for a CBRN attack. Metropolitan Medical Response Systems (MMRS) was created under HHS' Office of Emergency Preparedness. In 1999, MMRS were in 27 cities and consist of trained and equipped local emergency teams. The Systems also participate in DOD's Domestic Preparedness Program.⁶⁹ The President has requested \$30 million for FY 2001 for HHS' WMD Preparedness and MMRS. The Office of Emergency Preparedness plans on

developing 25 new Systems for a total of 97 Systems by the end of FY 2001.⁷⁰ The end goal of HHS is to have MMRS for the 120 most populous cities

The HHS released a fact sheet describing the MMRS:⁷¹

Because of the very rapid response time that would be required in countering the consequences of such terrorist acts, HHS' strategic plan includes developing partnerships with local jurisdictions to develop an enhanced Metropolitan Medical Response System (MMRS) as the primary local resource in responding to the health and medical consequences of a nuclear, biological or chemical (N/B/C) terrorist incident. The MMRS plan serves to coordinate the public safety, public health and health services sector responses to an N/B/C terrorist incident. The MMRS is an enhanced local capability of the existing system. At the same time, HHS is improving the federal capability to rapidly augment state and local responses. The federal medical response component includes four national and geographically dispersed NMRT/WMDs (National Medical Response Team/ Weapons of Mass Destruction).

The Metropolitan Medical Response System (MMRS) concept was generated by a group of state and local subject matter experts that met in July of 1995 at the request of HHS' Office of Emergency Preparedness. The original concept of a Metropolitan Medical Strike Team soon expanded into the current systems approach. Pilot tested in the Washington, D.C., and Atlanta areas, systems development was initiated in fiscal year 1997 in the following 25 cities: New York, N.Y.; Los Angeles, Calif.; Chicago, Ill.; Houston, Texas; Philadelphia, Pa.; San Diego, Calif.; Detroit, Mich.; Dallas, Texas; Phoenix, Ariz.; San Antonio, Texas; San Jose, Calif.; Baltimore, Md.; Indianapolis, Ind.; San Francisco, Calif.; Jacksonville, Fla.; Columbus, Ohio; Milwaukee, Wis.; Memphis, Tenn; Boston, Mass.; Seattle, Wash.; Denver, Colo.; Kansas City, Mo; Honolulu, Hawaii; Miami, Fla.; and Anchorage, Alaska. The following 20 jurisdictions initiated systems development in fiscal year 1999: Pittsburgh, Pa; Nashville, Tenn; Charlotte, N.C.; Cleveland, Ohio; El Paso, Texas; New Orleans, La; Albuquerque, N.M.; Ft. Worth, Texas; Oklahoma City, Okla.; Austin, Texas; St. Louis, Mo.; Salt Lake City, Utah; Long Beach, Calif.; Tucson, Ariz.; Oakland, Calif.; Portland, Ore.; Minneapolis/St. Paul, Minn.; Tulsa, Okla.; Sacramento, Calif.; and the Hampton Roads, Va. area. The goal is to develop Metropolitan Medical Response Systems for the 120 most populous metropolitan areas in the United States within five years. HHS is currently working to develop a "balance of the nation" strategy for those jurisdictions that would not be included in the list of 120 most populous cities.

The MMRS emphasizes enhancement of local planning and response system capability, tailored to each jurisdiction, to care for victims of a terrorist incident involving a weapon of mass destruction. These systems are characterized by: a concept of operations, specially trained responders, special pharmaceuticals, detection, personal protective equipment, decontamination, communication, and medical equipment and other supplies, and enhanced emergency medical transport and emergency room capabilities. The program includes a focus on biological response, including early warning and surveillance, mass casualty care and plans for mass fatality management. The concept of operations includes the local jurisdictions' plan regarding anticipated requirements federal health and medical augmentation assistance to include the forward movement of victims (when local healthcare systems become overloaded) via the National Disaster Medical System.

HHS recognizes that each city has its own unique, existing emergency medical system. Many have special HAZMAT response capabilities. Therefore, specific plans must be developed uniquely for each city that can build on existing systems and adapt them to meet a nuclear, biological or chemical challenge. Implementation of these plans will include special equipment, supplies, and pharmaceutical procurement and training. A "concept of operations" plan will also be developed with each city regarding federal health and medical augmentation assistance in response to a threatened or actual terrorist incident involving

weapons of mass destruction.

National Pharmaceutical Stockpile Program

HHS began to use the CDC to build a national stockpile of vaccines and medicines against potential biological and chemical agents in FY 1999. The funding request for FY 2001 is \$52 million.⁷² However, there has been criticism of the vaccine program. According to a June, 1999, GAO report, the intelligence agencies disagree with HHS on which vaccine stockpiles should be built, revealing a lack of coordination between agencies for medical countermeasures:⁷³

We have also observed a disconnect between intelligence agencies' judgments about the more likely terrorist threats particularly the chemical and biological terrorist threat and certain domestic preparedness program initiatives. For example, the Department of Health and Human Services' (HHS) fiscal year 1999 budget amendment proposal for its bioterrorism initiative included building for the first time a civilian stockpile of antidotes and vaccines to respond to a large- scale biological or chemical attack and expanding the National Institutes of Health's research into related vaccines and therapies. Specifically, the Omnibus Consolidated and Emergency Supplemental Appropriations Act (P. L. 105- 277) included \$51 million for the Centers of Disease Control and Prevention to begin developing a pharmaceutical and vaccine stockpile for civilian populations.

HHS' legislatively required operating plan discusses several chemical and biological agents selected for its stockpiling initiatives. These agents were selected because of their ability to affect large numbers of people (create mass casualties) and tax the medical system. We observed that several of the items in HHS' plan did not match individual intelligence agencies' judgments, as explained to us, on the more likely chemical or biological agents a terrorist group or individual might use. 5 HHS had not documented its decision making process for selecting the specific vaccines, antidotes, and other medicines cited in its plan. Thus, it was unclear to us whether and to what extent intelligence agencies' official, written threat analyses were used in the process to develop the list of chemical and biological terrorist threat agents against which the nation should stockpile. Further, we have not seen any evidence that HHS' process incorporated the many disciplines of knowledge and expertise or divergent thinking that is warranted to establish sound requirements to prepare for such a threat and focus on appropriate medical preparedness countermeasures.

An April, 2000 GAO report, highlights again the difference between the HHS and other agencies' judgements in which vaccines should be stockpiled:⁷⁴

Without the benefits that a threat and risk assessment provides, many agencies have been relying on worst case scenarios to generate countermeasures or establish their programs. Worst case scenarios are extreme situations and, as such, may be out of balance with the threat. In our view, by using worst case scenarios, the federal government is focusing on vulnerabilities (which are unlimited) rather than credible threats (which are limited). By targeting investments based on worst case scenarios, the government may be over funding some initiatives and programs and under funding the more likely threats the country will face. As an example, we have testified that the Department of Health and Human Services is establishing a national pharmaceutical and vaccine stockpile that does not match intelligence agencies' judgments of the more likely chemical and biological agents that terrorists might use. In some of our current work at other federal agencies, we are continuing to find that worst case scenarios are being used in planning efforts to develop

programs and capabilities.

These GAO comments understate a problem that permeates the federal government response to the threat of biological attacks, and inevitably to the state, local, and private sector response as well. First, there seems to be no systematic examination of lethality data and effects models to determine what data and models are credible and what level of uncertainty is involved. Second, there is no systematic effort to determine how the behavior of military agents might differ from the normal disease, and what steps might have been taken to limit detection and defeat effective treatment. Third, there is no evidence of a systematic technical net assessment of the probable progress in defensive measures like vaccines versus progress in the offensive technologies necessary to defeat them. Finally, the entire concept of “cost to defeat” given measures like stockpiling by focusing on alternative agents seems to be alien to the biological sciences community.

There is, of course, no way to determine what level of classified activity is taking place. In general, however, the apparent tendency to treat biological weapons as if their effectiveness and treatment was a known quantity, and as if their use was an outbreak of disease rather than a carefully planned act of war is deeply disturbing. Such an approach may be valid in the near term for terrorists, but it is not valid for state actors, particularly because it often leads to the assumption that the US will only have to deal with one kind of attack at a time, and that some sort of reliable detection and characterization system will be present.

Public Health Surveillance System for WMD

CDC is leading the effort to upgrade the public health surveillance system to detect WMD attacks on the homeland. The FY 2001 requested budget of \$86.5 million would allow the CDC to expand local and state preparedness efforts, improve WMD detection capabilities, and improve laboratory and medical capacity at the local, state, and national level.⁷⁵

Research and Development

HHS research focuses on developing defenses against potential CB attacks. The FY 2001 requested funding is \$92 million. \$45.2 million will go to the NIH for R&D on vaccines,

therapeutics, diagnostics, and genomics. \$30 million will go to the Office of Secretary for R&D on improved civilian stockpiles of anthrax and small pox vaccines. \$9 million will go to the FDA to develop rapid diagnostic tools and to expedite the pharmaceutical approval process of possible medicines against CB agents. HHS R&D funding will also go to the CDC for its Rapid Toxic Screen project and to research equipment for first responders.

Total Funding

The following chart on HHS counterterrorism spending adapted from the 2000 OMB counterterrorism funding report shows that HHS' counterterrorism efforts are being exclusively focused on WMD preparedness. The FY 2001 requested budget of \$265.37 million is slightly lower than FY 2000 budget, but from FY 1998 to FY 2000, funding increased over 16 fold.⁷⁶

Table Twenty-Two

Department of Health and Human Services Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	15.90	173.12	277.56	265.37
Preparing for and Responding to Terrorist Acts	0.00	138.25	165.60	173.63
Research and Development	15.90	34.87	111.96	91.74
<i>WMD Preparedness</i>	15.90	173.12	277.56	265.37
Preparing for and Responding to WMD Terrorism	0.00	138.25	165.60	173.63
Medical Responder Training Exercises	0.00	3.00	1.00	2.00
Other	0.00	2.00	3.10	10.60
Other Planning and Assistance to State/Locals	0.00	16.25	16.50	17.43
Public Health Infrastructure/Surveillance	0.00	62.00	88.00	85.50
Special Response Units	0.00	4.00	5.00	6.10
Stockpile of Vaccines and Therapeutics	0.00	51.00	52.00	52.00
Research and Developments	15.90	34.87	111.96	91.74
Basic Research, incl. Gene Sequencing	13.00	17.23	21.76	21.76
Detection/Diagnostics	0.00	5.68	5.68	8.28
Other	0.00	1.85	31.72	0.00
Personal/Collective Protection	0.00	0.00	0.00	1.20
Therapeutics/Treatments	0.00	3.98	4.35	4.35
Vaccines	2.90	6.13	48.45	56.15
*OMB Highlighted Programs				
Strengthening the Public Health Surveillance System for WMD	-	-	-	87.00
National Pharmaceutical Stockpile Program	-	-	-	52.00

Metropolitan Medical Response Systems and WMD Preparedness	-	-	-	30.00
Research and Development	-	-	-	92.00

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Holocaust Memorial Museum

Table Twenty-One shows Holocaust Memorial Museum counterterrorism spending adapted from the 2000 OMB counterterrorism funding report shows that \$2 million was appropriated in FY 1999 for the physical security of government facilities and employees.⁷⁷

Table Twenty-Three

Holocaust Memorial Museum Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	0.00	2.00	0.00	0.00
Physical Security of Government Facilities and Employees	0.00	2.00	0.00	0.00

Department of the Interior

Department of the Interior counterterrorism spending normally averages y around \$10 million.⁷⁸ The vast majority of the money goes to physical protection facilities.

Table Twenty-Four

Department of the Interior Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	10.92	14.01	9.66	9.66
Law Enforcement and Investigative Activities	0.17	0.20	0.22	0.22
Physical Security of Government Facilities and Employees	10.71	13.77	9.40	9.40
Preparing for and Responding to Terrorist Acts	0.05	0.05	0.05	0.05
<i>WMD Preparedness</i>	0.22	0.25	0.27	0.27
Law Enforcement and Investigative Activities	0.17	0.20	0.22	0.22
Preparing for and Responding to WMD Terrorism	0.05	0.05	0.05	0.05
Other	0.05	0.05	0.05	0.05

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Department of Justice and Federal Bureau of Investigation

Presidential Decision Directives 39 and 62 designated the DOJ, through the FBI, as the lead agency in domestic terrorism crisis management.⁷⁹ The FBI is responsible for preventing and responding to domestic terrorism.⁸⁰ It gathers and assesses intelligence on domestic threats.⁸¹ Its Criminal Division is tasked with all criminal investigations not specifically given to another division. Investigates incidents of computer-related crime and cyber-terrorism. Its National Security Division manages the Awareness of National Security Issues and Response (ANSIR) Program, a means of distributing unclassified threat information on terrorism and other national security threats to corporate security workers, law enforcement, and other government agencies. The Criminal Investigative Division leads the FBI's Legal Attaché Program to conduct law enforcement investigations abroad, including those pertaining to terrorist acts. It has a broad mandate for conducting investigations into organized crimes, and is. "Responsible for contacts with other Executive Branch agencies; Interpol; foreign police and security officers based in Washington, D.C.; and national law enforcement associations."

According to a speech by President Clinton in 1995, "A CIA official serves as the deputy chief of the International Terrorism Section at the FBI." This office works to investigate acts of international terrorism and foreign terrorists within the borders of the United States and abroad.

There is also an office for Domestic Terrorism/Counterterrorism Planning This office contains the domestic terrorism operations unit, which monitors militias; the special events management unit; the weapons of mass destruction countermeasures unit; and the domestic terrorism analysis unit. It serves as the "program manager for WMD threats and incidents, including the coordination of the threat credibility assessment process," and provides a point of contact for assistance to the field and to other agencies. It helps staff the FBI HQ Strategic Information Operations Center (SIOC) during exercises and actual incidents, and works in conjunction with DOE's Office of Safeguards and Security to ensure that FBI, DOE, and local elements know their responsibilities and roles during a terrorist incident at a DOE site.

This office also creates Domestic Emergency Support Teams (DEST) The composition of a rapid deployment team will vary case-by-case and will include members of several agencies. Overall policy coordination rests with the Domestic Terrorism/Counterterrorism Planning office under the weapons of mass destruction unit. The role of the DEST is to provide expert advice and guidance to the FBI's On-Scene Commander (OSC) for the event, and to coordinate follow-on response assets.

National Domestic Preparedness Office (NDPO)

There are a wide range of additional DOJ and FBI activities. The Attorney General directed the FBI in October 1998 to lead an interagency coordination initiative to serve as the single point of contact and clearinghouse for WMD information for state and local emergency responders. Federal agencies involved include HHS, DOD, DOE, EPA, DOJ/OJP, and FEMA. Other federal agencies interested in participating include the U.S. Coast Guard, Veteran's Administration, and the Nuclear Regulatory Commission.

The NDPO was set up in ways designed to ensure that it did not replace or usurp any agency's authority and that it would rather serve as a central coordinating entity with the goal of integrating and streamlining federal assistance:⁸²

The NDPO will be an interagency effort to enhance coordination among federal programs offering terrorism preparedness assistance to states and local communities. As such, it is intended to serve as the central coordinating office and information clearinghouse for federal assistance programs, with the goal of integrating and streamlining government assistance. As an information clearinghouse, the NDPO will provide details on federal assistance programs to state and local response agencies. The NDPO is not intended to be the creation of a new federal bureaucracy or to usurp the assistance programs under the management of other agencies, but rather to be a "one-stop shop" for state and local responders seeking information regarding federal domestic preparedness assistance and as a forum for federal domestic preparedness programs to coordinate policy affecting those programs.

The NDPO will be organized into six program areas to coordinate and share information related to federal domestic preparedness programs and to provide state and local first responders with a single, central point of contact for information about these programs. These program areas will provide an interagency forum in each area for coordination of federal policy and program assistance to state and local emergency responders. For instance, federal programs providing training will be assessed in this forum in order to eliminate duplication and to ensure that training programs adhere to minimum national standards. The NDPO will be staffed by federal, state and local program coordinators and experts, most of whom are already engaged on a full- or part-time basis in domestic preparedness activities. In the coordination of federal programs, it is the NDPO's objective to ensure proper representation of experts from all disciplines responsible for domestic preparedness and emergency response. However, NDPO staff will not supplant the functions that are the responsibilities of its constituent departments and agencies, but rather serve as a

forum to coordinate these programs.

The NDPO will not serve, nor is it intended to serve, as an operational entity. Response activities will remain with the various departments and agencies whose functions and responsibilities in a WMD event are described in the Federal Response Plan Terrorism Annex.

The NDPO describes its functions and activities as follows:⁸³

A Vision for Working with First Responders to Enhance Domestic Preparedness - The NDPO will provide a forum to assess training needs at all levels and identify solutions as part of a national training strategy. The NDPO will act as a clearinghouse for information about federal WMD training, including the establishment and maintenance of a training catalog for first responders. The NDPO will not have “veto power” over any agency’s programs, but rather, NDPO will work to avoid duplication among the federal programs by providing a forum to coordinate federal efforts.

Exercises - The NDPO will provide WMD exercise recommendations, assistance and technical support to federal, state or local agencies planning efforts. The NDPO, in its coordinating role, will facilitate the sharing of lessons learned through maintenance of databases, “after-action reports”, and analyses. With the participation of all federal agencies involved in conducting WMD exercises, the NDPO will be able to facilitate the planning and coordination of WMD exercises between federal, state, and local officials.

Equipment/Research Development - The NDPO will coordinate federal efforts to provide the emergency response community with equipment necessary to prepare for, and respond to, a WMD terrorist incident. NDPO will help establish and maintain a Standardized Equipment List (SEL) to guide the responder community in identifying the types and models of equipment available which meet agreed upon standards of performance and reliability. The NDPO will facilitate the dissemination of information about new and developing technologies through the member agencies of the NDPO. Existing technology review panels, such as the Interagency Board (IAB, co-chaired by FBI and DoD), will be leveraged to ensure interoperability, best performance, and reliability of equipment produced for the response communities.

Information Sharing and Outreach - State and local participation in the NDPO is a significant mission success factor. As such, personnel estimates are based upon the goal of ensuring that state and local experts are well-represented in each of the program areas. Therefore, the NDPO hopes to fill approximately one-third of its program staff, or 20 positions with state and local representatives, with approximately three state and local personnel per functional area. Participation from federal agencies involved in preparedness, planning, and response is essential to ensuring that federal programs meet the needs of state and local communities. The role of each of the federal partners is to assist state and local jurisdictions in enhancing their domestic preparedness capabilities by providing assistance in the areas of planning, equipment, technical assistance, training, exercise support, and information. Each federal partner will continue to provide its equipment, training, exercise, and technical assistance programs, but each will do so consistent with agreed upon national WMD preparedness policy and guidelines. The EPA supports federal counterterrorism programs by using and building upon the established hazardous materials response structure and mechanism at the federal, state, and local level.

Public Speaking Assistance -- The NDPO will coordinate public speaking engagements relevant to domestic preparedness and its programs by maintaining a list of qualified speakers and topics. The NDPO will be able to provide public speaking assistance at the national, regional, state, and local levels. Through its information-sharing efforts, appropriate speakers will be recommended for upcoming speaking engagements. In addition to speakers representing NDPO itself, the NDPO will maintain a voluntary database for speakers with expertise in other areas. This data will be drawn from all of the participating agencies and regions nationwide.

Health and Medical Services - Specifically, the NDPO will serve as a “one-stop-shopping” point of information and referral for WMD-related health and medical preparedness issues and questions from stakeholders, states, and local jurisdictions. Second, it will serve as a mechanism for Health and Human

Services to facilitate the coordination and review of health and medical issues with regard to domestic preparedness. Health care systems must have the ability to meet the unique challenges posed by a terrorist act involving a WMD. It will fall upon the local jurisdiction's existing public health and medical systems to manage adequately and effectively the human health consequences of a WMD terrorist incident. Providing appropriate care for the affected population and obtaining critical health system assets, including health professionals, pharmaceuticals, equipment, and facilities, are crucial to a successful response. Health system response requirements are driven by the type of WMD incident encountered, and the setting in which it occurs (rural community, suburb, city, or major metropolitan area). A chemical incident will result in immediate effects at a known site, on-scene determination of the causative agent, and a timely response. The effects of the release of a biological weapon, however, may not be apparent for days or even weeks and would include response issues such as mass prophylaxis, mass patient care, mass fatality management and infection control.

It is too soon to appraise the NPDO's effectiveness, but the GAO noted the need for an agency such as the NDPO to coordinate federal assistance to local and state responders in testimony it gave in April 2000:⁸⁴

The federal government cannot prepare for CBRN incidents on its own. Several improvements are also warranted in intergovernmental relations between federal, state and local governments. For example, we found that federal agencies developed some of their assistance programs without coordinating them with existing state and local emergency management structures. In addition, the multitude of federal assistance programs has led to confusion on the part of state and local officials. One step to improve coordination and reduce confusion has been the creation of the National Domestic Preparedness Office within the Department of Justice to provide "one stop shopping" to state and local officials in need of assistance. This office has recently prepared a draft plan on how it will provide assistance.

There is still a need to better focus and coordinate federal programs to assist state and local governments prepare for terrorist CBRN attacks. For example, while local officials have praised federal CBRN training programs, some of the initial programs failed to leverage existing state and local response mechanisms. Further, some local officials have viewed the growing number of CBRN training programs as evidence of a fragmented and possibly wasteful federal approach toward combating terrorism. For example, at about the same time the Department of Defense was developing its Domestic Preparedness Program courses, FEMA and the Department of Justice were jointly developing a similar or potentially overlapping 2-day basic concepts course on emergency response to terrorism. Similarly, multiple programs for equipment—such as the separate DOD and Public Health Service programs and the new Department of Justice equipment grant program—are causing frustration and confusion at the local level and are resulting in further complaints that the federal government is unfocused and has no coordinated plan or desired outcome for domestic preparedness.

A major federal initiative to provide better focus and to coordinate federal assistance programs is the National Domestic Preparedness Office. The Office, which was recently funded in the Consolidated Appropriations Act for Fiscal Year 2000, is just getting organized. The Office will function as an interagency forum to coordinate federal policy and program assistance for state and local emergency responders. For instance, the Office will assess federal training programs to eliminate duplication and ensure that the training adheres to minimum national standards. It is to coordinate and serve as an information clearinghouse for federal programs devoted to supporting state and local emergency responder communities in the area of CBRN-related domestic preparedness planning, training, exercises, and equipment research and development. However, the Office will not have veto power over any agency's programs, so its authorities to actually prevent or stop duplicate programs will be limited.

Since our last testimony before this Subcommittee, the National Domestic Preparedness Office has drafted

an action plan. According to the plan, the Office will focus on (1) identifying existing needs assessment tools, (2) cataloging all federal domestic preparedness training, (3) verifying that federal domestic preparedness training initiatives meet the applicable standards, (4) identifying existing training delivery systems and coordinate among federal agencies, (5) coordinating the development of sustainment CBRN training for emergency responders, and (6) facilitating the incorporation of lessons learned into training curriculums.

Office for State and Local Domestic Preparedness Support (OSLDPS)

“The Office of Justice Program's (OJP) Office for State and Local Domestic Preparedness Support (OSLDPS) was created to assist state and local response agencies throughout the United States prepare for incidents of domestic terrorism.”⁸⁵ OSLDPS helps state and local officials in five ways.

State Domestic Preparedness Equipment Program

One is the State Domestic Preparedness Equipment Program to help state and local jurisdictions purchase first responder equipment and fund state planning efforts. In FY 1999, \$51.8 million was available, \$8 million for state planning and \$43.8 million for equipment purchases.⁸⁶ The FY 2001 requested budget is \$78 million. Equipment that can be bought with the grant money is stated on NDPO's Standardized Equipment List.⁸⁷ The FBI also provides first responder training specifically with bombs and WMD at its Hazardous Devices School. The training course teaches bomb identification, neutralization, and disposal. The FY 2001 request for this program is \$4.6 million.

Assistant Attorney General Laurie Robinson describes the program on as followings in the State Domestic Preparedness website:⁸⁸

The threat of terrorist incidents in our Nation presents enormous challenges to the Federal Government and, more significantly, to State and local governments. To address these challenges, the Federal Government is committed to assisting State and local governments better prepare for and respond to terrorist incidents, should they occur. The role of the States in strategic planning—namely, the coordination of resources and responses—and in assessing overall State and local capabilities is a critical component of OJP's State and local domestic preparedness initiative. Indeed, the critical role of local government agencies as the Nation's primary first response groups must be reflected in any domestic preparedness plan the States develop. In recognition of the role local jurisdictions play in any weapons of mass destruction (WMD) response, it is expected that local police, fire, hazardous material, and emergency medical units will receive the majority of funds under this program.

Receipt of funds under the program will be contingent on a State's development of two separate, but related, documents. The first is a State-based Needs Assessment, and the second is a Three-Year Statewide

Domestic Preparedness Strategy. The Needs Assessment will require each State to assess its requirements for equipment, first responder training, and other resources involved in a WMD response. This Needs Assessment will form the basis of the Statewide Strategy. The Strategy will provide a "roadmap" of where each State will target grant funds received under the OJP equipment program and provide OJP a guide on how to target first responder training and other resources available through OJP's Office for State and Local Domestic Preparedness Support. It is also important to understand that the Strategy is a multiyear document and will continue to guide deployment of these resources, by both the States for equipment funds and OJP for other resources, over the next 3 years.

Through this effort, \$51.8 million will be made available to the individual States under the Fiscal Year 1999 State Domestic Preparedness Equipment Program: \$8 million will be distributed to support State planning efforts and \$43.8 million will be available to support equipment purchases. The Attorney General and I believe that the best programs are those that reflect Federal, State, and local coordination and are built on an active partnership with State and local officials. Such partnerships are critical to the successful preparation of our Nation's communities to deal with terrorist threats. Further, such partnerships will strengthen our Nation's capacity to respond to terrorist acts.

Metropolitan Fire and Emergency Medical Services Training Program

The OSLDPS also helps local and state responders through the Metropolitan Fire and Emergency Medical Services Training Program. This is DOJ's primary program to help first responders. DOJ established this program after the Antiterrorism and Effective Death Penalty Act of 1996 authorized the Attorney General, in consultation with FEMA, to provide training for metropolitan fire and emergency service departments to respond to terrorist attacks. The Metropolitan Fire and Emergency Medical Services Training Program is designed to train the local responders who would then train other responders in the community, though DOJ also provides direct training. For FY 1998 and 1999 total, the program received \$10 million and trained 44,000 individuals in 95 cities and metropolitan areas. For FY 2000, the program received \$8 million plus \$2 million to work with DOD to create distance learning material.⁸⁹

A March, 2000, GAO report provides the following program description:⁹⁰

Justice provides WMD training to first responders primarily through its Metropolitan Firefighters and Emergency Medical Services Program but also uses the National Domestic Preparedness Consortium to provide such training. Justice, with assistance from FEMA's National Fire Academy, designed the metropolitan program to prepare first responders for terrorist incidents involving WMD. Justice designed the program to be presented in the largest 120 metropolitan municipalities, which includes cities and counties. In September 1999, Justice increased the number of jurisdictions targeted for the program from 120 to 255. According to Justice officials, the additions were to make the program more responsive to the needs of local responders by providing training to the 120 cities included in Defense's program as well as each state capital and/or the largest city in each state previously excluded from both Justice's and Defense's training programs. Justice either trains-the-trainer or directly trains fire, emergency medical services, and hazardous materials personnel in local communities. Justice received \$5 million in each year of fiscal years 1998 and 1999 to carry out the training segment of its program. For fiscal year 2000, Congress appropriated

\$8 million to Justice for training firefighters, emergency services personnel, and state and local law enforcement personnel. The fiscal year 2000 appropriation also provided \$2 million for Justice to work with Defense in developing distance learning instructional tools such as interactive computer software and video transmission of WMD-related instructional materials.

The training lasts 16 hours and comprises five modules: understanding and recognizing terrorism, implementing self-protective measures, scene security, tactical considerations, and incident command overview. The overall objective of the course is to enable the participants to recognize the circumstances that indicate a potential terrorist act and to take precautionary measures. Through mid-November 1999, 44,000 participants in 95 cities and counties had received the training. This total includes those trained directly by Justice's instructors and the students later trained by the instructors.

The Metropolitan Firefighters program has been an example that critics like the GAO have cited in arguing for better federal integration of terrorism programs. DOD administers the Domestic Preparedness Program and FEMA administers WMD courses at its National Fire Academy and Emergency Management Institute in Maryland. The problem is the potential and actual overlap in first responders' training among the DOJ, DOD, and FEMA programs. Furthermore, critics argue it is inefficient for responders in each city to attend three programs from three departments when an integrated program would save time and resources.⁹¹

OSLDPS Technical Assistance Activities

The third way OSLDPS helps is with the six technical assistance activities that the OSLDPS provides. The activities include risk/threat/vulnerability assessments, consequence management plan reviews, response plan development, grant application assistance, training, and conference design and support.⁹²

- **RISK/THREAT/VULNERABILITY ASSESSMENTS** - The threat of terrorism and mass casualties cannot be denied, nor should it be ignored. Preparation begins with an understanding of vulnerability and the development of a strategy for reducing it. OSLDPS TA can assist local responders and emergency planners in identifying and evaluating those sites that represent the most attractive targets to would-be terrorists, whether government buildings, high use commercial facilities, or infrequently used special event venues. Once identified, potential consequences can be estimated for a range of terrorism scenarios, involving local expertise in calculating the possible outcomes. This data can then be matched against local response capabilities to determine acceptable levels of risk and specific equipment, training, or other capability shortfalls.
- **CONSEQUENCE MANAGEMENT PLAN REVIEWS** - OSLDPS TA can assist Local, City, and State government agencies review their plans for dealing with the consequences of acts of terrorism, offering recommendations to enhance the effectiveness of emergency response to mass casualty events. The reviews are conducted by police, fire, and emergency medicine specialists from across the nation, with specialized training in dealing with the threat posed by chemical, biological, and nuclear/radiological WMD. Reviews are strictly for the purpose of identifying areas of possible improvement intended to enhance overall performance. The review process is professional-helping-professional, and conducted in a low-key,

publicity-averse fashion. Results are provided to local officials on a close-hold basis, mirroring the confidentiality afforded all information provided to TA personnel during the review.

- **RESPONSE PLAN DEVELOPMENT** - OSLDPS TA can assist in the preparation of consequence/emergency management plans, providing agencies in one jurisdiction with the experience gained from cities and states across the nation. Working with local experts from the emergency response communities, TA specialists can provide insight into WMD-driven strategic and tactical planning considerations, interface with other jurisdictions (including the role of Federal assets), incident procedural flows, on-scene and command communications, emergency medical response. TA is not a substitute for local level planning, but an augmenting resource available to provide specialized knowledge and experience to a jurisdiction's existing planning team.
- **GRANT APPLICATION ASSISTANCE** - OSLDPS TA is available to States involved in the preparation of OJP grant applications. Specialists can assist in all stages of the development, writing and review of applications prior to submittal.
- **TRAINING** - OSLDPS offers a broad spectrum of training to responders, ranging from Domestic Preparedness Program (DPP) awareness and "train the trainer" courses to advanced specialist training, including courses offered through the National Domestic Preparedness Consortium. OSLDPS has also prepared "special topics" training for delivery to local jurisdictions, including the Senior Officials Seminar and the Responder Exercise Design Course. OSLDPS TA can also review existing training programs and materials employed at the jurisdiction-level and offer recommendations for enhancements.
- **CONFERENCE DESIGN AND SUPPORT** - OSLDPS TA can develop, conduct and facilitate conferences and meetings addressing terrorism preparedness issues. OSLDPS can assist in securing speakers, providing advice on agenda design, and supporting document preparation. Expert facilitation, whether of large gatherings or small working groups, can result in enhanced meeting effectiveness and focused, goal-oriented outcomes.

State Domestic Preparedness Equipment Program Needs Assessment and Strategy Development Initiative

OSLDPS's fourth method of helping first responders is the State Domestic Preparedness Equipment Program Needs Assessment and Strategy Development Initiative. The Initiative requires all fifty states to assess risks and needs, then use the information to develop strategies to counter WMD terrorism. These assessments are intended to provide a country-wide survey of WMD readiness as well as a basis for developing a Three-Year Strategy for obtaining responder equipment as mandated by the OSLDPS State Domestic Preparedness Equipment Program.⁹³

Assessments are essential means for gathering information, understanding the current state of readiness among states and localities, and for helping guide program direction and development, including decisions for prioritizing and allocating the resources (training, equipment, and exercises) intended to lessen the vulnerability of communities to terrorist use of weapons of mass destruction (WMD). Assessments ensure that measures taken to reduce

vulnerabilities are justifiable and that resources are appropriately targeted to address identified risks and requirements. OSLDPS views assessments as the cornerstone of its state and local domestic preparedness efforts.

Formal assessments have been largely absent from most Federal programs directed at addressing WMD terrorism. OSLDPS is changing that. During Fiscal Year 1999, OSLDPS undertook a major two-phase nation wide needs assessment aimed at providing a macro view of emergency response requirements across the nation. Phase I of this assessment, entitled “Responding to Incidents of Domestic Terrorism: Assessing the Needs of State and Local Jurisdictions” was released in June of 1999. Phase II of the report was released in March of 2000.

While the June 1999 and March 2000 reports viewed the United States at the macro national level, OSLDPS is currently focusing in more detail at the state and local levels. As part of the OSLDPS “Fiscal Year 1999 State Domestic Preparedness Equipment Program,” states will be required to conduct individual needs and risk assessments and, using the information gathered, develop individual state strategies addressing issues of training, equipment, and technical assistance in domestic preparedness support. These assessments, collectively known as OSLDPS State Domestic Preparedness Equipment Program Needs Assessment and Strategy Development Initiative will result in detailed information for each of the fifty states. To assist states in completing this project, OSLDPS is providing both planning grants and technical assistance, including assessment tools and instruments.

These OSLDPS state-based needs assessments are intended to provide a country-wide survey of the current WMD response environment. Working closely with other Federal agencies, including the Centers for Disease Control and Prevention (CDC) and the Federal Bureau of Investigation (FBI), OSLDPS will engage City, County, and State emergency managers, law enforcement officers, and public health officials to help individual jurisdictions pinpoint vulnerabilities and develop plans for countering WMD terrorism. The assessment results will serve not only as a roadmap for program planning, but also as a benchmark for measuring

program

effectiveness.

As part of its responsibilities under the OSLDPS State Domestic Preparedness Equipment Program, each state will use the findings from the assessments as the basis for developing a Three-Year Strategy, which will serve as a roadmap for identifying where each state will target equipment grant funds and guide OSLDPS on how best to target first responder training and other resources. These state assessments will be carried out this spring and summer. To facilitate the process, OSLDPS will be sponsoring a series of Regional Workshops for invited State officials.

The practical problem with these activities is that they depend on valid threat and effects, either of which seem to be available.

TOPOFF Exercises

The fifth way OSLDPS helps is the situational exercises including top officials (TOPOFF) that are to be incorporated into training exercises. These situational exercises received \$3.5 million for FY 1999.⁹⁴

As part of OJP's first responder training/domestic preparedness initiative, the Conference Report (H.Rpt. 105-825, p.999) accompanying the Justice Department's Fiscal Year 1999 Appropriations Act provides \$3.5 million for situational exercises for state and local emergency response personnel.

The Conference language further directs that a portion of these funds be used to comply with language found in the Senate Report (S.Rpt. 105-235) requiring that a "TOPOFF" exercise be included under any exercise initiative. Under the Senate Report, two types of exercises are discussed. The first is a major national level "TOPOFF" exercise. The other is to incorporate situational exercises as part of OJP's efforts to improve the capabilities of state and local emergency personnel response to incidents of domestic terrorism.

Similar language is found in the House Report (H.Rpt. 105-636) which directs the use of "confidence building exercises based on threat driven scenarios" be incorporated into OJP's training efforts.

The National Commission on Terrorism noted that funding for TOPOFF has been inadequate and those exercises have not yet taken place.⁹⁵

National Domestic Preparedness Consortium

The DOJ also administers first responder training through the National Domestic

Preparedness Consortium. The Consortium members consist of Fort McClellan, Alabama, New Mexico Institute of Mining and Technology, Texas A&M University, Nevada Test Site, and Louisiana State University. The WMD specialty training provided at Fort McClellan is chemical explosive agents; at New Mexico Institute of Mining and Technology is bombs and explosive devices; at Texas A&M is emergency medical services, at Nevada Test Site is radiological agents; and at Louisiana State University is law enforcement and biological events. The Conference Committee Report for DOJ's FY 1998 appropriation directed the Attorney General to use the Consortium for the DOJ's WMD training objectives and to provide funding for the Consortium's first responder training in Fort McClellan and in New Mexico Institute of Mining and Technology. The Conference Committee Report for FY 1999 directed DOJ to use the Consortium to the fullest possible extent and appropriated \$24 million for Consortium members. Fort McClellan received \$2 million and \$8 million respectively for FY 1998 and 1999 and will receive \$13 million for FY 2000. The FY 2001 request for Fort McClellan is \$15 million.⁹⁶ The other four Consortium members received total \$2 million and \$12 million for FY 1998 and 1999 and will receive \$14 million for FY 2000. For FY 1999, the Consortium trained about 3,000 individuals.⁹⁷

Awareness of National Security Issues and Response Program (ANSIR)

ANSIR is a program within the National Security Division of the FBI that serves to disseminate unclassified security and threat information to corporate security directors, law enforcement, and other government agencies.⁹⁸

The Awareness of National Security Issues and Response (ANSIR) Program is the FBI's National Security Awareness Program. It is the "public voice" of the FBI for espionage, counterintelligence, counterterrorism, economic espionage, cyber and physical infrastructure protection and all national security issues. The program is designed to provide unclassified national security threat and warning information to U.S. corporate security directors and executives, law enforcement, and other government agencies. It also focuses on the "response" capability unique to the FBI's jurisdiction in both law enforcement and counterintelligence investigations.

Information is disseminated nationwide via the ANSIR-Email and ANSIR-FAX networks. Each of the FBI's 56 field offices has an ANSIR coordinator and is equipped to provide national security threat and awareness information on a regular basis to corporate recipients within their jurisdiction. ANSIR-FAX was the first initiative by the U.S. government to provide this type of information to as many as 25,000 individual U.S. corporations with critical technologies or sensitive economic information targeted by foreign intelligence services or their agents. ANSIR-Email increases the capacity for the number of recipients to exceed 100,000 which should accommodate every U.S. corporation who wishes to receive

information from the FBI. Interested U.S. corporations should provide their email address, position, company name and address as well as telephone and fax numbers to the national ANSIR Email address at ansir@leo.gov. Individual ANSIR Coordinators in the respective field divisions will verify contact with each prospective recipient of ANSIR Email advisories.

The FBI is the lead agency for a variety of national security concerns. With regard to foreign counterintelligence activity, theft of U.S. technology and sensitive economic information by foreign intelligence services and competitors has been estimated by the White House and others to be valued up to a hundred billion dollars annually. It is therefore prudent and necessary that we provide information to those who are the targets of this activity. Critical infrastructure protection, both cyber and physical, is also a major focus of the FBI and the ANSIR program helps to identify these infrastructures and ensure that communication with the FBI is established.

Each ANSIR coordinator in the FBI's 56 field offices is a member of the American Society for Industrial Security. This membership enhances public/private sector communication and cooperation for the mutual benefit of both. FBI ANSIR Coordinators meet regularly with industry leaders and security directors for updates on current national security issues.

The ANSIR program focuses on the "techniques of espionage" when relating national security awareness information to industry. Discussing techniques allows us to be very specific in giving industry representatives tangible information to help them decide their own vulnerabilities. These techniques include compromise of industry information through "dumpster diving" where Foreign Intelligence Services and competitors may try to obtain corporate proprietary information, or listening devices which may be as simple as using a police scanner to tune in the frequency of the wireless microphone being used in the corporate boardroom. Through the ANSIR program and the discussion of techniques of espionage corporations are able to learn from the experiences of others enabling them to avoid adverse results.

Along with awareness, the ANSIR program provides information about the FBI's unique "response" capability with regard to issues of national security. The FBI has primary jurisdiction for a variety of criminal and counterintelligence investigations which impact on national security. For instance, the recent passage of the Economic Espionage Act of 1996 opened up new areas of FBI response to the wrongful acquisition of intellectual property. It also encourages corporations to consider how best to protect their proprietary information or trade secrets from both domestic and foreign theft.

The FBI ANSIR Coordinator in the local field office is the point of contact for information about the FBI's national security programs and also to receive initial information which may result in a response by the FBI. U.S. corporations should also contact the local ANSIR Coordinator to receive ANSIR-Email or ANSIR-FAX information.

National Institute of Justice

The National Institute of Justice (NIJ) is the lead agency in developing a standard for first responder equipment. NIJ is working with the Technical Support Working group to develop wearable toxic agents detectors and easy access protective masks.⁹⁹

Total Department of Justice and FBI Funding

Table Twenty-Five shows total DOJ counterterrorism spending. It is adapted from the

2000 OMB counterterrorism funding report. It shows a steady increase in appropriations. Overall spending has increased over 45% from FY 1998 to \$949.25 million for FY 2001 requested.¹⁰⁰

Table Twenty-Five

Department of Justice Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	647.09	793.99	782.02	949.25
Law Enforcement and Investigative Activities	346.90	328.91	346.24	409.53
Physical Security of Government Facilities and Employees	84.29	105.08	117.12	171.22
Physical Security of National Populace	29.00	41.76	31.67	30.79
Preparing for and Responding to Terrorist Acts	159.90	301.37	250.12	307.26
Research and Development	27.00	16.87	36.88	30.45
<i>WMD Preparedness</i>	100.80	201.22	217.18	254.66
Law Enforcement and Investigative Activities	43.00	39.74	39.74	43.24
Physical Security of National Populace	1.00	1.44	1.22	1.23
Preparing for and Responding to WMD Terrorism	41.80	147.35	143.54	189.25
Equipment for First Responders	12.00	95.00	85.00	88.00
First Responder Training and Exercises	10.00	26.47	38.45	73.45
Other	1.80	2.00	2.20	2.80
Other Planning and Assistance to State/Locals	18.00	23.88	17.89	25.00
Research and Development	15.00	12.69	32.69	20.94
Detection/Diagnostics	3.00	2.69	2.69	3.94
Personal/Collective Protection	12.00	10.00	30.00	17.00
*OMB Highlighted Programs				
Equipment Grants for First Responders	-	-	-	78.00
Domestic Preparedness Training	-	-	-	31.00
Hazardous Devices School	-	-	-	4.60
Center for Domestic Preparedness at Fort McClellan	-	-	-	15.00
Technology and Standards Development	-	-	-	17.00

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

National Security Community

Presidential Decision Directive 39 designated the National Coordinator for Security, Infrastructure Protection, and Counterterrorism at the National Security Council the lead agency responsible for coordination of policies and programs dealing with foreign CBRN terrorism.¹⁰¹ The National Security Community is requesting \$340 million for FY 2001 for

research and development to combat the CBRN threat. The research is designed for military needs but can yield technologies useful for domestic preparedness.¹⁰² Table Twenty-Six summarizes National Security Community counterterrorism spending. It is adapted from an OMB counterterrorism funding report.¹⁰³

Table Twenty-Six

National Security Community, including the Department of Defense, Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	4,496.12	4,682.51	5,117.17	5,124.06
Law Enforcement and Investigative Activities	2,042.33	2,067.79	2,213.24	2,213.52
Physical Security of Government Facilities and Employees	2,075.47	2,036.47	2,122.75	2,173.85
Physical Security of National Populace	0.15	0.04	0.15	0.15
Preparing for and Responding to Terrorist Acts	104.20	256.18	358.58	233.84
Research and Development	270.98	322.03	422.45	502.71
<i>WMD Preparedness</i>	180.56	408.15	475.82	467.21
Law Enforcement and Investigative Activities	7.10	20.96	20.41	19.47
Preparing for and Responding to WMD Terrorism	2.71	156.39	161.50	100.74
First Responder Training and Exercises	0.05	49.90	32.10	10.20
Other Planning and Assistance to State/Locals	0.00	15.60	8.50	10.30
Special Response Units	2.66	90.89	120.90	80.24
Research and Development	170.75	230.80	293.90	347.00
Basic Research, incl. Gene Sequencing	44.50	0.00	6.25	37.50
Detection/Diagnostics	0.25	34.10	48.45	62.30
Modeling, Simulation, Systems Analyses	0.00	8.60	10.00	10.00
Other	126.00	140.00	161.50	141.00
Personal/Collective Protection	0.00	0.00	0.00	10.00
Personal/Environmental Decontamination	0.00	6.50	17.10	21.00
Therapeutics/Treatments	0.00	12.00	16.50	22.20
Vaccines	0.00	29.60	34.10	43.00

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Nuclear Regulatory Commission

The following chart on Nuclear Regulatory Commission counterterrorism spending adapted from the 2000 OMB counterterrorism funding report shows most of the money is going towards WMD preparedness, and specifically towards protecting the populace from attacks using nuclear and radiological materials, or which strike at nuclear facilities:¹⁰⁴

Table Twenty-SevenNuclear Regulatory Commission Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	3.48	3.21	3.21	3.24
Law Enforcement and Investigative Activities	0.65	0.40	0.40	0.40
Physical Security of Government Facilities and Employees	0.42	0.40	0.40	0.40
Physical Security of National Populace	2.39	2.39	2.39	2.39
Preparing for and Responding to Terrorist Acts	0.02	0.02	0.02	0.05
<i>WMD Preparedness</i>	3.04	2.79	2.79	2.79
Law Enforcement and Investigative Activities	0.65	0.40	0.40	0.40
Physical Security of National Populace	2.39	2.39	2.39	2.39

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Smithsonian

Table Twenty-Eight shows Smithsonian counterterrorism spending. It is adapted from the 2000 OMB counterterrorism funding report and shows that the \$50,000 is being requested for FY 2001 for the physical security of the Smithsonian.¹⁰⁵

Table Twenty-EightSmithsonian Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	0.00	0.00	0.00	0.05
Physical Security of Government Facilities and Employees	0.00	0.00	0.00	0.05

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Department of State

The State Department is the lead agency for international terrorism. For example, it manages the Terrorist Interdiction Program. The program helps selected vulnerable countries to

stop terrorists from entering or using their territory. The FY 2001 request is \$4 million.¹⁰⁶

Embassy Protection

The bulk of State funds, however, go to the physical protection of facilities abroad and have little to do with homeland defense. The President's FY 2001 budget requests \$1.2 billion¹⁰⁷ and \$3.4 billion in advance appropriations for FY 2002 through FY 2005. For FY 2001, \$500 million will go towards new overseas facilities, \$200 million above FY 2000 enacted \$300 million. \$200 million will go towards new protective measures for embassies such as alarms and perimeter barriers, an increase of \$200 million from FY 2000 enacted. \$342 million will go towards high security readiness, \$74 million above FY 2000 enacted \$268 million. \$68 million will go towards the State Department's Anti-Terrorism Assistance (ATA) Program, an increase of \$35 million from FY 2000 enacted \$33 million. The ATA funding level provides \$30 million to establish a center for anti-terrorism and security training to meet worldwide demand for ATA programs.

The White House Press Secretary released the following statement:¹⁰⁸

The President's FY 2001 budget includes more than \$1.1 billion to reduce further the risk of loss of life from terrorist attacks on our overseas diplomatic missions. This represents an increase of over \$500 million in additional Federal funds to address enhanced security needs of diplomatic and consular facilities overseas. The request also includes \$3.4 billion in advance appropriations for fiscal years 2002 through 2005 to provide a solid foundation for long-term building needs.

New Construction

--Invest \$500 million in new overseas facilities in FY 2001, an increase of \$200 million above the FY 2000 enacted level.

--Consolidate the requirements of all foreign affairs agencies in new embassy construction. --Establish a solid foundation for future years with \$3.4 billion advance appropriation.

Increase Protective Measures

--Invest \$200 million to begin a new series of increased protective measures such as perimeter barriers, alarms, and access control equipment for overseas facilities to meet applicable diplomatic security standards and address emergent needs as they are identified, an increase of \$200 million over FY 2000 enacted.

Sustain and Improve Security Readiness

--Maintain a high level of security readiness at a cost of \$342 million in FY 2001, an increase of \$74

million above FY 2000 enacted. This cost includes both the recurring costs of additional security measures such as guards for overseas facilities and the operation and maintenance costs of security improvements already in place.

--Augment security personnel corps with an additional \$16 million for 161 security professionals to create a surge capacity to respond quickly to evolving terrorist threats.

--Increase support for the Anti-Terrorism Assistance Program to \$68 million, an increase of \$35 million above the FY 2000 enacted level, to provide a robust training component. This funding level includes \$30 million to establish a center for anti-terrorism and security training to meet growing worldwide demand for ATA programs.

Coordinator for Counterterrorism

The Coordinator of Counterterrorism is the focus of counterterrorism efforts at the Department of State. It leads interagency teams (FBI, DOJ, CIA, DOD, FAA, etc.) in consultations and cooperation with foreign countries and works with intelligence community to identify state sponsors of terrorism. It also leads FEST teams and oversees the Technical Support Working Group (TSWG).

Foreign Emergency Support Teams (FEST)

The Foreign Emergency Support Teams (FEST) are emergency response teams led by an officer from the Office for Counterterrorism and staffed by representatives of DOD, CIA, FBI, and other agencies. A team may be dispatched within hours via a specially dedicated airplane (supplied by DOD) and is intended to be a small and flexible team of experts to assist an Ambassador and host government in resolving a terrorist crisis.

Technical Support Working Group

The Technical Support Working Group is an n interagency team funded mostly by DOD. It conducts counterterrorism technology R&D and prototyping, focusing on explosives detection and technologies that will detect and protect against WMD terrorism, and .coordinates and manages the National Counterterrorism Research and Development Program. The TSWG is made up of representatives from 8 federal departments and over 50 agencies. It also has cooperative programs with Canada, the United Kingdom, and Israel to develop counterterrorism technologies.

Bureau of Consular Affairs

The Bureau of Consular Affairs works with the S/CT, INR/TNC, DS, the intelligence community, and consulates abroad to maintain systems to deny suspected terrorists entry to the United States. It also issues warnings and travel advisories pertaining to terrorist threats.

Bureau of Diplomatic Security

The Bureau of Diplomatic Security protects U.S. personnel and facilities abroad from terrorists. It investigates passport and visa fraud which may accompany terrorist acts, and operates the Overseas Security Advisory Council which maintains a security and terrorism related electronic bulletin board for non-official U.S. citizens overseas. It also administers the Anti-Terrorism Assistance Program which has trained over 17,000 officials from 89 countries in counterterrorism. The program costs approximately \$16,000,000 annually.

Anti-Terrorism Assistance (ATA) Program

The State Department administers the Anti-Terrorism Assistance (ATA) Program through the Bureau of Diplomatic Security. This program is directed at foreign countries, but has an indirect impact in reducing the terrorist threat to the US.

ATA received \$33 million in FY 2000, and, according to the White House Press Secretary, the President is requesting \$68 million for FY 2001, including \$30 million to establish a center for anti-terrorism and security training to meet the worldwide demand for ATA programs.¹⁰⁹ The OMB reports the FY 2001 request for ATA is \$64 million. As of August 4, 1999, 20,000 representatives from more than 100 countries have been trained. A State Department Fact Sheet describes the program as follows:¹¹⁰

The United States is engaged in a vigorous campaign to promote by the year 2000 the universal adoption and ratification of all eleven existing international terrorist conventions. Every nation has the responsibility to arrest or expel terrorists, shut down their finances, and deny them safe haven. Our goal is to strengthen the rule of law against terrorism globally.

In June the Department hosted an important counterterrorism conference that included representatives from 22 nations in the Middle East, South Asia, Central Asia, Europe, and Canada. The conference promoted international cooperation against terrorism and the sharing of information on terrorist groups and countermeasures.

The United States conducts the successful Anti-terrorism Training Assistance program, which trains foreign law enforcement personnel in such areas as airport security, bomb detection, maritime security, VIP protection, hostage rescue, and crisis management. To date, we have trained more than 20,000 representatives from more than 100 countries.

Total State Department Funding

The following chart on State Department counterterrorism spending adapted from the 2000 OMB counterterrorism funding report shows a huge increase in appropriations, mostly to go for embassies.¹¹¹ The WMD preparedness spending has increased over 210% from FY 1998 to \$72 million for the FY 2001 request.

Table Twenty-Nine

Department of State Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	186.00	1579.00	791.00	1312.00
Law Enforcement and Investigative Activities	27.00	53.00	46.00	80.00
Physical Security of Government Facilities and Employees	151.00	1512.00	727.00	1224.00
Preparing for and Responding to Terrorist Acts	6.00	6.00	6.00	6.00
Research and Development	2.00	8.00	2.00	2.00
<i>WMD Preparedness</i>	23.00	46.00	37.00	72.00
Law Enforcement and Investigative Activities	19.00	41.00	33.00	68.00
Preparing for and Responding to WMD Terrorism	4.00	4.00	4.00	4.00
Special Response Units	4.00	4.00	4.00	4.00
Research and Development	0.00	1.00	0.00	0.00
Other	0.00	1.00	0.00	0.00
*OMB Highlighted Programs				
Embassy Security	-	-	-	1200.00
Anti-Terrorism Assistance Program	-	-	-	64.00
Terrorism Interdiction Program	-	-	-	4.00

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Department of Transportation

DOT's programs cannot be clearly separated into WMD and Critical Infrastructure Protection components. One program that has WMD aspects is Transportation Infrastructure Assurance Research and Development, managed by the Research and Special Programs Administration. The program researches CB detection systems for major terminals such as

subways, airports, and rail stations. The program also researches Intermodal Terminal Security and the intermodal freight transportation network. The FY 2001 request is \$3 million. Another DOT program is the Human Factors Analysis for Transportation Systems. The project analyzes the limitations of human preparedness, prediction, and response related to modes of transportation. The project's FY 2001 request is \$0.4 million.¹¹²

The DOT is continuing to acquire explosives detection technologies to improve screening accuracy, requesting \$100 million for FY 2001. The DOT also wants further research and development into security to meet the growing and changing threat of terrorism. The FY 2001 request for the program is \$49.4 million. Security will also be improved at vital FAA facilities. \$18.6 million is the FY 2001 request.¹¹³

In cases of air piracy, the FAA is responsible for coordination of all law enforcement activity. In FY97, total spending for unclassified terrorism-related programs totaled approximately \$296,800,000.

Table Thirty shows total DOT counterterrorism spending. It is adapted from the 2000 OMB counterterrorism funding report, which shows that most of the funding is going to protect transportation systems from conventional attacks and not towards WMD preparedness.¹¹⁴

Table Thirty

Department of Transportation Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	169.30	270.78	277.21	298.15
Law Enforcement and Investigative Activities	3.90	4.21	4.48	4.68
Physical Security of Government Facilities and Employees	17.86	18.16	19.54	20.94
Physical Security of National Populace	99.78	193.58	199.08	216.50
Preparing for and Responding to Terrorist Acts	3.16	3.04	3.52	6.03
Research and Development	44.60	51.79	50.60	49.65
<i>WMD Preparedness</i>	0.00	0.00	0.45	2.50
Preparing for and Responding to WMD Terrorism	0.00	0.00	0.00	2.50
Equipment for First Responders	0.00	0.00	0.00	2.50
Research and Development	0.00	0.00	0.45	0.00
Detection/Diagnostics	0.00	0.00	0.45	0.00

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Department of Treasury

The Treasury has responsibility for a number of counterterrorism function. The United States Secret Service is developing chemical and biological detection, mitigation, and decontamination support for all Presidential movements. The Service is constructing a chemical and biological detection and protective program that combines multiple systems: fixed detectors, collective protection systems, and portable detection equipment.

The Bureau of Alcohol, Tobacco, and Firearms (ATF) is the lead federal agency in investigating armed violent crime, arson, and explosions. ATF has four National Response Teams that can arrive within 24 hours to major bombing and arson sites. The bureau is also researching the effects of large car bombs along with the US Army Corps of Engineers and the Defense Technical Research Agency.

The Customs Service is responsible for stopping CBRN materials from entering the country. The U.S. Secret Service is responsible for security at major events. The two services work together to prevent an airborne attack at major events. Customs Air and Marine Interdiction Division will supply the air support to enforce temporary flight restricted areas, to survey the area, and to transport Secret Service assault teams and snipers. The FY 2001 request for this joint program is \$16 million. The funds will allow 19 special agents to be trained and equipped for the air security counter-assault team.

The following chart on Treasury counterterrorism spending is adapted from the 2000 OMB counterterrorism funding report. It shows a nearly an \$100 million increase for the FY 2001 request.¹¹⁵

Table Thirty-One

Department of Treasury Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	341.36	368.01	348.00	440.21
Law Enforcement and Investigative Activities	213.13	212.13	189.53	285.73
Physical Security of Government Facilities and Employees	64.30	67.51	68.46	63.46

Physical Security of National Populace	15.34	19.06	16.58	16.58
Preparing for and Responding to Terrorist Acts	47.89	68.52	70.70	71.70
Research and Development	0.70	0.79	2.73	2.74
WMD Preparedness	18.01	19.46	25.87	25.87
Physical Security of Government Facilities and Employees	5.14	5.14	8.84	8.84
Preparing for and Responding to WMD Terrorism	12.88	14.32	17.03	17.03
Equipment for First Responders	0.99	2.02	2.23	2.23
Other	0.35	0.73	0.20	0.20
Special Response Units	11.53	11.57	14.60	14.60
*OMB Highlighted Programs				
Air Security Protective Operations	-	-	-	16.00

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

US AID (Now State Department)

Table Thirty-Two shows counterterrorism spending by US AID. It is adapted from the 2000 OMB counterterrorism funding report shows over \$50 million went towards preparing for and responding to terrorist acts in FY 1998.¹¹⁶ Virtually all AID spending affects foreign countries, however, and not homeland defense.

Table Thirty-Two

US AID Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	5.68	54.89	5.83	5.01
Physical Security of Government Facilities and Employees	2.68	3.49	3.98	2.66
Preparing for and Responding to Terrorist Acts	3.00	51.40	1.40	2.35
WMD Preparedness	3.00	1.40	1.40	2.35

Preparing for and Responding to WMD Terrorism	3.00	1.40	1.40	2.35
First Responder Training and Exercises	0.30	1.40	1.40	2.35
Other	2.70	0.00	0.00	0.00

Department of Veterans Affairs

Presidential Decision Directive-62 instructs the VA to assist the U.S. Public Health Service (USPHS) in maintaining an adequate national stockpile of pharmaceuticals. Four caches are maintained in strategic locations that would be dispatched to a scene of a WMD attack to help the capability USPHS National Medical Response Teams.

The VA also assists the CDC in maintaining the National Pharmaceutical Stockpile, which is located in certain cities in the US. VA receives funds from the agencies they support to maintain the stockpiles. The VA also trains medical personnel at National Disaster Medical System hospitals. VA is working on constructing a counterterrorism training program to include with its training. USPHS can transfer up to \$1 million a year to VA for the training.

The following chart on VA counterterrorism spending adapted from the 2000 OMB counterterrorism funding report reflects the fact that VA supports its counterterrorism program from funding transferred by other agencies.¹¹⁷ It should be noted that some expert have proposed significantly expanding the VA's contingency role in responding to biological attacks, both in using its medical facilities for response purposes and in playing a role in vaccine distribution and immunization.

Table Thirty-Four

Department of Veterans Affairs Spending for Combating Terrorism and WMD Preparedness

	<u>FY1998</u>	<u>FY1999</u>	<u>FY2000</u>	<u>FY2001</u>
<i>Combat Terrorism</i>	0.01	0.04	0.00	0.00
Preparing for and Responding to Terrorist Acts	0.01	0.00	0.00	0.00

*OMB Highlighted Programs

Stockpiling Pharmaceuticals		-	-	-	N/A
Training Medical Personnel		-	-	-	N/A

Source: Adapted by Steve Chu and Preston Golson from Executive Office of the President, Office Management and Budget, "Annual Report to Congress on Combating Terrorism," May 2000

*denotes programs highlighted in OMB report. Figures part of 2001 budget

Federal and State/Local Cooperation

The federal government has set forth a detailed policy for state and local cooperation, and it is clear from the preceding description of agency activity that extensive work is underway to improve coordination with state and local law enforcement agencies, emergency planning groups, and a wide range of different responders. A number of regional centers have been set up and federal agencies and state and local governments have been involved in a range of exercises. There has also been an increasing effort to involve the private and civil sector, particularly in areas like health care, the media, and utilities.

Limits to Cooperation

There are, however, no clear measures of the scope and effectiveness of these efforts to date, and state and local authorities and private sector capabilities differ sharply even within major metropolitan areas. In many cases, the coordination effort also has not gone beyond command post exercise-like activities whose main purpose has been to educate state and local actors in the generic risk of attacks.

These exercises and activities now seem to be most effective in dealing with relatively low levels of attack, with effects limited to those that states and localities often deal with in emergencies caused by weather, accidents, low level terrorism, or natural outbreaks of disease. Planning for large-scale high explosive attacks and most chemical attacks – which may be similar in effect to major Hazmat accidents – may be covered by such procedures, although there seems to be only a limited effort to determine critical vulnerabilities and consider the broader impact of such attacks when they strike at utilities, key medical facilities, etc.

The unclassified data available do not indicate that critical node analysis has been carried

out in most areas. The federal efforts seems to be a “feed forward” system that assumes that state and local needs are relatively predictable, and that many capabilities will exist in all states and localities. While an effort is underway to inventory current equipment and capabilities, it is not clear that this will always reveal the weakest or “critical” links limiting state and local capabilities, or that either the federal government or states will be able to deal with the complex problems created by the very different capabilities of given localities and jurisdictions. This problem is further complicated by interstate jurisdiction problems in the many target areas that involve more than one state, and by the inability to predict the nature and scale of the attack(s), and promptly characterize the nature and scale of attacks and their effects once they occur.

There are still significant legal and jurisdictional problems in federal-state-local cooperation in gathering intelligence – the most critical aspect of defense, and in law enforcement and defense. Grand jury and other laws limit full communication upwards from the local level, while there are severe limits on what intelligence and law enforcement agencies can do if there is even a risk that a US citizen might be involved in surveillance and an investigation.

There is, as yet, little practical planning, organization, and training for major CBRN attacks of the kind that may occur in the future. Nuclear attacks have only been explored to a limited extent, and there is little detailed planning for response to the level of direct effects that can occur or to the long term and secondary effects which may require a response over weeks, months, and years. Even the more sophisticated attack models and exercises being used assume that radioactive plumes and fall out are relatively predictable and that enough knowledge exists to predict the radiation thresholds that produce serious casualties that require prompt treatment and the areas that will be affected.

West Nile Outbreak

The 1999 West Nile virus outbreak in New York City presents an example of the problems involved. It caused encephalitis in 62 people and killed seven people. The outbreak was viewed by many as a test of bioterrorism preparedness. Several aspects of the investigation went well, as GAO stated in its preliminary correspondence on the outbreak:¹¹⁸

Information collected to date indicates that many officials and experts believe aspects of the outbreak investigation went very quickly and very well. These include the physician's reporting of the initial unusual symptoms and the role the local health department epidemiologists played in quickly mobilizing a broad-based outbreak investigation. Further, particular aspects of the communications between involved parties were considered useful for disseminating information. For example, throughout much of the crisis, daily conference calls on the status of events were conducted involving officials from as many as 18 different local, state, federal and other agencies. Finally, experts also point out that while the virus was initially incorrectly diagnosed as another related virus, the misdiagnosis did not affect the appropriate treatments for patients or the public health response.

However, the outbreak also revealed many problems in bioterrorism preparedness. The GAO reported that,¹¹⁹

Most parties interviewed to date also believe there are lessons to be learned from the events, particularly related to communication and infrastructure issues, that may be relevant in designing future preparedness measures. Even though this was a relatively small outbreak, it consumed the time of dozens if not hundreds of officials from local, state, and federal public health and other agencies and organizations, and greatly strained available resources. Many involved officials believe that the outbreak was another "wake-up call" that public health officials must anticipate and be better prepared to respond to such surprises. Officials also believe that the outbreak illustrates the need for a better public health infrastructure at the local, state, and national level to control infectious diseases, particularly those that are vector-borne. Work to date indicates that any problems identified are likely to revolve around such things as the following:

Communication between and among local, state, and federal agencies. Rapid and reliable communication between public health agencies is considered essential to preparedness and coordination--as the ability to disseminate and share information rapidly among public health officials helps ensure that decisions are made with the most current information available. Officials involved in the West Nile events indicated that the communications that occurred (for example, the daily conference calls and phone conversations between agency and organization officials) helped update involved parties as the investigation unfolded. However, some key officials indicated to us that they believed this means of sharing information was time-consuming and inefficient and that alternatives for communicating detailed information were needed so they could use their expertise and skills to conduct the investigation. Some people also indicated that there was much confusion during the course of events about "who to call" for various types of information or to handle various responsibilities or who within each agency could be considered a responsible spokesperson and information source.

Communication between public health agencies and other organization with relevant information, such as animal health experts. Livestock animals and wildlife are often considered sentinels, providing an early warning device for diseases that could harm people. Assessments of the West Nile events and many officials we interviewed said that the events highlighted the need for better integration and communication between animal/wildlife health communities and public health. Since the initial outbreak, CDC, state wildlife veterinarians, and an expanding group of federal and other agencies are using deaths in crows as sentinel events to define the current geographic distribution of mosquitoes and birds infected with West Nile virus.

The adequacy of epidemiological capacity and local level disease surveillance systems. The outbreak was initially identified because an astute physician reported two unusual cases of illness to the City Health Department, and active surveillance in New York City confirmed 62 human cases of the disease. Physicians are required to report encephalitis cases to the Health Department; however, the West Nile investigation confirmed that such reporting often did not occur. During the West Nile investigation, the six New York City Health Department staff who normally track over 50 reportable infectious diseases in the city--along with several others detailed to assist from other divisions and agencies--worked long hours

seven days a week to contact relevant officials at 70 hospitals to identify potential cases, interview patients and families, track cases, and ensure laboratory samples were shipped to appropriate parties, among other duties. Officials indicated that the availability of even the small number of trained staff in New York City was critical to the quick response to the initial outbreak. Such capacity at the local level is thought to be lacking in many other locations.

The adequacy of laboratory capacity—especially “surge capacity” to allow a quick response to an unexpected crisis. A frequent theme of discussions and assessments has been the adequacy of laboratory infrastructure at the state and federal levels for performing timely and thorough laboratory analyses. Officials pointed out that there are only two federal laboratories capable of handling those infectious agents considered of most concern. Further, most laboratories, including veterinary laboratories, are not equipped to identify diseases that are rarely seen. Inadequate “surge capacity,” the ability to deal with a sudden increase in needed testing, was another cited concern. According to officials we spoke with, laboratory capacity for performing the tests needed to identify the West Nile virus and to diagnose which people had the virus was consumed quickly by this relatively small outbreak.

Potential problems in distinguishing between a naturally occurring outbreak and one that is intentionally caused. While the West Nile virus outbreak is thought to have been a naturally-occurring event and officials interviewed indicated that the investigation did not find otherwise, at one point there was speculation in media reports that the outbreak might have had an unnatural (bioterrorist) origin. Because of this, experts indicate that this episode does illustrate the potential problems in distinguishing natural disease from an intentional attack. The source of the disease (whether natural or intentional) would not change the process to diagnose and treat patients. However, if local health officials are informed of a bioterrorist incident or threat, or if a health department or CDC investigation determines that an event is likely a bioterrorist one, then additional organizations would need to become involved to carry out a criminal investigation. Current recommended protocols are to notify the Federal Bureau of Investigation and law enforcement officials, who would also seek to determine whether terrorists had targeted additional locations for release of the disease.

It should be noted that GAO did not address the issue of the ability to characterize and treat a biological weapon as distinguished from a normal pattern of disease, or the lessons learned from this experience if the attack occurred as the result of a large-scale attack by a state actor, proxy, or well organized and efficient terrorist/extremists.

The Lessons from “Jointness”

The US has learned over the years how to react to many kinds of emergencies, some at relatively large-scale by civil standards. In general, however, the burden of response falls first on local authorities and the local private sector, then on states, and then on the federal government. Existing capabilities are generally adequate or response can be improvised as needed. The same is true of law enforcement, although foreign and national counterterrorist and counterextremist activity has a higher element of federal involvement in both intelligence and enforcement. The resulting capabilities to deal with low-level threats to the US homeland are generally good for

low level threats and attacks, and the effects of failure are highly localized. They will be tragic but not catastrophic.

The situation changes radically as the level of attack escalates and changes in type. It can be argued that most practical chemical and radiological attacks will strain the existing structure of local-state-federal response, but will not be radically different in impact from a major chemical spill or Hazmat incident if the public reaction can be contained, and authorities make the limits of the attack clear. At the same time, even at this level of attack, a large number of private, state, local, and federal entities may be involved in unfamiliar activities where both past experience and currently plans are not adequate to the task.

The problem grows steadily more severe as the threat escalates and both steadily more unfamiliar and unpredictable. Nuclear and biological attacks can reach levels where the priority of detection and prevention forces new and drastic approaches to intelligence and law enforcement, and where any effort to plan response becomes an exercise in managing chaos. Local capabilities of all kind can be saturated and collapse. States will confront problems that they cannot anticipate, and the federal government may find that the first casualty in homeland defense, like war, is not truth but rather the plan of battle.

There is no way to validate such a conclusion with hard data, and the results are impressionistic, but neither the literature available nor practical experience in attending meetings and simulations indicates that federal, state, and local governments as yet fully understand the extent to which they will have to deal with unpredictable events they cannot properly characterize at any point in their defense and response activities, and with the failure of their plans and organizational efforts. There is a "Task Force Smith" character to many such efforts. Capability is assumed either to exist or to be developed in the future. The ability to meet and discuss is confused with the ability to react. Federal, state, and local governments talk at each other, rather than fully communicate. Critical details are ignored, and real world limits in capability are never discovered.

It is interesting consider the experience of the American military in this light. No amount

of planning, coordination, organization, and designation of command authority ever created effective joint operations. Jointness was forced on the military by experience and by defeat. Every important lesson was learned the hard way. As a result, the need for true jointness became both practical doctrine and practical years after all of the problems involved had supposedly been solved.

In the process, the US military had to radically change its training and exercise doctrine. It learned that effective coordination can be helped with truly demanding command post exercises, but only if the participants are stressed to the point of defeat and are forced to be realistic. Exercises designed to produce success have been proven to be a failure ever since the breakdown in US command at Kasserine Pass. Furthermore, the US military learned that tactical execution required truly demanding field exercises, and that every aspect of jointness that was not simulated and testing in the field failed. And, the Gulf War, Somalia, and Kosovo still revealed that major problems still existed in jointness and coordination.

The problems in achieving effective “jointness” in homeland defense against CBRN attacks are likely to be far more daunting, particularly because it is far from clear what attacks should be exercises, that realistic exercises are affordable, and that much of the experience from one exercise will apply to a different type of attack in a different area.

This is not a reason to give up on trying to deal with high levels of attack. It is, however, a reasons not to confuse meetings, discussions cloaked as exercises, inventories, and creating new lines of authority as effective action. It is a good reason for the federal government to carry out as many realistic exercises as possible, and above all to firmly establish the limits of what it can do in mid to high level attacks, and the operational limits of “jointness” at the state and local level. It is good reason to question whether creating a new czar, lead agency, or cabinet member will accomplish any more in practice than the somewhat similar debate over how to conduct the war on drugs. It is also good reason to assume that the capability to improvise will be more important than preexisting plans. Above all, it is good reason at every level of government not to confuse assigning responsibility with creating capability.

How Other Nations Deal With These Threats

Given the theater-driven nature of most threats, it is surprising that the US is often ahead of its friends and allies in dealing with the threats posed by state actors, their proxies, and foreign and domestic terrorists/extremists. Indeed, many Europeans see the US as over-reacting to marginal threats in an almost paranoid fashion. This is partly a result of the fact that the US does often over-dramatize given threats and the need for given actions, but it also may reflect the fact that Europe both does not face the same scale of regional threats as the US and already faces major problems in funding its existing security requirements.

The situation is different in the case of America's friends and allies in the Middle East, the Gulf, and Asia – although most of our friends and allies are just beginning to understand just how different the threats they face can be if covert, state, terrorist, or extremist attacks use weapons of mass destruction. Even Israel and South Korea have done comparatively little to improve their deterrence and defense capabilities against such attacks, or to improve their response capabilities beyond very limited, and largely symbolic, civil defense measures.

Many aspects of what our friends and allies have done are classified, or are not made public. The General Accounting Office did, however, publish a survey of the activities in five key friendly countries in May 2000: in Canada, France, Germany, Israel, and the United Kingdom. The GAO found striking similarities in their response:¹²⁰

The five countries we examined have similarities in how they are organized to combat terrorism.

- The countries generally have the majority of organizations used to combat terrorism under one lead government ministry. However, because many other ministries are also involved, the countries have created interagency coordination bodies to coordinate both within and across ministries. For example, while many countries generally have their intelligence and law enforcement organizations under their ministries of interior or equivalent, they also need to coordinate with their ministries of foreign affairs, defense, and health or emergency services.
- The countries have clearly designated who is in charge during a terrorist incident—typically their national or local police.
- The countries have national policies that emphasize prevention of terrorism. To achieve their policies, the countries use a variety of strategies, including intelligence collection, police presence, and various security measures such as physical barriers at the entrances to public buildings.

- These countries primarily use their general criminal laws (e.g., those for murder or arson) to prosecute terrorists. The countries also have special terrorism-related laws that allow for special investigations or prosecution mechanisms and increased penalties.
- The countries' executive branches provide the primary oversight of organizations involved in combating terrorism. This oversight involves reviewing the programs and resources for effectiveness, efficiency, and legality.

The five countries we examined also had similarities in how they allocate resources to combat terrorism. Officials in the ministries involved said they make resource allocations based upon the likelihood of threats taking place, as determined by intelligence assessments. While the officials we met with discussed resource levels in general, none of the five countries tracked overall spending on programs to combat terrorism.

Such spending was imbedded in other accounts for broad organizational or functional areas such as law enforcement, intelligence, and defense. Officials in all countries told us that because of limited resources, they made funding decisions for programs to combat terrorism based on the likelihood of terrorist activity actually taking place, not the countries' overall vulnerability to terrorist attack. They said their countries maximize their existing capabilities to address a wide array of threats, including emerging threats, before they create new capabilities or programs.

The GAO also found, however, that countries differed in terms of both the strength of their central governments, and their perceptions of the threat. Officials in Canada, France, and Germany stated that the current threat from terrorism in their countries was low. This tracks with the Department of State report on global terrorism, terrorism. It also states that in Europe has declined, in part, because of the increased vigilance by security forces and the recognition by some terrorist groups that long-standing political and ethnic controversies should be addressed by negotiations. For example, the remnants of Germany's Red Army Faction, once among the world's deadliest, announced the dissolution of their organization.

At the same time, British officials said that terrorism related to Northern Ireland continues to take place and poses a real threat depending, in part, on developments in the peace process. They added that although activity is at historically low levels, the threat remains and is linked to developments in the peace process. Officials from all five countries cited the threat of terrorists using chemical, biological, radiological, and nuclear weapons as particularly unlikely. Israeli officials indicated that the level of terrorism fluctuated with the peace process—terrorism typically increased when the peace process is working, because those opposed to the peace process tried to derail it through violence.

Leadership and Management

The GAO found a common pattern of central leadership and coordination in dealing with the issues involved,¹²¹

Specifically, each country places the majority of resources for combating terrorism under one ministry, but each recognizes that it must coordinate its efforts to develop national policy on combating terrorism so it has interagency coordination bodies. Each country also has clearly designated leadership at the scene of terrorist incidents. The five countries have policies and strategies that emphasize the prevention of terrorism using resources such as intelligence collection, police presence, and security measures. In addition, each country uses its general criminal laws (e.g., those for murder or arson) to prosecute terrorists. The countries also have special terrorism-related laws that allow for special investigation or prosecution mechanisms, and increased penalties. In each of the five countries, the executive branch provides the primary oversight of organizations involved in combating terrorism.

Lead Organization With Policy Coordination

In four countries, most of the resources to combat terrorism—law enforcement and intelligence services—are centralized under a lead agency, generally the countries' ministry of interior or equivalent.⁷ For example, the French Ministry of Interior includes the National Police and the two domestic intelligence agencies that have a primary role in combating terrorism. However, officials from all the countries said they view counterterrorism as an intergovernmental effort that requires coordination among law enforcement, intelligence, and other parts of the government that may be involved in combating terrorism, including foreign affairs, the military, and health and emergency services. Since they view combating terrorism as an interagency effort, officials in each country identified the prime minister or the chancellor as the one person in charge of combating terrorism. Below that level, the effort to combat terrorism requires an interagency body to formulate policy, coordinate activities, and provide recommendations to the prime minister or the chancellor. In Israel, for example, there is an interagency body called the Bureau for Counterterrorism that coordinates activities and provides advice to the prime minister regarding terrorism matters. Appendix I shows the interior ministries or equivalent that lead efforts to combat terrorism and the interagency bodies that provide coordination and advice on terrorism issues to the prime minister or the chancellor.

Clearly Designated Incident Leadership

All five countries have clearly designated who is to be in charge during a terrorist incident. For example, in the United Kingdom, the local Chief Constable (i.e., chief of police) has overall control of all aspects of handling a terrorist incident. For Israel, the National Police are in command within Israel, and the military are in command in the occupied territories. Appendix I provides details on who is designated to command at terrorist incidents for the rest of the countries.

In Israel, the National Police are under one ministry; however, the main domestic and international intelligence services are not in the same ministry as the National Police and report directly to the prime minister.

Incident leadership is reinforced through written agreements and contingency plans or other agreements. For example, in Canada, the Royal Canadian Mounted Police has written agreements with major municipal police departments on who leads the incident response. The French government has written interagency contingency plans with command and control details for such terrorist situations as a heightened threat, aircraft hijacking, ship hijacking, or a chemical attack.

Officials in the five countries stated that they use the agreements or plans as the basis of their exercises to practice their response, which further reinforces who leads at the incident site. Clear incident command is also strengthened because the incident commander controls all response elements, including police, fire, medical, and other emergency services. Thus, there is one commander for police activities (e.g., assaults, arrest, and gathering evidence) as well as other emergency activities (e.g., evacuation, search and rescue, medical treatment, and decontamination). Officials in the United Kingdom cited the importance of having one person—the Chief Constable—in charge of the entire response. Officials in the other four countries made similar comments on the need for clear and unified leadership for the whole range of activities in a response to a terrorist attack.

Policies and Strategies

The GAO also found that all five countries had some strategies in common, and ones which emphasized prevention over response, and which placed a heavy emphasis on intelligence in order to support the prevention effort:¹²²

Each country had developed policies to combat terrorism through their experience with various terrorist groups. The five countries' national policies to combat terrorism, which were not always written, emphasized prevention. Canadian officials were the only ones to provide us with their written policies on terrorism. Officials in the other countries told us they had no written policies. To implement their national policies, these countries had strategies that included intelligence collection, police presence, and other deterrent measures.

For example, the strategies in all five countries include domestic intelligence, and each has at least one security intelligence organization that gathers intelligence on domestic terrorist activities. Officials we spoke with said that an effective intelligence capability is essential for preventing acts of terrorism in their countries. In general, the role of their domestic security intelligence organizations is to prevent acts of terrorism by gathering information through a variety of sources and methods; assessing the threats to security; and monitoring and sometimes disrupting the activities of certain groups considered to be a threat within the country.

All of the countries' domestic intelligence organizations are separate from their law enforcement organizations. In Canada, France, and the United Kingdom, these organizations are under a single ministry. In Germany there are parallel federal and state intelligence and law enforcement organizations, and both are under their respective ministries of the interior. In Israel, the intelligence organizations report directly to the prime minister, and the national police are under the Ministry of Public Security. Cooperation between both law enforcement and intelligence organizations was cited by officials in all five countries as important, in part, because the domestic intelligence organizations do not have powers of arrest. Law enforcement organizations become involved in combating terrorism when information from the intelligence services indicates that criminal activity has occurred, or is likely to occur, or when their own criminal intelligence sources indicate such.

...In addition to a strong intelligence capability, we found that the countries' strategies included using a visible police presence to prevent acts of terrorism. For example, in France, when there is a specific terrorist threat, law enforcement increases its public presence in a visible show of force. Likewise, the German Federal Border Police can provide additional manpower to supplement state police at events such as political demonstrations. In Israel, the National Police, as well as military personnel, is present at various locations throughout the metropolitan areas to respond to incidents as needed.

As part of their prevention strategies, the five countries use a variety of other techniques to deter terrorist

attacks. For example, all five countries use physical barriers in certain critical areas and government buildings to deter direct attacks. Other techniques are as follows. In Israel, individuals and their belongings are often physically searched by police, defense personnel, or security contractors and pass through metal detectors before entering such places as shopping centers, airports, and local attractions. In the United Kingdom, police use video cameras to monitor daily events and watch for suspicious activity in London. In France, persons entering government buildings typically walk through metal detectors.

Claimed Reliance on Criminal Prosecution as the Major Response and Deterrent

Rather than deterrence and retaliation, most countries relied largely on conventional criminal prosecution and punishment – although Israel seems to have understated the linkage between the deterrent and offensive use of its military forces and counterterrorism, and Britain seems to have understand the role of its military forces and intelligence branches in performing direct operations against terrorist groups:¹²³

All five countries use their general criminal laws to prosecute offenses omitted during a terrorist act, such as the crimes of murder, arson, kidnapping, and hijacking. According to Canadian officials, treating terrorism as ordinary crime removes the political element and thereby dilutes the effectiveness of the terrorist act. The countries have also enacted a variety of special laws that relate to terrorism that may include a statutory definition or description of terrorism, or may invoke special investigation or prosecution procedures, or provide for increased penalties.

Under French law, certain criminal offenses are considered terrorism when the acts are intentionally linked to an individual or group whose purpose is to cause a serious disruption of public order through intimidation or terror. Penalties may be increased if a criminal offense is related to such terrorism. France also has special judicial procedures to address terrorism such as special courts and prosecutors. Germany's criminal code has a special prohibition against the formation and support of a terrorist association.

In addition to its general criminal laws, Israel has two principal laws that govern terrorism that contain a number of criminal offenses such as supporting terrorist organizations. The United Kingdom has two principal terrorism laws that designate a number of criminal offenses relating to membership in and support of terrorist organizations. Appendix III provides additional information on the terrorism-related laws in the five countries.

Oversight, Planning, Programming, and Budgeting

None of the countries carried out oversight, planning, programming, and budgeting activities similar to those in the US:¹²⁴

Oversight reviews of programs and resources for effectiveness, efficiency, and legality are primarily the responsibility of those ministers in the executive branch that have a role in combating terrorism. Officials told us that in their parliamentary style of government, ministers are accountable for oversight and that this function is embedded in the ministers' responsibilities. They generally viewed oversight as an ongoing routine function of agency management, not an independent or separate review function. For example, in

France, the Minister of the Interior, through their daily activities, reviews or oversees the activities of those resources within the Ministry.

The legislatures in these countries do not hold oversight hearings or write reports that evaluate programs to combat terrorism. In these parliamentary style governments, the legislative branches do not provide ongoing independent oversight of efforts to combat terrorism. While the five countries do conduct some legislative review of national security activities (e.g., through designated legislative committees), these reviews generally have not focused on activities to combat terrorism. At times, some members of the legislative branch are included in standing or ad hoc executive oversight bodies. In Canada and Israel, independent reviews of activities to combat terrorism are done by their national audit agencies. Appendix IV summarizes oversight organizations and functions in the five countries we visited.

Officials in the ministries involved in combating terrorism within the five countries we visited said they made resource allocations based upon the likelihood of threats taking place, as determined by intelligence assessments. While the officials we met with discussed resource levels in general, none of the five countries tracked overall spending on programs to combat terrorism. Such spending was imbedded in other accounts for broad organizational or functional areas such as law enforcement, intelligence, and defense. Due to resource constraints, they said their countries maximize their existing capabilities to address a wide array of threats, including emerging threats, before they create new capabilities or programs.

Resource Allocations Are Targeted at Likely Threats, Not Vulnerabilities: Limited Concern with WMD Threats

The GAO also found that none of the countries shared threat perceptions similar to those that are now the focus of US planning, although part of the reason for this response is that the GAO only examined their response to conventional terrorism, and not to the potential threat that state actors might carry out covert attacks:¹²⁵

The five countries we reviewed receive terrorist threat information from their civilian and military intelligence services and foreign sources. Using various means, each of the countries' intelligence services continuously assess these threats to determine which ones could result in terrorist activity and require countermeasures, which ones may be less likely to occur but may emerge later, and which ones are unlikely to occur.

Officials in all countries told us that because of limited resources, they made funding decisions for programs to combat terrorism based on the likelihood of terrorist activity actually taking place, not the countries' overall vulnerability to terrorist attack. For example, each of the countries may be vulnerable to a chemical, biological, radiological, or nuclear attack by terrorists, but officials believe that such attacks are unlikely to occur in the near future for a variety of reasons, including the current difficulty in producing and delivering these types of weapons.

Furthermore, officials in one country told us that the effects of these types of weapons would alienate the population from the political aim of the terrorist groups and therefore did not view this type of attack as likely. Officials we spoke with believed that conventional bombs and other traditional means, such as hijacking, are more likely to occur.

For less likely but emerging threats, officials in the five countries told us that they generally try to maximize their existing capabilities for responding to such threats, rather than create new programs or capabilities. For example, the same capabilities used to respond to a fire, industrial explosion, or chemical spill would be used for a terrorist incident involving chemical, biological, radiological, or nuclear weapons.

In addition, officials in each country said additional capabilities from neighboring states, provinces, cities, or national governments could be used by local authorities if the situation exceeded their capabilities. For example, Germany plans to rely on existing capabilities within the states rather than develop new federal capabilities.

Likewise, Israel has not developed new capabilities, but it has a nationwide program that provides gas masks and training to its citizens for defense against chemical or biological attack in wartime that officials said has use for terrorist attacks.

The countries generally did not have major training programs in place to train emergency response personnel for chemical, biological, radiological, or nuclear attacks. However, the United Kingdom has a limited program to train selected police officials as incident commanders and is considering a training program for response personnel in selected locations. Also, Canada has launched a policy initiative to develop a strategy to strengthen national counterterrorism response capability, particularly the ability to respond to chemical, biological, radiological, and nuclear terrorist attacks.

Only France has created new capabilities to respond to chemical, biological, radiological, and nuclear terrorist attacks.

Learning from Foreign Countries

These conclusions imply that the US has comparatively little to learn from the overall response its friends and allies are making to the emerging threats posed by weapons of mass destruction and new forms of covert state and terrorist/extremist attack. This may reflect the fact that Israel sees such threats largely in military terms, and most European nations do not face the mix of global threats facing the US. France is the only nation in Europe that has had enough recent experience with nations and movements that might use weapons of mass destruction to have some kind of contingency capability.

At the same time, it is clear that all five countries have seen the need for a single lead agency, emphasize prevention, and separate intelligence from police and related prevention and enforcement activity. They also have unified leadership in response to incidents. This tends to reinforce the conclusion that having a single lead agency or office lead the US may be an important reform, and that the US might also benefit from having a unified leader for all forms of incident response.

Commission Recommendations

While the federal government has failed to provide either meaningful transparency or measures of effectiveness, for its efforts, three major commissions have released reports with recommendations applying to federal counterterrorism efforts in 1999 and 2000. The Advisory Panel to Assess Domestic Response Capabilities, also known as the Gilmore Commission, released its first report, “Assessing the Threat,” on December 15, 1999. The National Defense Authorization Act for Fiscal Year 1999 created the Gilmore Commission. The Act directed the Gilmore Commission to assess federal domestic preparedness programs, including training for local responders, coordination and funding, and local equipment deficiencies, and to release three annual reports. The Commission gave eight recommendations on domestic preparedness in its first report.

The National Commission on Terrorism, also known as the Bremer Commission, released its report, “Countering the Changing Threat of International Terrorism,” in June 2000. The 1999 Foreign Operations, Export Financing, and Related Programs Act established the Bremer Commission and directed the Commission to review federal counterterrorism policies regarding the prevention and punishment of international terrorism against the United States. The Commission excluded domestic terrorism and consequence management from the scope of its study. The Commission had a wide variety of recommendations ranging from intelligence to domestic preparedness.

Comparison of Major Recommendations

The U.S. Commission on National Security/21st Century, also known as the Hart-Rudman Commission, was mandated to examine and propose changes to the national security strategy to prepare for the 21st Century. The Hart-Rudman Commission released its strategy report, “Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom,” on April 15, 2000. Though the Hart-Rudman Commission gave broad strategic recommendations, some apply to federal counterterrorism efforts. Table Thirty-Five illustrates which of these recommendations coincide and which do not. Since the each commission had a

different area of focus, no identical recommendation came from all three commissions. However, there are areas where the recommendation of two of the three commissions match. Many recommendations from the Gilmore Commission and the Hart-Rudman Commission coincide with the Bremer Commission because the Bremer Commission had the widest scope on terrorism

Table Thirty-Five

Comparison of Commission Recommendations

	Gilmore	Bremer	Hart-Rudman
Executive Coordination	X	X	
Congressional Coordination	X	X	
Information Collection/Sharing	X	X	
Authority Roles	X	X	
Controls of Pathogens		X	X
International Consensus Against Terrorism		X	X
Biological Surveillance		X	X
National Plan	X		
Threat Assessments	X		
Terms and Definitions	X		
Responder Standards	X		
Personal Liability		X	
State Sponsorship		X	
Terrorist Organization Designation		X	
National Fight Against Terrorism		X	
Preparedness Practice		X	
Special Forces			X

Source: Adapted by Steve Chu

Evaluating Major Recommendations

The previous analysis validates many of these recommendations, although it raises important questions about others.

Gilmore and Bremer Commissions: Executive Coordination and Management

The Gilmore Commission had similar recommendations to the Bremer Commission in four areas: executive coordination, congressional coordination, information collection and dissemination, and authority roles. For executive coordination, both commissions recognize that the federal agencies are uncoordinated in regards to counterterrorism. To alleviate this problem, the Gilmore Commission supports the concept of the NDPO:

...the Federal bureaucratic structure is massive and complex. In various forums, state and local officials consistently express frustration in understanding where or how to enter this bureaucratic maze to obtain information, assistance, funding and support. In addition, Federal programs, especially those involving grants for funding or other resources, may be overly complicated, time consuming, and repetitive.

In recent months, the Federal Bureau of Investigation, pursuant to its "lead-agency" role (specified in the related Presidential Decision Directives) for crisis management for terrorism involving weapons of mass destruction, was directed by the Attorney General of the United States to organize, within its own resources, a National Domestic Preparedness Office (NDPO). The ostensible purpose of the NDPO is to serve as a focal point and "clearinghouse" for related preparedness information and for directing state and local entities to the appropriate agency of the Federal government for obtaining additional information, assistance, and support. There has been discussion about the issue of whether the FBI is the appropriate location or whether the NDPO structure and approach is the most effective way to address the complexities of the Federal organization and programs designed to enhance domestic response capabilities. The Panel is convinced that the *concept* behind the NDPO is sound, and notes with interest that the Congress has recently authorized and appropriated funds (\$6 million) for the operation of the NDPO. While that authority will give the NDPO some wherewithal to operate and to hire persons from outside the FBI, the Panel has seen no specific direction to other Federal agencies to provide personnel or other resources to the NDPO, to assist in a concerted, well-coordinated effort.

The Bremer Commission takes a more direct approach to solving the coordination problem and recommends that the national counterterrorism coordinator participate in OMB budget decisions:

The United States does not have a single counterterrorism budget. Instead, counterterrorism programs exist in the individual budgets of 45 departments and agencies of the Federal Government. The National Coordinator for Security, Infrastructure, and Counterterrorism (currently a member of the President's staff) is responsible for ensuring that the counterterrorism programs in these departments and agencies meet the President's overall counterterrorism objectives. To discharge this responsibility, the National Coordinator established a process to set priorities, develop counterterrorism initiatives and review their funding in agency budgets. This process is an efficient means of balancing counterterrorism program requirements against other agency priorities, but it has a significant drawback. The National Coordinator has no role in the critical step when the Office of Management and Budget (OMB) decides what agency programs will be funded and at what levels. This decision is conveyed to the agencies when budget revisions are passed back to the agencies (called passbacks).

The Commission believes that whoever coordinates the national counterterrorism effort on behalf of the President should also have the authority to ensure that the President's counterterrorism objectives are

reflected in agency budgets. That means the coordinator should participate with OMB in the passback of counterterrorism budget submissions, as well as in the final phase of the budget process when agencies appeal OMB's decisions

Gilmore and Bremer Commissions: Congressional Oversight

The Gilmore and Bremer Commissions also agreed that congressional coordination and oversight of counterterrorism programs needed improvement. The Gilmore Commission recommended an ad hoc Joint Special or Select Committee to coordinate congressional involvement in counterterrorism:

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

The Bremer Commission did not go as far as to recommend a joint committee but did suggest joint hearings as a first step towards congressional coordination:

...Congress should develop mechanisms for coordinated review of the President's counterterrorism policy and budget, rather than having each of the many relevant committees moving in different directions without regard to the overall strategy.

As a first step, the Commission urges Congress to consider holding joint hearings of two or more committees on counterterrorism matters. In addition, to facilitate executive-legislative discussion of terrorism budget issues, the House and Senate Appropriations committees should each assign to senior staff responsibility for cross-appropriations review of counterterrorism programs.

Finally, the Commission notes the importance of bipartisanship both in Congress and in the executive branch when considering counterterrorism policy and funding issues.

Both the Gilmore and Bremer Commissions highlighted the need for improved information collection and dissemination between counterterrorism officials. The Gilmore Commission cited the Los Angeles area and New England as possible models information sharing and suggests additional security clearances for state and local officials:

State and local officials express the need for more "intelligence", and for better information sharing among entities at all levels on potential terrorist threats. While the Panel is acutely aware of the need to protect classified national security information, and the sources and methods by which it may have been obtained,

the Panel believes that more can and must be done to provide timely information—up, down, and laterally, at all levels of government—to those who need the information to provide effective deterrence, interdiction, protection, or response to potential threats. This may entail granting security clearances to additional officials at the state and local level. And as noted, the FBI report on Project Megiddo, and the briefings of its findings to state and local officials, is salutary.

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

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

Gilmore and Bremer Commissions: Intelligence Gathering and Sharing

The Bremer Commission provides a series of specific recommendations to improve intelligence gathering and sharing. The Commission received much criticism for recommending the CIA recruitment of terrorist informants even if they have been involved in human rights violations. However, the Commission said that the CIA had been creating an “overly risk averse” environment and needed to send a clear message that recruiting terrorists is a good thing.

There seems good reason to endorse this conclusion. The use of suspect informants is the source of most civil law enforcement activity and much of the collection of human intelligence collection. If law enforcement and intelligence agencies were denied access to such sources on legal or humanitarian grounds, this would cripple their activities and produce immense additional human suffering. Terrorists are not usually criminals, and often have strong ideological motives. They are harder to track and subvert, and they are potentially far more dangerous. In the case of terrorists associated with the risk of CBRN attacks on the use, the threat is so great that it can literally be catastrophic. The Bremer Commission's recommendation is common sense, opposing it means trying to live in a fantasy world that makes no sense at all.

The Bremer Commission also concluded that the FBI has a “risk-averse culture” and needed to clarify the guidelines for collecting information on possible international terrorists. Among the other recommendations of the Bremer Commission was the relaxation of DOJ

scrutiny for approving electronic surveillance, the need for modern computer and communications technology to keep up with terrorists, the need for more linguists, and the need for the maximum dissemination of terrorist-related information as the law allows to relevant officials. There seems to be considerable truth in these comments as well, but it is unclear that the FBI has a risk averse culture as distinguished from DOJ, and part of the problem seems to be the tacit assumption that the same procedures should be followed for all threats. There almost certainly is a strong case for treating the risk of CBRN attacks differently from lower level threats, and establishing review and authorization procedures to take more “risks” in detecting and preventing such attacks.

Gilmore and Bremer Commissions: Clarify Authority and Command and Control - Giving the Department of Defense a Lead Role

The fourth and last area of agreement between the Gilmore and Bremer Commissions was the need to clarify authority and command and control when a terrorist act occurs. The Gilmore Commission believes that the issues of “who’s in charge” and how command and control is transferred from local responders to federal officials needs to be resolved. The Gilmore Commission said:

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

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

The Bremer Commission made two related recommendations about authority and

command and control, one of which caused some controversy. The Commission recommended the DOD create contingency plans to take assume the lead in the case of a terrorist act so devastating that no other agency is capable of handling. The Commission said:

The Department of Defense's ability to command and control vast resources for dangerous, unstructured situations is unmatched by any other department or agency. According to current plans, DoD involvement is limited to supporting the agencies that are currently designated as having the lead in a terrorism crisis, the FBI and the Federal Emergency Management Agency (FEMA). But, in extraordinary circumstances, when a catastrophe is beyond the capabilities of local, state, and other federal agencies, or is directly related to an armed conflict overseas, the President may want to designate DoD as a lead federal agency. This may become a critical operational consideration in planning for future conflicts. Current plans and exercises do not consider this possibility.

An expanded role for the DoD in a catastrophic terrorist attack will have policy and legal implications. Other federal agencies, the states, and local communities will have major concerns. In preparing for such a contingency, there will also be internal DoD issues on resources and possible conflicts with traditional military contingency plans. These issues should be addressed beforehand.

Effective preparation also requires effective organization. The DoD is not optimally organized to respond to the wide range of missions that would likely arise from the threat of a catastrophic terrorist attack. For example, within DoD several offices, departments, Unified Commands, the Army, and the National Guard have overlapping responsibilities to plan and execute operations in case of a catastrophic terrorist attack. These operations will require an unprecedented degree of interagency coordination and communication in order to be successful.

There are neither plans for the DoD to assume a lead agency role nor exercises rehearsing this capability. Hence, these demanding tasks would have to be accomplished on an ad hoc basis by the military.

The recommendation was distorted by some to mean that the DOD should be the lead agency in all cases of terrorist acts, an assertion the Commission has denied. The Commission recognized that it is possible for a terrorist act to be so overwhelming that only the DOD would be capable responding. The Commission also recommended clarification of the legal authority of responders have in instances of catastrophic terrorism so no one hesitates or acts improperly. The Commission said:

The Constitution permits extraordinary measures in the face of extraordinary threats. To prevent or respond to catastrophic terrorism, law enforcement and public health officials have the authority to conduct investigations and implement measures that temporarily exceed measures applicable under non-emergency conditions. These may include cordoning off of areas, vehicle searches, certain medical measures, and sweep searches through areas believed to contain weapons or terrorists.

Determining whether a particular measure is reasonable requires balancing privacy and other rights against the public interest in coping with a terrorist threat which may lead to massive casualties. Advance preparation is the best way to deal successfully with a terrorist incident without jeopardizing individuals' Constitutional rights.

The Gilmore Commission is almost certainly correct in assuming that someone must be in charge, but this could vary by type of attack and mid to high levels of attack will inevitably directly involve the President and National Security Council. Creating a peacetime Czar or Cabinet level official is only one step in resolving the problem of operational authority.

Similarly, the recommendations of the Bremer Commission seem valid when the attack involves response to a nuclear attack or a biological attack of any significance. It is far less clear that such a response is needed to high explosive or most chemical attacks. At the same time, it will be vital to ensure that biological attacks are properly characterized and that medical science shapes the response. This again illustrates the fact that extensive simulation is needed to determine how best to assign not only lead responsibility in given types attacks, but how to ensure that all proper expertise is given a proper role in leading the response.

Hart-Rudman and Bremer Commissions: Biological Pathogens, International Consensus against Terrorism, and Strengthening of Public Health Systems

The Bremer Commission also had some recommendations that were similar to those of the Hart-Rudman Commission. The three common areas were: control of biological pathogens, international consensus against terrorism, and strengthening of public health systems. As part of a greater counterproliferation effort, the Hart-Rudman Commission recommended an international ban on the creation, transfer, trade, and weaponization of biological pathogens as well as programs to deal with existing stockpiles:

The United States should seek enhanced international cooperation to combat the growing proliferation of weapons of mass destruction. This should include an effective and enforceable international ban on the creation, transfer, trade, and weaponization of biological pathogens, whether by states or non-state actors. Also, when available and implemented with rigor, cooperative programs to deal with existing stockpiles of nuclear, biological, and chemical weapons are cost-effective and politically attractive ways to reduce the dangers of weapons and weapons material proliferation.

The Bremer Commission observed the US controls on the transfer of pathogens and related equipment is nonexistent and recommended HHS to strengthen security and Congress to create stricter controls of pathogens and related equipment:

The Secretary of Health and Human Services should strengthen physical security standards applicable to the storage, creation, and transport of pathogens in research laboratories and other certified facilities in

order to protect against theft or diversion. These standards should be as rigorous as the physical protection and security measures applicable to critical nuclear materials.

The Congress should:

- Make possession of designated critical pathogens illegal for anyone who is not properly certified.
- Control domestic sale and transfer of equipment critical to the development or use of biological agents by certifying legitimate users of critical equipment and prohibiting sales of such equipment to non-certified entities.
- Require tagging of critical equipment to enable law enforcement to identify its location.

Hart-Rudman and Bremer Commissions: Strengthening the International Consensus Against Terrorism and the International Convention for the Suppression of the Financing of Terrorism:

The two commissions gave recommendations to strengthen the international consensus against terrorism. The Hart-Rudman Commission gave a broad suggestion:

The United States should also strive to deepen the international normative consensus against terrorism and state support of terrorism. It should work with others to strengthen cooperation among law enforcement agencies, intelligence services, and military forces to foil terrorist plots and deny sanctuary to terrorists by attacking their financial and logistical centers.

The Bremer Commission was more specific in deepening the international consensus against terrorism by recommending the US ratify the International Convention for the Suppression of the Financing of Terrorism:

In addition to domestic efforts, disrupting fundraising for terrorist groups requires international cooperation. A new United Nations convention, the International Convention for the Suppression of the Financing of Terrorism, provides a framework for improved cooperation. Each signing party is to enact domestic legislation to criminalize fundraising for terrorism and provide for the seizure and forfeiture of funds intended to support terrorism. The parties are to cooperate in the criminal investigation and prosecution of terrorism fundraising, and in extraditing suspects.

...The Congress should promptly ratify the International Convention for the Suppression of the Financing of Terrorism and pass any legislation necessary for full implementation.

The final common recommendation of the Bremer and Hart-Rudman Commissions was the need to strengthen public health capabilities. The Hart-Rudman Commission gave a general recommendation to augment U.S. capabilities, while the Bremer Commission specifically recommended an international surveillance program to monitor outbreaks and terrorist

experimentation with pathogens.

Different Recommendation Areas

The Hart-Rudman Commission only had one counterterrorism recommendation different from the other commissions. The Commission said the US should have specialized forces capable of dealing with threats and blackmail from terrorism and CBRN weapons.

Gilmore Commission: Threat Assessments

The Gilmore Commission focused on domestic preparedness and gave four additional recommendations. One was on threat assessments. The Commission felt that not enough attention was being given to higher-probability/lower-consequence threats and recommended more study of those threats in addition to the lower-probability/higher-consequence threats:

The Panel has indicated its concern about a preoccupation with the “worst-case scenario,” and the attendant assumption that any lesser incident can be addressed equally well by planning for the most catastrophic threat—ignoring the fact that higher-probability/lower-consequence attacks might present unique challenges of their own. As noted, this approach may not be the best means of setting budgetary priorities and allocating resources. The Panel is convinced, therefore, that more attention should be directed to assessments of the higher-probability, lower-consequence end of the potential terrorist threat spectrum—not at the expense of, but in addition to, assessments and analyses of the higher-consequence threat scenarios.

It is not really clear that this is the case in the field, and in much of the practical work being done at the agency and state/local levels. Many of the planning sessions, meetings, and simulations taking place outside the National Security area, do focus on “higher-probability/lower-consequence attacks” even when they describe them as higher level attacks. This, however, illustrates the need to plan for a spectrum of levels and means of attack, and for neither higher-probability/lower-consequence attacks” nor the worst case.

Gilmore Commission: National Strategy for Domestic Preparedness and CBRN Terrorism Response

Another recommendation of the Gilmore Commission is the creation of a national strategy for domestic preparedness and CBRN terrorism response. The Commission is aware that the NDPO plans on developing a national strategy for domestic preparedness issues but

suggests that a true national strategy must be bottom up and have presidential direction:

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

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

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

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

By focusing on higher-probability/lower-consequence threats, while recognizing and addressing concerns about lower-probability/higher-consequence events, a national strategy can lay the groundwork for assessing and monitoring the threat, and for making adjustments to response strategies as required. As has been argued elsewhere, too much of the Federal effort to date—even those programs that ostensibly are

designed to enhance state and local response capabilities—has been predicated on the tacit assumption that preparing for the “worst case” will automatically encompass lesser threats. The foregoing analysis suggests otherwise, because the nature and scale of the consequences can vary so widely. This needs to be recognized and articulated at the national level.

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

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

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

In all frankness, this recommendation has only tenuous logic. It is certainly true that most of the burden of responding to low level attacks and response will fall on local and state officials, but it is not clear that they need a national strategy as much as flexible national assistance than can supplement their activity when needed. Providing a flexible federal capability to deal with bottom up demand is certainly necessary, but it is uncertain that this is a strategy in any normal sense of the term. Conversely, federal response is most needed to deal with mid and high level attacks, even if these are not the most probable near-term contingency.

This issue does, however, raise the broader issue of clearly distinguishing between risks where state and local authorities must have primary responsibility and the kind of CBRN attacks that the federal government must deal with. One problem with much of the current approach to counterterrorism is that it assumes that levels of threat that federal, state, and local authorities have deal with for years deserve the same special attention as new and much more serious threats to the American homeland. There seems no reason that this should be the case.

Gilmore Commission: Standardization of Legal Terms

The final two recommendations by the Gilmore Commission deal with standardization. The Commission recommended codification of terms and definitions related to terrorism. The Commission cited the different definition of weapons of mass destruction by the Nunn-Lugar-Domenici Act and 18 U.S.C, Section 2332a, the definition of terrorism by the FBI and DOD, and the absence of a definition for mass casualties. There may well be a need for such action, but not at the cost of creating legislative inflexibility. Such legislation should also explicitly recognize the threats posed by proliferation and state actors, and not simply “terrorism” If necessary, it should make it clear that there are radically different levels and means of attacks and specify what differences – if any – are needed in the US response.

Gilmore Commission: National Standards for Equipment

The Commission recommended the creation of national standards for equipment used by responders to a terrorist incident. The Commission recognized that different response entities may have incompatible equipment that would greatly diminish responder capabilities. The Commission is aware of DOJ’s efforts through the National Institute of Justice to develop a list of equipment that meets certain standards, but the Commission suggested that more research and development was needed to develop effective standards for compatibility and inter-operability:

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

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

In order to develop and maintain operationally effective standards for equipment compatibility and inter-

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

To help to reassure responders that the equipment that is being used is in fact capable of doing what it is designed to do, it is likely that an ambitious program of independent testing and evaluation will have to be undertaken. The Panel recognizes that any such program will likely have to be conducted—because of its national implications—under Federal sponsorship; and will require the addition or reallocation of significant resources. For reasons that are self-evident, local responders are insisting that testing be done with “live” agents.

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

The problem with this recommendation is that it assumes that federal, state, and local authorities already know the effects of CBRN attacks, what to stockpile to respond to them, where to put the stockpiles, and when and how to distribute them. This may be true in case of lower levels of attack, although it is brutally clear in meeting after meeting that local and state officials, and elements of federal agencies, see such stockpiles as one more way of getting more federal money to solve long-standing problems or provide new capabilities that have little to do with terrorism. There is a real risk of creating a new federal entitlements program.

The problem is very different in dealing with more lethal levels of CBRN attacks. It is not clear that federal, state, and local authorities know what to buy, where to put it, or how to ensure it can get to the user. There are certainly some cases where the need is obvious, but in many cases – particularly in the event of biological and nuclear attacks, far more work needs to be done on requirements planning.

Bremer Commission: Treatment of Former and Future States of Concern

The Bremer Commission focused on what could be improved to combat international terrorism. The Commission’s remaining recommendations were mainly related to designation of state sponsors and foreign terrorist organizations and to national counterterrorism efforts. For designations, the Commission recommended that the US keep Iran and Syria on the list of state sponsors:

Iran remains the most active state supporter of terrorism. Despite the election of reformist President Khatami in 1997, the Iranian Revolutionary Guard Corps and Ministry of Intelligence and Security have continued to be involved in the planning and execution of terrorist acts. They also provide funding, training, weapons, logistical resources, and guidance to a variety of terrorist groups. In 1999, organizations in Tehran increased support to terrorist groups opposed to the Middle East peace process, including Lebanese Hizbollah and Palestinian rejectionist groups such as the Islamic Resistance Movement (HAMAS), the Palestine Islamic Jihad (PIJ), and the Popular Front for the Liberation of Palestine-General Command (PFLP-GC). Iran continues to assassinate political dissidents at home and abroad. The Iranians responsible for terrorism abroad are often also responsible for political oppression and violence against reformers within Iran. So a firm stance against Iranian-sponsored terrorism abroad could assist the reformers.

There are indications of Iranian involvement in the 1996 Khobar Towers bombing in Saudi Arabia, in which 19 U.S. citizens were killed and more than 500 were injured. In October 1999, President Clinton officially requested cooperation from Iran in the investigation. Thus far, Iran has not responded.

International pressure in the Pan Am 103 case ultimately succeeded in getting some degree of cooperation from Libya. The U.S. Government has not sought similar multilateral action to bring pressure on Iran to cooperate in the Khobar Towers bombing investigation.

The Syrian Government still provides terrorists with safehaven, allows them to operate over a dozen terrorist training camps in the Syrian-controlled Bekaa Valley in Lebanon, and permits the Iranian Government to resupply these camps. Since its designation as a state sponsor of terrorism, Syria has expelled a few terrorist groups from Damascus, such as the Japanese Red Army, but these groups already were of marginal value to Syrian foreign policy. Meanwhile, Damascus continues to support terrorist groups opposed to the peace process. Although Syria recently made a show of "instructing" terrorists based in Damascus not to engage in certain types of attacks, it did not expel the groups or cease supporting them. This suggests Syria's determination to maintain rather than abandon terrorism.

The Bremer Commission also recommended that the US designate Afghanistan as a state sponsor and consider designating Pakistan or Greece as countries "not cooperating fully with U.S. antiterrorism efforts." On Pakistan, the Commission said:

Pakistan has cooperated on counterterrorism at times, but not consistently. In 1995, for example, Pakistan arrested and extradited to the United States Ramzi Ahmed Yousef, who masterminded the World Trade Center bombing in 1993. In December 1999, Pakistan's cooperation was vital in warding off terrorist attacks planned for the millennium. Even so, Pakistan provides safehaven, transit, and moral, political, and diplomatic support to several groups engaged in terrorism including Harakat ul-Mujahidin (HUM), which has been designated by the United States as a Foreign Terrorist Organization (FTO). HUM is responsible for kidnapping and murdering tourists in Indian-controlled Kashmir. Moreover, as part of its support for Usama bin Ladin, HUM has threatened to kill U.S. citizens.

The Commission suggested that countries designated "Not Cooperating Fully" should not be eligible for the Department of State's Visa Waiver Program. For non-state sponsored terrorist organizations, the Commission recommended more frequent updating and inclusion of groups into the Secretary of State's designation of Foreign Terrorist Organization. The Commission also recommended that Congress review of Foreign Terrorist Organization statute to determine if

changes need to be made.

Bremer Commission: Targeting Terrorist Financial Resources

For national counterterrorism efforts, the Commission recommended that the US target terrorist financial resources. The Commission suggested the creation of a joint task force of all relevant agencies that combat terrorist fundraising to develop and implement a plan to disrupt terrorist financial activities. The Commission also suggested that the Office of Foreign Assets Control in the Department of Treasury created a unit dedicated to enforcing economic sanctions against terrorist organizations. The Commission said:

Rather than relying heavily on the FTO process, the U.S. Government should take a broader approach to cutting off the flow of financial support for terrorism from within the United States. Anyone providing funds to terrorist organizations or activities should be investigated with the full vigor of the law and, where possible, prosecuted under relevant statutes, including those covering money laundering, conspiracy, tax or fraud violations. In such cases, assets may also be made subject to civil and criminal forfeiture.

In addition, the Department of the Treasury could use its Office of Foreign Assets Control (OFAC) more effectively. OFAC administers and enforces economic sanctions. For example, any U.S. financial institution holding funds belonging to a terrorist organization or one of its agents must report those assets to OFAC. Under OFAC's regulations, the transfer of such assets can be blocked. OFAC's capabilities and expertise are underutilized in part because of resource constraints.

Other government agencies, such as the Internal Revenue Service and Customs, also possess information and authority that could be used to thwart terrorist fundraising. For instance, the IRS has information on nongovernmental organizations that may be collecting donations to support terrorism, and Customs has data on large currency transactions. But there is no single entity that tracks and analyzes all the data available to the various agencies on terrorist fundraising in the United States.

These recommendation make excellent sense, provided that they are carried out under sufficient review to ensure that the selection of groups and individuals to be monitored does not become an abuse of civil liberties, or lead to surveillance of groups that are politically undesirable or who criticize the US without posing a threat of violence.

Bremer Commission: Monitoring Foreign Students

The Bremer Commission proposed that the federal government create a monitoring system of foreign students to ensure none are exploiting the US educational system for terrorist purposes. The Commission said:

While the problems of controlling America's borders are far broader than just keeping out terrorists, the

Commission found this an area of special concern. For example, thousands of people from countries officially designated as state sponsors of terrorism currently study in the United States. This is not objectionable in itself as the vast majority of these students contribute to America's diversity while here and return home with no adverse impact on U.S. national security. However, experience has shown the importance of monitoring the status of foreign students. Seven years ago, investigators discovered that one of the terrorists involved in bombing the World Trade Center had entered the United States on a student visa, dropped out, and remained illegally. Today, there is still no mechanism for ensuring the same thing won't happen again.

One program holds promise as a means of addressing the issue. The Coordinated Interagency Partnership Regulating International Students (CIPRIS), a regional pilot program mandated by the 1996 Illegal Immigration Reform and Immigrant Responsibility Act (IIR/IRA) collects and makes readily available useful and current information about foreign student visa holders in the United States. For example, CIPRIS would record a foreign student's change in major from English literature to nuclear physics. The CIPRIS pilot program was implemented in 20 southern universities and is being considered for nationwide implementation after an opportunity for notice and comment. The Commission believes that CIPRIS could become a model for a nationwide program monitoring the status of foreign students.

This proposal drew much criticism from civil liberties organizations that claimed the monitoring would infringe on civil liberties and constitutional rights. In balance, however, the Bremer Commission seems correct. Studying in the US is not a right. Student visas are granted only to legitimate students for a specific course of study. Tracking students to the point of ensuring that they (a) meet the terms of their visa, and (b) there is some record of their course of study is little more than common sense.

Bremer Commission: Liability Insurance

The Bremer Commission recommended that the FBI and CIA reimburse their agents for the full cost of personal liability insurance so that agents could be more aggressive in combating terrorism and not fear lawsuits for officially sanctioned activities. Providing such insurance seems valid and providing it would not affect adequate supervision or discipline or the right to sue and seek legal redress with all of the attendant public scrutiny.

Bremer Commission: Realistic Exercises

The Commission also recommended more federal preparedness exercises and more funding for TOPOFF, the senior management exercise administered by the DOJ and FEMA. The Commission said:

In addition to DoD exercises, a realistic interagency exercise program, with full participation by all relevant federal agencies and their leaders, is essential for national preparedness to counter a catastrophic terrorist

attack. In June 1995, the President established an interagency counterterrorist Exercise Subgroup and program which included preparation for a catastrophic terrorist attack. However, not all federal agencies have participated in or budgeted for these exercises.

Additionally, in September 1998, Congress funded and mandated the Department of Justice and the Federal Emergency Management Agency to conduct a counterterrorism and consequence management exercise, called TOPOFF, involving relevant federal agencies and their senior leadership, with select state and local governments participating, to evaluate the U.S. Government's preparedness for a catastrophic terrorist incident. However, sufficient funding was not provided and there is no requirement to exercise on a regular schedule.

The President should direct (1) the Exercise Subgroup, under the direction of the national coordinator for counterterrorism, to exercise annually the government's response to a catastrophic terrorism crisis, including consequence management; and (2) all relevant federal agencies to plan, budget and participate in counterterrorism and consequence management exercises coordinated by the Exercise Subgroup and ensure senior officer level participation, particularly in the annual exercises.

As has been noted earlier, it is far more important that federal, state, and local authorities understand what they really need to do and how to do it than to establish new lines of authority, fund the wrong program, and focus efficiently on the wrong set of contingencies and requirements.

General Recommendations

The US faces real and growing potential threats from state actors, their proxies, or independent extremists and terrorists. While US agencies and analysts have tendency to exaggerate the immediate threat, or the threat posted by given actors, there are many potentially hostile foreign and domestic sources of such threats, and some key threats like biological weapons involve rapidly changing technologies that will pose a steadily growing threat to the America homeland.

It is also clear from the proceeding analysis that the federal government is making major progress in many areas, and laying the groundwork for improved cooperation with states, localities, the private sector, and the public. Indeed by the standards of many governments that face far more clear threats than the US, the US has already made significant progress in beginning to address these issues. In many cases, the US is already well ahead of its friends and allies.

At the same time, there still seems to be much that can be done. Some detailed recommendations have already been discussed in the analysis of the threat, and federal activities and spending by agency, and the recommendations of various commissions. There are, however, a number of additional recommendations that could help refine and improve the US effort..

Planning for Both Higher-Probability, Lower-Consequence and Low Probability/Catastrophic Events

The US must come firmly to grips with the fact it does not exist at the end of history and has not forged a kinder and gentler world:

- *Unchecked vulnerability is an unacceptable danger for “the world’s only superpower.”* Nature may abhor a vacuum, but enemies do not, and the evolution of more effective homeland defense is almost certainly essential to deterrence. At the same time, the very term “homeland defense” can be misleading. There are no boundaries that separate US counterproliferation and counterterrorist activity in defense of the American homeland from defense of its allies, military forces, and citizens overseas.
- *Deterrence, counterproliferation, counterterrorism, and law enforcement must be closely linked in dealing with these new threats, and it is clear that US must rethink many of its current security concepts.* Even the strongest advocates of homeland defense must recognize that a better offense may often be more effective than improved defense. Improving the offensive threat of retaliation overseas may often be the best way of defending both US interests overseas and US territory. A given investment in strengthening our allies may often be a better defense against proliferation and terrorism than investing in domestic counterterrorism programs. Hard trade-offs may have to be made between investments in the intelligence needed to intimidate and deter foreign states and terrorist groups, and the law enforcement capabilities needed to intercept attackers once they enter the US.
- *The US cannot afford to rely on rethinking the offense as a substitute for improved*

defense, anymore that it can use defense as a substitute for deterrence, offense, and retaliation: The US cannot prepare itself for the new threats posed by asymmetric warfare, foreign proliferation and terrorism, and domestic violence using new means like chemical, biological, and information warfare without much stronger programs to prevent such attacks in the US and to respond to them if they succeed. The world of the 21st Century will not be a repetition of the mutual assured destruction of the Cold War. Radical states, regimes acting under extreme pressure, terrorists, and American citizens can turn threats like chemical, biological, and nuclear weapons into grim realities in ways the US will never be able to deter with complete confidence.

- *The US must act now if it is to prepare for the future.* Developing an effective program means thinking at least 25 years into the future. It will take at least a decade for federal, state, and local authorities to develop the organization they need to deal with these threats. There are massive organizational problems that federal, state, and local authorities must solve to cooperate efficiently. The role of the federal government must be redefined in ways that are both compatible with a free society and which can preserve one when it is under attack and when attacks are successful. It will take years of exercises, tests, and training to determine what courses of action can be made to work and are most effective. Investing in such a process of change means that it must be flexible and modular enough to react to the fact no one can predict the nature of future attacks, but any meaningful improvement in capability will be so expensive that it can only be justified if it can cope with uncertainty.
- *The US must decide whether it will begin now to fund effective defenses attacks on a scale far different from any form of covert or serious attack than it has planned to deal with since the end of its efforts to provide civil defense against nuclear attack.* Marginal changes in federal, state, and local efforts, and in the relationships between federal, state, and local agencies, can do much to cope with the threat posed by attacks using large amounts of high explosives, chemical weapons, and low-lethality biological and radiological attacks. While the level varies by state and locality, attacks involving 1,000

to 10,000 do not require radical changes in response capabilities. Nuclear and high lethality biological attacks can, however, easily produce casualties in excess of 10,000-100,000 Americans. To date, most studies and exercises indicate that existing programs and capabilities would not be adequate to deal with such attacks, and they would require far more decisive federal action and intervention than is currently feasible. There are those who argue strongly that no such threat currently exists and those who argue with equal force that they are inevitable. The present reaction of the federal government seems to be to try to improve near-term response capabilities to deal with lower levels of attack while conducting research and development into the higher levels of attack, but the policies involved remain unclear and the actions of federal agencies reflect very different perceptions of these threats.

- *The US must take a new approach to research and development and technology:* There are many areas of new technologies which must be moved off the drawing board, tested, deployed, and modified if the US is to have defensive tools that begin to match its offensive capabilities. At the same time, the US needs careful net assessments of the trends in the threat and how these impact on new approaches to defense and response. Effective planning means that the US cannot afford to mix the myth of technology with the reality. The past track record of US efforts to create and use new technologies in its defense is one of amazing eventual success. At the same time, it is one of almost universal evidence that even the best technologists cannot be trusted to create successful and deployable tools with anything like the promised effectiveness at the promised cost and time.

The development of such a complex approach to threat assessment, based on a frank admission of the vast uncertainties involved, goes against the basic grain of the American character, and forces far more demanding criteria for program justification than are normally required. The US cannot, however, deal effectively with threats posed by state actors, their proxies, or independent extremists and terrorists unless it adopts such an approach.

Even if the US adopts such an approach, however, it will still have to concentrate its limited

resources on making marginal improvements in current capabilities to deal with current threats, while adopting a research and development-driven approach to dealing with more serious and emerging threats. As a result, any US program is likely to have marginal impact, and require constant evolution for at least the next half decade.

Reacting to the Uncertain Nature of the Threat

There are many “true believers” who feel that a given threat will or will not materialize in a given form. Given the inherently uncertain nature of predictions as to who will be a threat, the means of attack they will use, and the effectiveness of the means of attack they use, it is almost certain that some of these “true believers” will prove to be right. The problem is that there is no sufficient evidence to say which threats are most important, or to predict the means of attack and level of effectiveness.

Federal programs are being forced to deal with an extremely broad spectrum of potential threats that individually have low probability, but where there is high probability that some of these threats will emerge as threats to the American homeland. As a result, each agency and department tends to threat the threat in terms of its own mission and institutional bias, and this problem cannot be resolved by central direction. Having the National Security Council, a “terrorism” czar, or an interagency forum agree on a given threat or threats will not affect the laws of probability. Uncertainty is simply uncertainty.

There is also an inherent danger in attempting to create a truly coherent program. When a truly high degree of uncertainty exists regarding the need for specific forms of federal action, enforcing a high degree of coherence from the center may actually interfere with the efficient use of resources. In many cases, individual agencies will achieve a higher capability to deal with uncertainty if they suboptimize around those marginal steps each can take to improve their existing capabilities to deal with a wide range of threats. This is particularly true in a sharply resource-constrained environment where many potentially desirable actions will remain unfunded until a much clear pattern of threats emerges.

This is particularly true because the threats at issue involve a wide spectrum of extremely

lethal biological weapons and nuclear weapons. Large amounts of high explosive, chemical weapons, and less lethal biological weapons can produce truly tragic consequences. However, the level of deterrence, defense, and response pales in terms of cost in comparison with the ability to deter, defend, and respond to the kind of attacks that could involve casualties far in excess of 10,000 Americans and billions of dollars worth of damage.

There are three further problems involved in such threat analyses that badly need to be dealt with in further US efforts to plan and execute effective programs:

- *Most of the lethality and effects data for chemical, biological, radiological, and nuclear weapons involve major uncertainties that badly need to be resolved, and the federal government is just beginning to develop effective models and simulations of such effects.* There is no lack of effects data or models per se, simply an immense lack of credibility and parametric modeling of uncertainty in a form that goes from dramatizing the problem to being useful in developing specific lessons for federal, state, and local responses. These problems have also been compounded by a natural tendency to build models to justify given policy recommendations or programs. To be blunt, agencies in the federal government, FCRCs, contractors, and NGOs are far better at using analysis to market given policies and programs than to perform analysis per se. There is a striking lack of intellectual rigor and analytic integrity in many of today's efforts that must be remedied if the US is to prioritize federal actions and funding.
- *Programs shaped around today's threats, or some prioritization based on current assessments, will not solve any of the key problems in planning and programming.* Democracies do not suddenly develop solutions they can then keep secret from their enemies. US programs take time to implement and must be publicly funded and implemented in an open society. As a result, potential attackers can adopt new methods of attack and respond to any remaining gaps in US capability. This makes it absolutely essential to explicitly analyze the cost of defeating any given federal program over time, and the probable impact improving any US capability will have in driving attackers to

use other means.

- *New methods of analysis must be development that examine the present and future balance of offensive, defensive, and response capabilities. They must be supported by adequate net technological assessments, and analysis of countermeasures and costs to defeat all ongoing and proposed federal activities.* It is difficult enough to analyze current or near-term risks, but such analysis simply is not adequate. Effective US programs can take a decade or more to fully implement, and the technology shaping current threats is constantly changing. This is not simply a matter of basic advances like biotechnology, it is a matter of the steadily growing dissemination of the technology equipment needed to produce and deliver large amounts of high explosive, chemical weapons, and biological weapons. Much of the description of potential threats does not explicitly analyze the potential growth or changes in threat technology even when it proposes the adoption of new deterrent, defensive, and response technologies over a period of many years. There is a lack of technological net assessment that is a key not only to identifying and prioritizing effective programs, but to managing them so they counter technology growth.

The Lack of “Transparency” in Federal Programs

There is nothing unique about the lack of transparency in federal programs to deal with the threats posed by state actors, their proxies, and foreign and domestic extremist, and the use of high explosives, chemical, biological, radiological, and nuclear weapons. The US budget, and agency program and budget description often fail to describe their budgets, the nature of their programs, and measures of effectiveness in any detail. Aside from the Department of Defense, there are virtually no future year spending projections, and the Department of Defense classifies the breakouts of its future year spending projections that provide any useful description of how money is to be spent.

Far too much of the federal literature on “terrorism,” however, is threat-driven. It does not describe and justify the program, it describes the threat. There is no description of exactly

what program activities are involved, or of past, current, and projected costs. There are no measures of effectiveness, or total spending and procurement are confused with such spending. As a result, it becomes extremely difficult to understand what the federal government is doing and why it should do it. Many of the descriptions that agencies do provide raise real questions about the extent to which given agencies have simply reshaped existing activities to take account of the fact the Congress is providing new incremental funding, and counter-terrorism has become fashionable.

These problems are compounded in part by the fact that OMB is required to report to the Congress, but there is no central agency charged with creating a plan, program, and budget. At the same time, they are compounded by a host of jurisdictional problems with the Congress, and the lack of a single committee or joint committee structure that could provide a cohesive degree of overview. As a result, there is a large pool of federal reporting on individual problems and issues, but little effort to appraise the overall program.

There are those who would argue that part of the reason for the lack of transparency is security. There are certainly areas like intelligence where detailed program descriptions could compromise security. There are other areas where too detailed a description of US investigative and response capabilities could aid an attacker in planning an attack. In broad terms, however, there is little reason to classify most of the information needed to allow outside analysts to fully understand the nature of federal efforts, and there are good reasons to require federal agencies to provide such data.

To put it bluntly, far too many federal activities seem to have limited substantive value, raise major uncertainties, reflect the reshaping of existing programs to obtain incremental funding, or raise questions about duplication. Furthermore, there is a tendency to imply short-term solutions can be found to long-term problems, or fund minor palliatives simply for sake of seeming to act. Few, if any, programs provide any picture of what it will cost to fully implement the activities agencies are now beginning. None seem to provide meaningful measures of effectiveness, or any analysis of the current and future costs of “defeating” the capabilities being

funded.

- *While there are sharp limits to how much coordination can be forced on a wide range of federal activities, the federal effort would almost certainly benefit from a requirement for a comprehensive annual report similar to the one the Secretary of Defense provides on the national security activities of the Department of Defense, and for including both a net assessment of the threats and US capabilities, and the future year budget implications of given federal activities as well as a description of the current budget request.*
- *Regardless of how the issue of Congressional jurisdiction is resolved, there is also a clear case for requiring the federal government to submit an annual budget justification document, and future year budget plan, that covers all related federal activities at the same time the President submits the federal budget. Such a document could be both unclassified and classified. It would thus ensure that the Executive Branch had to coordinate its programs fully as part of the budget process. It would ensure that whoever is in charge in the federal government had real review authority, and control of money is generally better than a title. It would ensure that all elements of Congress reviewed a common plan, which may be far more important than creating a single new committee. It would also allow full public review and state and local access to the overall federal plan. It is easy to talk about “reinventing government;” it would be nice to actually provide some degree of functional transparency in a critical new mission area.*

Focusing on Priorities, Programs, and Trade-offs: Creating Effective Planning, Programming, and Budgeting

The US would face serious resource allocation problems even if CBRN threats were less uncertain and ambiguous. The threat posed by covert, terrorist, or extremist use of weapons of mass destruction is only one of the new threats the US must react to. Homeland defense includes direct threats such as missile attack, and other evolving threats like information warfare. There are other transnational threats like narcotics, organized crime, and illegal immigration that pose a

serious threat to American society even if they are not military or paramilitary in character. At the same time, the US faces major problems in funding its existing future year defense program, and its civil discretionary and entitlements budget. Money is, and will remain, a critical factor, and will force hard trade-offs on all government action.

This report focuses on the threats to the American homeland posed by state actors, the use of proxies, terrorist and extremist attacks by foreign groups or individuals, and terrorist and extremist attacks by residents of the US using conventional weapons and weapons of mass destruction. Separate reports focus on the threat posed by direct attacks by foreign states using weapons like ballistic missiles, and the threat of information and economic warfare.

This focus is not intended to imply that the emerging threats to the American homeland can be neatly compartmented, or do not interact. The spectrum of threats foreign governments can pose includes all of these methods of attack. Well-organized foreign and domestic terrorist/extremist groups have the *potential* to pose a wide range of high explosive, chemical, biological, and information warfare threats. There are no rules that say foreign governments and foreign and domestic terrorist/extremist groups cannot cooperate or piggyback on each other's activities. In broad terms, however, the threats to the American homeland posed by state actors, the use of proxies, terrorist and extremist attacks by foreign groups or individuals, and terrorist and extremist attacks by residents of the US using conventional weapons and weapons of mass destruction require a different mix of responses. These responses can only be discussed in terms of practical alternatives if it is narrowed down to the point where each of the major relevant homeland defense options can be analyzed in depth.

As is the case with national missile defense, this report also deals with issues that are highly politicized. Preparing to deal with the spectrum of threats posed by foreign states and terrorists using weapons of mass destruction is currently fashionable and "politically correct." This has had major benefits in many ways. The President and high level officials have set forth clear policies for dealing with many aspects of the problem. The Congress has passed dramatic new legislation, and major changes are well underway to improve federal, state, and local preparation to deal with the threat. There is new money available to federal agencies at a time

when severe budget constraints exist on virtually every form of government spending.

Unfortunately, however, the very popularity of the issue of terrorism and weapons of mass destruction also means that there has been a rush to react to potential threats without developing a common definition of the combined threat posed by covert attacks by state actors, state use of proxies, terrorist and extremist attacks by foreign groups or individuals, and terrorist and extremist attacks by residents of the US. There is still insufficient definition of the different kinds of threat that different kinds of weapons of mass destruction pose and how these relate to threats using conventional explosives. In many cases, departments and agencies are defining the nature and intensity of the threat to meet their own internal needs and perceptions, or are acting on assumptions that imply a far better ability to predict the future than can possibly exist.

As yet, there is only limited coordination in many federal, state, and local efforts except at the organization chart level. Departments and agencies struggle for resources and influence, and there are good reasons for the resulting “feeding frenzy. Even if one ignores all federal funding for critical infrastructure protection, funding for counterterrorism has risen from \$8.3 billion in FY1998 to \$12.9 billion in FY2001, and funding for new efforts like dealing with the threat posed by weapons of mass destruction have risen from approximately \$645 million in FY1998 to \$1.6 billion in FY2001.

Under these conditions, old programs are being recast to suit new policy priorities and rhetoric, while agencies compete to create new programs and assume lead responsibility. In some ways, homeland defense has replaced the Strategic Defense Initiative as the “next best thing.” As the GAO and CBO have pointed out, the sharp rise in spending has not yet led to tight central management of the homeland defense effort, although there is a growing and steadily more effective effort to develop balanced and coordinated capabilities. There also has been little success in estimating the mid and long term budget implications of program growth and new responsibilities at the federal level, much less the state and local level. Many RDT&E efforts have been started without clear deployment and life cycle implementation plans, and there are few meaningful measures of effectiveness for federal spending.

The sharp limits on how much money and human resources can be allocated to this aspect of homeland defense will, however, soon force the US to be much more selective in choosing the programs it can continue to expand or sustain. Even today, the government needs to make every effort to coordinate its efforts and prioritize them. Regardless of partisan rhetoric, it is clear that US is not yet prepared to pay for its existing military forces and capabilities. Furthermore, there are other major transnational problems like drugs immigration, and cybercrime. There are many unrelated shortfalls in law enforcement and emergency response capabilities. For example, the US faces a major crisis in medical spending even without considering the impact of responding to chemical, nuclear, and biological attacks, and is sharply reducing the size of its emergency medical facilities and hospital intensive treatment capabilities.

It is only possible to ignore these realities at the start of a homeland defense program, at a time when planning is large threat driven and the cost of new activities is relatively limited. As long as current outlays are limited, it is all too easy to can find a credible potential threat, issue warnings, make a speech, issue an executive order, or pass a law. Any competent analyst, contractor, research firm, NGO or advisory group can find a new way to focus on potential threats and the potential merit of uncosted and poorly defined solutions. The end result is start far more activities than can be finished, fail to consider the future trade-offs that must be made to deploy effective capabilities, duplicate other efforts, or refashion existing programs under new labels.

- *Improvements in policy and strategy are no substitute for effective management programming, budgeting, and measures of the effectiveness. The practical challenge is to use more management information systems and PPB methods to tie the efforts of government together develop clear priorities, ensure that cost estimates are provided of bring programs to maturity and sustaining them, tightly manage where the money goes on an ongoing basis, ensure that the risk of countermeasures and cost to defeat is assessed on a continuing basis, find suitable measures of effectiveness, and make suitable iterative trade-offs. In fact, one recommendation of this report is that there be one central point in the federal government charged with developing a budget*

overview of current programs, an analysis of their future year costs and deployment costs, relevance to the threat, and measures of effectiveness.

Unless this transparency is ruthlessly forced upon the federal government – both in the executive branch and Congress -- no amount of organizational changes, committees, legislation, and directives will create the proper focus. The creation of lead agencies will be a bureaucratic farce, and state and local authorities will be confronted with conflicting demands, and will often have little impact on federal bureaucratic infighting.

Equally important, Congressional oversight and effective outside review and constructive criticism will be impossible. The constant misuse of security classification will create large areas of “black programs” that encourages departmental empire building and a lack of management. Programs with limited relevance will be recast as part of the homeland defense effort, and areas that really need funding will be ignored.

Effective Action Must Be Broad-Based and Sub-Optimize Efficiently

At the same time, there are limits to how much coordination is practical, and how much central direction can be applied. The federal government, individual agencies, and state and local governments will often have to sub-optimize changes to their current programs in those areas where they can do the most in the near term with the least money. While the Clinton Administration is seeking to create a cohesive federal program, and has made progress towards this end, there are no models, analytic methods, or simulations which can hope to integrate all of the elements of homeland defense into some master analysis or set of priorities based upon a common model.

The problem is not specialization and compartmentation per se. It is that it must be the result of central management and oversight, particularly given the severe limits on what any foreseeable combination of allied, federal, state, and local efforts can do. Cost constraints will be

tight, trade-offs will be made whether or not they are made openly and explicitly, and the result will be anything but leak-proof. Most important, central direction is needed to ensure that the capabilities the US creates evolve to respond to reality and not to established bureaucratic priorities.

It is also far from clear that threat and risk assessments can be used to create a set of scenarios that focus the defense effort, or which prioritize it around a select and well-defined group of scenarios. Once again, the problem is to determine the range of low probability events the US may have to react to, and what this means for deterrence, offense, defense, and response. While it is most likely that the US will have to react to a series of relatively low level events in the near term, the cumulative probability that the US may have to react to a few much more serious events over the mid to long term may well be equally high. As a result, threat and risk assessments must consider nuclear and highly lethal biological attacks.

Furthermore, there are deep conceptual problems. As has already been discussed in depth, the range of threats simply are not predictable enough for given agencies to attempt more than a constantly evolving and uncertain process of suboptimization. Put differently, departments and agencies must often do what they can to improve their capabilities at the margin, rather than seek to create building blocks in some kind of coherent homeland defense.

Such efforts may not, however, have great impact on US ability to defend against nuclear and highly lethal biological attacks. They may give the impression of defense and response capability, but the end result may not be able to cope with very high levels of attack, which may well force all levels of government to improvise radically with little warning and under intense pressure. Marginal improvements in resources may fail to deal with response requirements or be impossible to allocate efficiently within the time windows required. This is particularly true because there currently seems to be little practical understanding of what a “worst case” or high level attack would really do, and how uncertain its effects now are.

Finally, the present coordination effort often focuses either on “worst cases” or on those federal programs identified as being directly designed to defend or respond to the threat state

actors, their proxies, or independent extremists and terrorists pose to the American homeland. This is almost certainly *not* the right way to will prove to create the most effective overall program to actually improve Homeland defense. Such a program must explicitly consider the offensive, deterrent, and retaliatory capabilities of US military and intelligence agencies, and the role their activities overseas can play in creating an effective deterrent to foreign attacks on the US.

As a result, the US needs to rethink its approach to develop a program that constantly evolves, and which is based on the dilemma that it must try to manage chaos:

- *Effective homeland defense must be based on responding to the patterns of threats that actually emerge, and to shifts in the most likely contingency requirements.* It is virtually an iron law that any effort will fail that is based upon the current theories of what threats *may* emerge in a given area. Once again, a guiding principle is that there is a timeline of at least a quarter of a century of uncertain risk. No program or analysis made today can possibly be based on the correct priorities. The issue is rather how quickly and effectively programs can anticipate change and react to it.
- *The key to a successful result is that sub-optimization must be deliberate and subject to broad review, and not simply evolve by accident. Whatever the federal government does, it must involve an explicit and well-reasoned balance between:*
 - Offense and defense
 - Action overseas and in concert with our friends and allies, and measures actually taken in the US.
 - Counterproliferation and counterterrorism.
 - Defense and response.
 - Including threats in the spectrum of threats requiring special action by the federal

government as part of homeland defense, and the role played by conventional law enforcement.

Managing Research and Development, Rather Than Treating CBRN As A Wish List and Slush Fund

Research and development programs receive little detailed description and the description that is provided often concentrates on the threat being dealt with, and provides little program detail. No agency provides a meaningful description of its future program, future costs, milestones, or measures of effectiveness. Cooperation with state and local agencies is often ignored, and when it is not, it tends to be discussed in anecdotal terms

There is no evidence that any department or agency has provided a technology net assessment to examine whether its programs will provide defensive capabilities that outpace advances in offensive capability. There is virtually no discussion of the risk posed by countermeasures or the cost to defeat current and planned programs. There is no discussion of the outyear costs of research and development activity or of estimated deployment schedules, measures of effectiveness, and life cycle costs. Almost without exception, there is no way to be certain to degree to which given programs in given departments or agencies are actually focused on CBRN and other counterterrorism activities, or have simply recast ongoing or desired programs to compete for such funds.

- Federal research and development efforts have a poor to dismal record of effective management. It is time to reverse this situation.

Looking Beyond CBRN: Dealing with All Medical Risks and Costs

The previous analysis indicates that there is a need for a zero-based review of the current data on the lethality of biological weapons, and for a comprehensive net technical assessment of current and future trends in biological offense and defense. Biological warfare defense and response efforts cannot, however, be separated from the need for an effective national health

program.

Response measures against biological and nuclear attacks can require truly massive increases in public health efforts and emergency services at a time when the US already faces major problems in funding medical entitlement programs and growing cost constraints are being placed on investments in medical capabilities which normally have high utilization rates. The response capabilities required to deal with large biological and nuclear “incidents” may simply be unaffordable without far more evidence that such attacks are likely, and effective treatment may simply be impossible. One grim result is that “triage” may have to be performed in ways that deliberately leave a very high number of casualties to die.

The risk of attacks on the American homeland that have massive medical consequences requires that homeland defense measures deal with two major interrelated problems in public health policy and spending.

- *There is a significant amount of medical literature -- including a recent report by the National Intelligence Council -- that indicates that the US is under significant cumulative threat of the outbreak of some disease for which current medical treatment is not adequate.* In short, the US may face a serious threat from nature as well as from foreign attackers and domestic extremists.¹²⁶
- *US medical spending has already reached the point where it dominates much of the end use of the entitlements in the federal budget,, and where drastic efforts are being made to down-size medical spending.* These facts are largely ignored in much of the current discussion of Homeland defense, which focuses on threats and then on research and development measures that do not have a deployment cost, and which often involves response efforts so limited in estimated casualties that the list of equipment is “affordable” largely because it is assumed that the existing infrastructure can deal with the casualties and the medical impact is both treatable and involves non-infectious threats. These assumptions, however, are only valid as long as the most serious threats are defined away and the eventual need to pay for facilities

and a full spectrum of response measures is ignored.

Homeland Defense and/or Law Enforcement

The US also faces major problems in defining the point at which federal intervention in some form of homeland defense program is needed, as distinguish from a reliance on normal federal, state, and local law enforcement. Many of the definitions now used for terrorism can include virtually any threat of violence by an individual or small group with a political or ideological agenda, or who is willing to attack civilians. In practice, however, most such threats are dealt with as normal law enforcement activities unless some foreign element is involved. Even in those cases where foreigners are involved, many cases are dealt with through normal law enforcement means.

It does not make sense to change these arrangements without clear cause, and the previous statistics on terrorism in the United States need to be kept in perspective in allocating law enforcement resources. According to the FBI's uniform crime statistics, there were 10 cities in the US with populations of 100,000 or more that had more than 100 murders in the first six months of 1999, and three with over 200 murders. If rapes and assaults are counted, there were 47 cities in the US with populations of 100,000 or more that had more than 1,000 "casualties" in the first six months of 1999, and nine with over 3,000.¹²⁷

There is a reason that it now takes some 40,000 armed men and women to try to secure the greater New York metropolitan area alone. There is also a reason why law enforcement activity cannot be centered around counterterrorism or dealing with low probability covert attacks until there is a far clearer and more dangerous threat than now appears to exist. At the same time, it is inconceivable that the US could develop an effective approach to homeland defense that did attempt to make use of these resources at every level of law enforcement.

- *The task is to find the right trade-offs between reliance on normal law enforcement and specialized homeland defense activity, and between using existing resources with other primary missions and creating new dedicated homeland defense components.*

Rule of Law, Human Rights, Asymmetric Warfare, High Levels of Attack and “New Paradigms”

Homeland defense impacts heavily on legal and human rights issues. Until now, the threats to the US have been limited enough so that the US can afford to shape its response on the basis of strict observance of civil law and human rights. There is also ample emergency authority for the President, Governors, and local officials to use virtually all of the assets of government to deal with homeland defense emergencies if they arise. Even restrictions on the use of the military, such as like the Posse Comitatus Act (18 USC 1385), have so many exceptions that the problem is much more likely to be getting sufficient warning to act than any practical legal barrier to effective action.

Much of the present discussion of legal and human rights issues, however, ignores what would happen if the threat of the use of biological or nuclear weapons against the US homeland became more tangible and immediate. It also ignores the real world effects of state actors or terrorists/extremists carrying out highly lethal attacks. These effects include the problems in human rights created by the need to deal with mass triage in the face of saturated medical facilities and/or to contain a civil population with force in the event of an attack using a highly infectious agent.

Today, the US has the luxury of examining such options with attitudes shaped by the fact such attacks do not seem imminent and there are no real precedents for the kind of damage that may occur. There have been no successful attacks using weapons of mass destruction in the US, barring minor incidents, and only one partially successful major attack overseas – the Aum Shinrikyo attack in Japan. No nation or group has yet exploited the use of effective biological weapons, in spite of the fact that many nations have developed such weapons, and nuclear proliferation remains contained enough to limit the threat posed by regimes and nations that have demonstrated a high willingness to take risks as well as terrorist and extremist groups.

America’s enemies are developing a steadily more sophisticated understanding of asymmetric warfare and America’s vulnerabilities. If major unconventional attacks occur and

succeed anywhere in the world in the years to come, such attacks might well become a new norm for asymmetric warfare. America's enemies might then respond by rapidly developing such capabilities to attack the US, and such shifts could occur relatively quickly and with little strategic warning. With luck, such a world will never happen. Reliance on luck, however, is scarcely a reliable criterion for planning. It is quite clear, however, that the US and its allies may face a very different future/

- *US intelligence efforts and law enforcement must both reorganize to deal with the risk of a “paradigm” shift in the willingness and ability to use weapons of mass destruction in unconventional attacks on the US homeland, and be given the proper legislation and regulations.* Many states are now involved in a process of proliferation that will change their capabilities to carry out such attacks. Advances in manufacturing, petrochemicals, and the biological science are making it steadily easier for both states and non-state actors to build lethal chemical and biological weapons. The technology and components to develop every aspect of nuclear weapons other than weapons grade uranium and plutonium are becoming steadily more available.

¹ United States General Accounting Office, GAO Report to Congressional Requesters, “Combating Terrorism, Federal Agencies’ Efforts to Implement National Policy and Strategy,” GAO/NSIAD-97-254, September 1997, p. 15.

² GAO/T-NSIAD-98-164, “Combating Terrorism,” April 23, 1998, P. 3.

³ GAO/T-NSIAD-98-164, “Combating Terrorism,” April 23, 1998, P. 4.

⁴ National Intelligence Council, “The Global Infectious Disease Threat and Its Implications for the United States, CIA NIE-99-17D, January 2000. <http://www.cia.gov/cia/publications/nie/report/nie99-17d.htm>.

⁵ FBI, Uniform Crime Reports, January-June 1999, November 21, 1999. Table 4.

⁶ GAO/T-NSIAD-98-164, “Combating Terrorism,” April 23, 1998, P. 3.

⁷ United States General Accounting Office, “Combating Terrorism: Issues in Managing Counterterrorist Programs, GAO/T-NSIAD-00-145,” April 6, 2000, <http://www.gao.gov/new.items/ns00145t.pdf>

⁸ GAO/T-NSIAD-98-164, “Combating Terrorism,” April 23, 1998, P. 4.

⁹ United States General Accounting Office, “Combating Terrorism: Comments on Bill H.R. 4210 to Manage Selected Counterterrorist Programs,” GAO/T-NSIAD-00-172, May 4, 2000, <http://www.gao.gov/new.items/ns00172t.pdf>

¹⁰ Cragin, Charles, “Defense Leaders Commentary: The Facts on WMD Civil Support Teams,” March 31, 2000, http://www.defenselink.mil/news/Mar2000/n0331200_20003311.html

¹¹ GAO, , “Combating Terrorism,” **GAO/NSIAD-97-254**, Sept. 26, 1997

¹² GAO, , “Combating Terrorism,” GAO/T-NSIAD-98-164. April 23, 1998, P. 6.

¹³ GAO/T-NSIAD-00-145, p. 5.

¹⁴ Center for Nonproliferation Studies, Monterey Institute of International Studies, “Agency Structures for Terrorism Response,” 1999, <http://www.cns.miis.edu/research/cbw/response.htm>

¹⁵ White House, Office of the Press Secretary For Immediate Release, "Funding for Domestic Preparedness and Critical Infrastructure Protection," Fact Sheet, January 22, 1999.

¹⁶ Executive Office of the President, Office of Budget and Management, "Annual Report to Congress on Combating Terrorism," May 2000

¹⁷ United States General Accounting Office, "Combating Terrorism: Issues in Managing Counterterrorist Programs," GAO/T-NSIAD-00-145, April 6, 2000, <http://www.gao.gov/new.items/ns00145t.pdf>

¹⁸ White House, Office of the Press Secretary, "Announcement on Counterterrorism Funding Request," May 17, 2000, http://www.state.gov/www/global/terrorism/000517_pres_funding.html

¹⁹ GAO, "Combating Terrorism," GAO/T-NSIAD-98-164, April 23, 1998.

²⁰ See GAO, "Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination," [GAO/NSIAD-98-39](#), Dec. 1, 1997; and "Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments," [GAO/NSIAD-98-74](#), Apr. 9, 1998.

²¹ See Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (known as the Gilmore Panel because its chairman is James S. Gilmore, III) and Statement of Norman J. Rabkin, Director National Security Preparedness Issues, National Security and International Affairs Division. Before the Subcommittee on Oversight, Investigations, and Emergency Management, Committee on Transportation and Infrastructure, House of Representatives, United States General Accounting Office, GAO/T-NSIAD-00-145, April 6, 2000.

²² Executive Office of the President, 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

²³ Executive Office of the President, 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

²⁴ Executive Office of the President, 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

²⁵ Center for Nonproliferation Studies, Monterey Institute of International Studies, “Agency Structures for Terrorism Response,” 1999, <http://www.cns.miis.edu/research/cbw/response.htm>

²⁶ Executive Office of the President, 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

²⁷ United States General Accounting Office, “Weapons of Mass Destruction: DOD’s Actions to Combat Weapons Use Should Be More Integrated and Focused,” GAO/NSIAD-00-97, May 26, 2000, <http://www.gao.gov/new.items/ns00097.pdf>

²⁸ United States General Accounting Office, “Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training,” GAO/NSIAD-00-64, March 21, 2000, <http://www.gao.gov/new.items/ns00064.pdf>

²⁹ Executive Office of the President, 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

³⁰ United States General Accounting Office, “Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training,” GAO/NSIAD-00-64, March 21, 2000, <http://www.gao.gov/new.items/ns00064.pdf>

³¹ United States General Accounting Office, “Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training,” GAO/NSIAD-00-64, March 21, 2000, <http://www.gao.gov/new.items/ns00064.pdf>

³² United States General Accounting Office, “Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training,” GAO/NSIAD-00-64, March 21, 2000, <http://www.gao.gov/new.items/ns00064.pdf>

³³ United States General Accounting Office, “Future Years Defense Program: Comparison of Planned Funding Levels for the 2000 and 2001 Programs,” GAO/NSIAD-00-179, June 14, 2000, <http://www.gao.gov/new.items/ns00179.pdf>

³⁴ United States General Accounting Office, “Chemical and Biological Defense: Program Planning and Evaluation Should Follow Results Act Framework,” GAO/T-NSIAD-00-180, May 24, 2000, <http://www.gao.gov/new.items/ns00180t.pdf>

³⁵ United States General Accounting Office, “Chemical and Biological Defense: Program Planning and Evaluation Should Follow Results Act Framework,” GAO/T-NSIAD-00-180, May 24, 2000, <http://www.gao.gov/new.items/ns00180t.pdf>

³⁶ United States General Accounting Office, “Chemical and Biological Defense: Program Planning and Evaluation Should Follow Results Act Framework,” GAO/T-NSIAD-00-180, May 24, 2000, <http://www.gao.gov/new.items/ns00180t.pdf>

³⁷ United States General Accounting Office, “Chemical and Biological Defense: Program Planning and Evaluation Should Follow Results Act Framework,” GAO/T-NSIAD-00-180, May 24, 2000, <http://www.gao.gov/new.items/ns00180t.pdf>

³⁸ United States General Accounting Office, “Chemical and Biological Defense: Observations on Non-medical Chemical and Biological R&D Programs,” GAO/T-NSIAD-00-130, March 22, 2000, <http://www.gao.gov/new.items/ns00130t.pdf>

³⁹ Department of Defense Tiger Team, “Department of Defense Plan for Integrating National Guard and Reserve Component Support for Response to Attacks Using Weapons of Mass Destruction,” January, 1998, http://www.defenselink.mil/pubs/wmdresponse/chapter_5.html

⁴⁰ Cragin, Charles, “Defense Leaders Commentary: The Facts on WMD Civil Support Teams,” March 31, 2000, http://www.defenselink.mil/news/Mar2000/n0331200_20003311.html

⁴¹ Cragin, Charles, “Defense Leaders Commentary: The Facts on WMD Civil Support Teams,” March 31, 2000, http://www.defenselink.mil/news/Mar2000/n0331200_20003311.html

⁴² Executive Office of the President, 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

⁴³ Center for Nonproliferation Studies, Monterey Institute of International Studies, “Agency Structures for Terrorism Response,” 1999, <http://www.cns.miis.edu/research/cbw/response.htm>

⁴⁴ Executive Office of the President, 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

⁴⁵ Center for Nonproliferation Studies, Monterey Institute of International Studies, “Agency Structures for Terrorism Response,” 1999, <http://www.cns.miis.edu/research/cbw/response.htm>

⁴⁶ Executive Office of the President, 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

⁴⁷ Executive Office of the President, 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

⁴⁸ Executive Office of the President, 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

⁴⁹ Executive Office of the President, 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

⁵⁰ United States General Accounting Office, “Chemical and Biological Defense: Observations on Non-medical Chemical and Biological R&D Programs,” GAO/T-NSIAD-00-130, March 22, 2000, <http://www.gao.gov/new.items/ns00130t.pdf>

⁵¹ Executive Office of the President, 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

⁵² Center for Nonproliferation Studies, Monterey Institute of International Studies, “Agency Structures for Terrorism Response,” 1999, <http://www.cns.mii.edu/research/cbw/response.htm>

⁵³ Environmental Protection Agency, “EPA Capabilities: Responding to Nuclear-Biological-Chemical (NBC) Terrorism,” EPA 550-F-00-008, May 2000, <http://www.epa.gov/ceppo/pubs/brochurejune2000.pdf>

⁵⁴ Environmental Protection Agency, “EPA Capabilities: Responding to Nuclear-Biological-Chemical (NBC) Terrorism,” EPA 550-F-00-008, May 2000, <http://www.epa.gov/ceppo/pubs/brochurejune2000.pdf>

⁵⁵ Executive Office of the President, 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

⁵⁶ Environmental Protection Agency, “EPA Capabilities: Responding to Nuclear-Biological-Chemical (NBC) Terrorism,” EPA 550-F-00-008, May 2000, <http://www.epa.gov/ceppo/pubs/brochurejune2000.pdf>

⁵⁷ Executive Office of the President, 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

⁵⁸ Executive Office of the President, 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

⁵⁹ United States General Accounting Office, “Combating Terrorism: Issues in Managing Counterterrorist Programs, GAO/T-NSIAD-00-145,” April 6, 2000, <http://www.gao.gov/new.items/ns00145t.pdf>

⁶⁰ Federal Emergency Management Agency, “Federal Response Plan, Notice of Change,” February 7, 1997, FEMA 229, Chg 11, http://www.fas.org/irp/offdocs/pdd39_frp.htm

⁶¹ Executive Office of the President, 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

⁶² Center for Nonproliferation Studies, Monterey Institute of International Studies, “Agency Structures for Terrorism Response,” 1999, <http://www.cns.miis.edu/research/cbw/response.htm>

⁶³ United States General Accounting Office, “Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training,” GAO/NSIAD-00-64, March 21, 2000, <http://www.gao.gov/new.items/ns00064.pdf>

⁶⁴ United States General Accounting Office, “Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training,” GAO/NSIAD-00-64, March 21, 2000, <http://www.gao.gov/new.items/ns00064.pdf>

⁶⁵ United States General Accounting Office, “Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training,” GAO/NSIAD-00-64, March 21, 2000, <http://www.gao.gov/new.items/ns00064.pdf>

⁶⁶ Executive Office of the President, 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

⁶⁷ Executive Office of the President, 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

⁶⁸ Executive Office of the President, 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

⁶⁹ United States General Accounting Office, “Combating Terrorism: Observations on Growth in Federal Programs,” GAO/T-NSIAD-99-181, June 9, 1999, <http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ns99181.pdf&directory=/diskb/wais/data/gao>

⁷⁰ Executive Office of the President, 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

⁷¹ Department of Health and Human Services, “Medical Response in Emergencies: HHS Role,” May 18, 2000, <http://www.hhs.gov/news/press/2000pres/20000518a.html>

⁷² Executive Office of the President, 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

⁷³ United States General Accounting Office, Combating Terrorism: Observations on Growth in Federal Programs, GAO/T-NSIAD-99-181, June 9, 1999, <http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ns99181.pdf&directory=/diskb/wais/data/gao>

⁷⁴ United States General Accounting Office, “Combating Terrorism: Issues in Managing Counterterrorist Programs, GAO/T-NSIAD-00-145,” April 6, 2000, <http://www.gao.gov/new.items/ns00145t.pdf>

⁷⁵ Executive Office of the President, 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

⁷⁶ Executive Office of the President, 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

⁷⁷ Executive Office of the President, 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

⁷⁸ Executive Office of the President, 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

⁷⁹ United States General Accounting Office, “Combating Terrorism: Issues in Managing Counterterrorist Programs, GAO/T-NSIAD-00-145,” April 6, 2000, <http://www.gao.gov/new.items/ns00145t.pdf>

⁸⁰ Executive Office of the President, 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

⁸¹ United States General Accounting Office, “Combating Terrorism: Observations on Growth in Federal Programs,” GAO/T-NSIAD-99-181, June 9, 1999, <http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ns99181.pdf&directory=/diskb/wais/data/gao>

⁸² National Domestic Preparedness Office, “Blueprint for the National Domestic Preparedness Office,” <http://www.ndpo.gov/blueprint.pdf>

⁸³ National Domestic Preparedness Organization website, <http://www.ndpo.gov/responders.htm>

⁸⁴ United States General Accounting Office, “Combating Terrorism: Issues in Managing Counterterrorist Programs,” GAO/T-NSIAD-00-145, April 6, 2000, <http://www.gao.gov/new.items/ns00145t.pdf>

⁸⁵ Department of Justice, Office of Justice Program, Office for State and Local Domestic Preparedness Support website, <http://www.ojp.usdoj.gov/osldps/>

⁸⁶ The Office of Justice Program's (OJP) Office for State and Local Domestic Preparedness Support (OSLDPS) FY 1999 State Domestic Preparedness Equipment Program Application <http://www.ojp.usdoj.gov/osldps/docs/FY99StatePrepEQUIPMENTAppKit.doc>

⁸⁷ Executive Office of the President, 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

⁸⁸ The Office of Justice Program's (OJP) Office for State and Local Domestic Preparedness Support (OSLDPS) FY 1999 State Domestic Preparedness Equipment Program Application <http://www.ojp.usdoj.gov/osldps/docs/FY99StatePrepEQUIPMENTAppKit.doc>

⁸⁹ United States General Accounting Office, “Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training,” GAO/NSIAD-00-64, March 21, 2000, <http://www.gao.gov/new.items/ns00064.pdf>

⁹⁰ United States General Accounting Office, “Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training,” GAO/NSIAD-00-64, March 21, 2000, <http://www.gao.gov/new.items/ns00064.pdf>

⁹¹ United States General Accounting Office, “Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training,” GAO/NSIAD-00-64, March 21, 2000, <http://www.gao.gov/new.items/ns00064.pdf>

⁹² The Office of Justice Program's (OJP) Office for State and Local Domestic Preparedness Support (OSLDPS) Technical Assistance Website, <http://www.ojp.usdoj.gov/osldps/ta.htm>

⁹³ The Office of Justice Program's (OJP) Office for State and Local Domestic Preparedness Support (OSLDPS) State Domestic Preparedness Equipment Program Needs Assessment and Strategy Development Initiative Website, <http://www.ojp.usdoj.gov/osldps/assessments.htm>

⁹⁴ The Office of Justice Program's (OJP) Office for State and Local Domestic Preparedness Support (OSLDPS) Exercises Website, <http://www.ojp.usdoj.gov/osldps/exercises.htm>

⁹⁵ National Commission on Terrorism, “Countering the Changing Threat of International Terrorism,” June, 2000

⁹⁶ Executive Office of the President, 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

⁹⁷ United States General Accounting Office, “Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training,” GAO/NSIAD-00-64, March 21, 2000, <http://www.gao.gov/new.items/ns00064.pdf>

⁹⁸ Federal Bureau of Investigation, ANSIR website, <http://www.fbi.gov/programs/ansir/ansir.htm>

⁹⁹ Executive Office of the President, 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

¹⁰⁰ Executive Office of the President, 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

¹⁰¹ United States General Accounting Office, “Combating Terrorism: Observations on Growth in Federal Programs,” GAO/T-NSIAD-99-181, June 9, 1999, <http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ns99181.pdf&directory=/diskb/wais/data/gao>

¹⁰² Executive Office of the President, 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

¹⁰³ Executive Office of the President, 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

¹⁰⁴ Executive Office of the President, 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

¹⁰⁵ Executive Office of the President, 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

¹⁰⁶ Executive Office of the President, 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

¹⁰⁷ Executive Office of the President, 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

¹⁰⁸ White House, Office of the Press Secretary, “Embassy Security Funding Fact Sheet,” February 10, 2000, http://www.state.gov/www/global/terrorism/fs_000210_embsy.html

¹⁰⁹ White House, Office of the Press Secretary, “Embassy Security Funding Fact Sheet,” February 10, 2000, http://www.state.gov/www/global/terrorism/fs_000210_embsy.html

¹¹⁰ U.S. Department of State, Office of the Spokesman, “U.S. Counterterrorism Efforts Fact Sheet,” August 4, 1999, http://www.state.gov/www/regions/africa/fs_anniv_cterrorism.html

¹¹¹ Executive Office of the President, 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

¹¹² Executive Office of the President, 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

¹¹³ Executive Office of the President, 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

¹¹⁴ Executive Office of the President, 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

¹¹⁵ Executive Office of the President, 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

¹¹⁶ Executive Office of the President, 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

¹¹⁷ Executive Office of the President, 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

¹¹⁸ United States General Accounting Office, “West Nile Virus: Preliminary Information on Lessons Learned,” GAO/HEHS-00-142R, June 23, 2000, <http://www.senate.gov/~schumer/GAO.WESTNILEVIRUS.pdf>

¹¹⁹ United States General Accounting Office, “West Nile Virus: Preliminary Information on Lessons Learned,” GAO/HEHS-00-142R, June 23, 2000, <http://www.senate.gov/~schumer/GAO.WESTNILEVIRUS.pdf>

¹²⁰ GAO, “United States General Accounting Office Report to Congressional Requesters,” Combating Terrorism, How Five Foreign Countries Are Organized to Combat Terrorism,” B-284585, GAO/NSIAD-00-85, April 2000.

¹²¹ GAO, “United States General Accounting Office Report to Congressional Requesters,” Combating Terrorism, How Five Foreign Countries Are Organized to Combat Terrorism,” B-284585, GAO/NSIAD-00-85, April 2000.

¹²² GAO, “United States General Accounting Office Report to Congressional Requesters,” Combating Terrorism, How Five Foreign Countries Are Organized to Combat Terrorism,” B-284585, GAO/NSIAD-00-85, April 2000.

¹²³ GAO, “United States General Accounting Office Report to Congressional Requesters,” Combating Terrorism, How Five Foreign Countries Are Organized to Combat Terrorism,” B-284585, GAO/NSIAD-00-85, April 2000.

¹²⁴ GAO, “United States General Accounting Office Report to Congressional Requesters,” Combating Terrorism, How Five Foreign Countries Are Organized to Combat Terrorism,” B-284585, GAO/NSIAD-00-85, April 2000.

¹²⁵ GAO, “United States General Accounting Office Report to Congressional Requesters,” Combating Terrorism, How Five Foreign Countries Are Organized to Combat Terrorism,” B-284585, GAO/NSIAD-00-85, April 2000.

¹²⁶ National Intelligence Council, “The Global Infectious Disease Threat and Its Implications for the United States, CIA NIE-99-17D, January 2000. <http://www.cia.gov/cia/publications/nie/report/nie99-17d.htm>.

¹²⁷ FBI, Uniform Crime Reports, January-June 1999, November 21, 1999. Table 4.