CSIS

Center for Strategic and International Studies
1800 K Street N.W.
Washington, DC 20006
(202) 775-3270
To contact: Acordesman@aol.com
Updates: CSIS.ORG

DEFENDING AMERICA
REDEFINING THE CONCEPTUAL BORDERS OF HOMELAND DEFENSE

US GOVERNMENT EFFORTS TO CREATE A HOMELAND DEFENSE CAPABILITY: PROGRAM BUDGET AND OVERVIEW

OVERVIEW OF FEDERAL SPENDING ON NATIONAL MISSILE DEFENSE, DEFENSE AGAINST ASYMMETRIC AND TERRORIST ATTACKS, AND ATTACKS ON INFORMATION SYSTEMS AND CRITICAL INFRASTRUCTURE

Anthony H. Cordesman
Arleigh A. Burke Chair in Strategy

REVISION: DECEMBER 12, 2000

Introduction

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 based on studies by the Office of Management and the Budget and Ballistic Missile Defense Organization.

It reflects the views of the author and not of the CSIS team working on the project.

Table of Contents

Introduction

There is no way to provide an adequate picture of the money the US now spends on Homeland defense. The data on ballistic missile defense are decoupled from the data on dealing with asymmetric threats and CBRN terrorism, and Critical Infrastructure Protection. There is no way to break out many efforts that contribute to Homeland defense but which do not involve dedicated programs. These involve arms control, strategic offensive forces and deterrent and retaliatory capabilities, foreign and theater deterrent and retaliatory capabilities, and emergency response and civil medical expenditures, the relevant activities of the Us Coast Guard, and many aspects of law enforcement activity, including those of the Customs Service and Immigration. The data on Critical Infrastructure Protection expenditures only deal with defense and not with information warfare capabilities and the offensive capabilities that might be used for defense and response.

The data that the Department of Defense provides on the cost of the counterterrorism program can only be loosely correlated with the data OMB provides on the same activities. At the same time, data are generally lacking on future year plans and program budgets, and most Departments and Agencies do not seem to generate such plans. There are many grave problems in the way the US government is managing its spending efforts, and no coordinated program and budget plan seems to exist for Homeland defense.

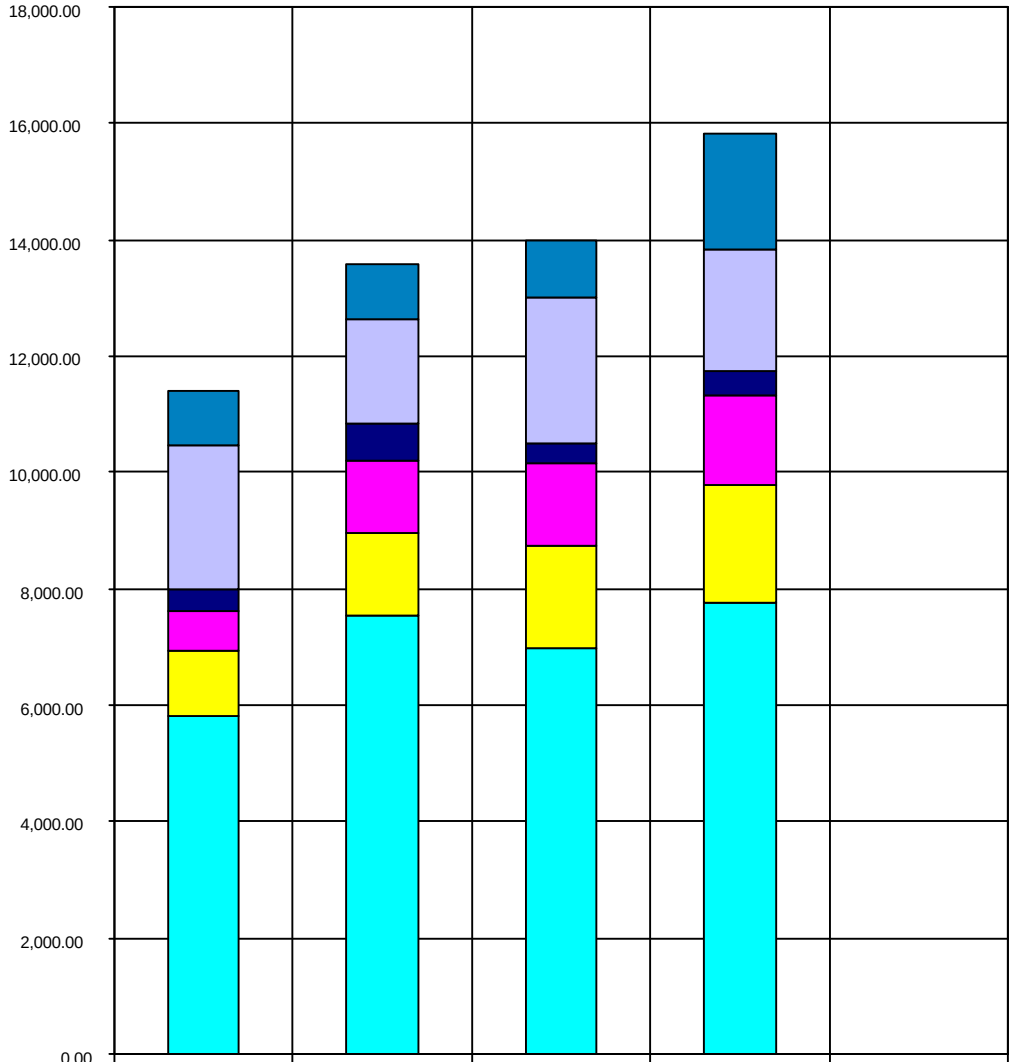
I. Total Cost of NMD, Counterterrorism, and Critical Infrastructure Protection

Figures 1.1 to 1.7 combine reporting by OMB on the cost of counterterrorism and critical infrastructure programs with Department of Defense estimates of spending on ballistic missile defense to provide a rough picture of US expenditures dedicated to Homeland defense, As is clear from the detailed studies of major areas of activity that follow, however, such data are limited, gravely flawed, and sometimes contradict the data provided in other sources.

Figure 1.1

Total Federal Spending on NMD, Terrorism, WMD, and CIP: FY1998-FY2001

(Current $US Millions)

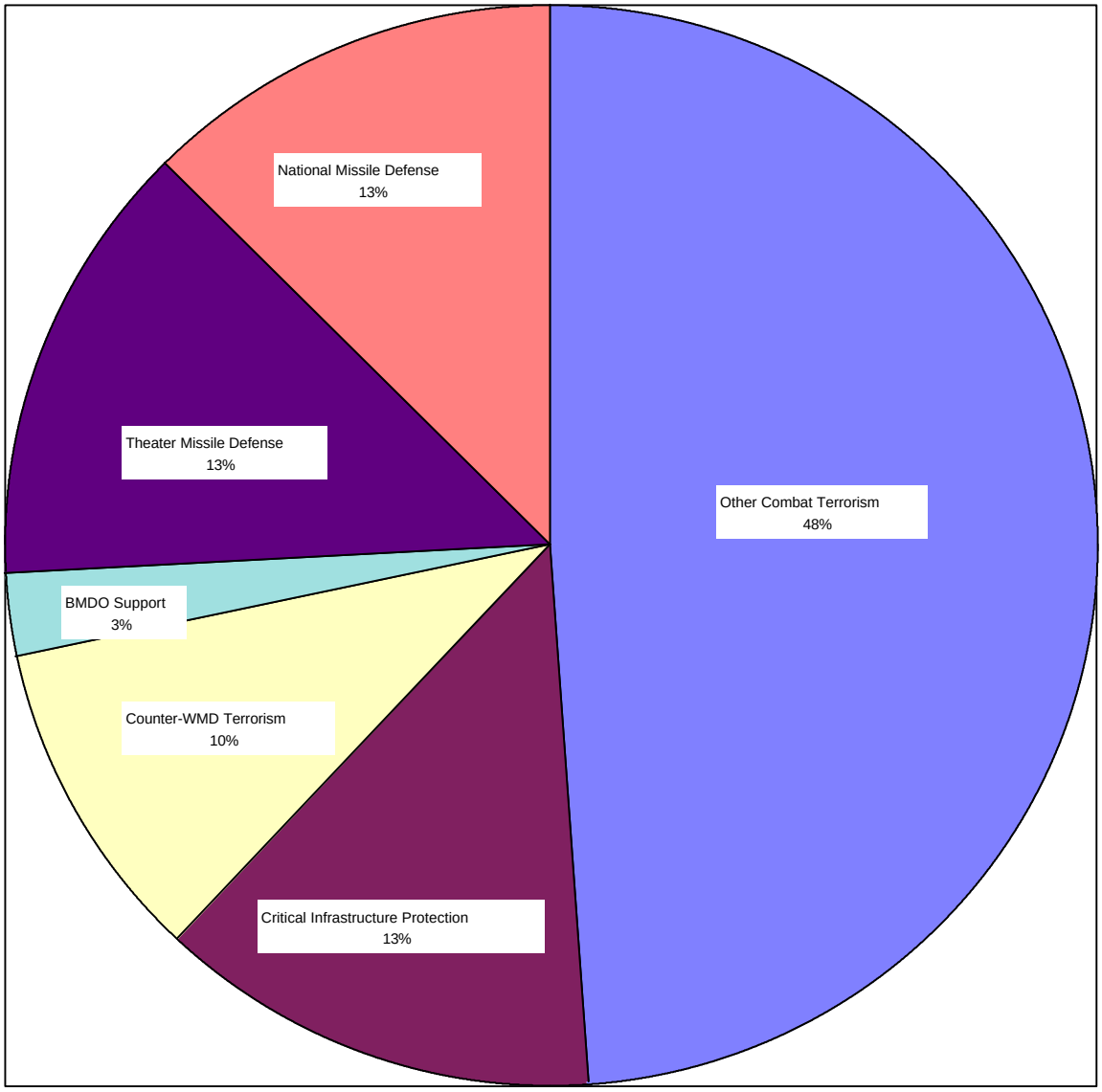


	FY1998	FY1999	FY2000	FY2001	
National Missile Defense	936	946	965.25	1,990.90	
Theater Missile Defense	2456	1816	2524.06	2082.72	
BMDO Support	408	637	316.72	417.03	
Counter-WMD Terrorism	645.32	1,238.44	1,453.74	1,554.96	
Critical Infrastructure Protection	1142	1428.57	1759.42	2027.25	
Other Combat Terrorism	5,810.74	7518.81	6965.98	7756.33	

Source: Adapted by Anthony H. Cordesman

Figure 1.2

Distribution of Federal Spending on NMD, Terrorism, WMD, and CIP by Activity: FY1998-FY2001
(Current $US Millions)

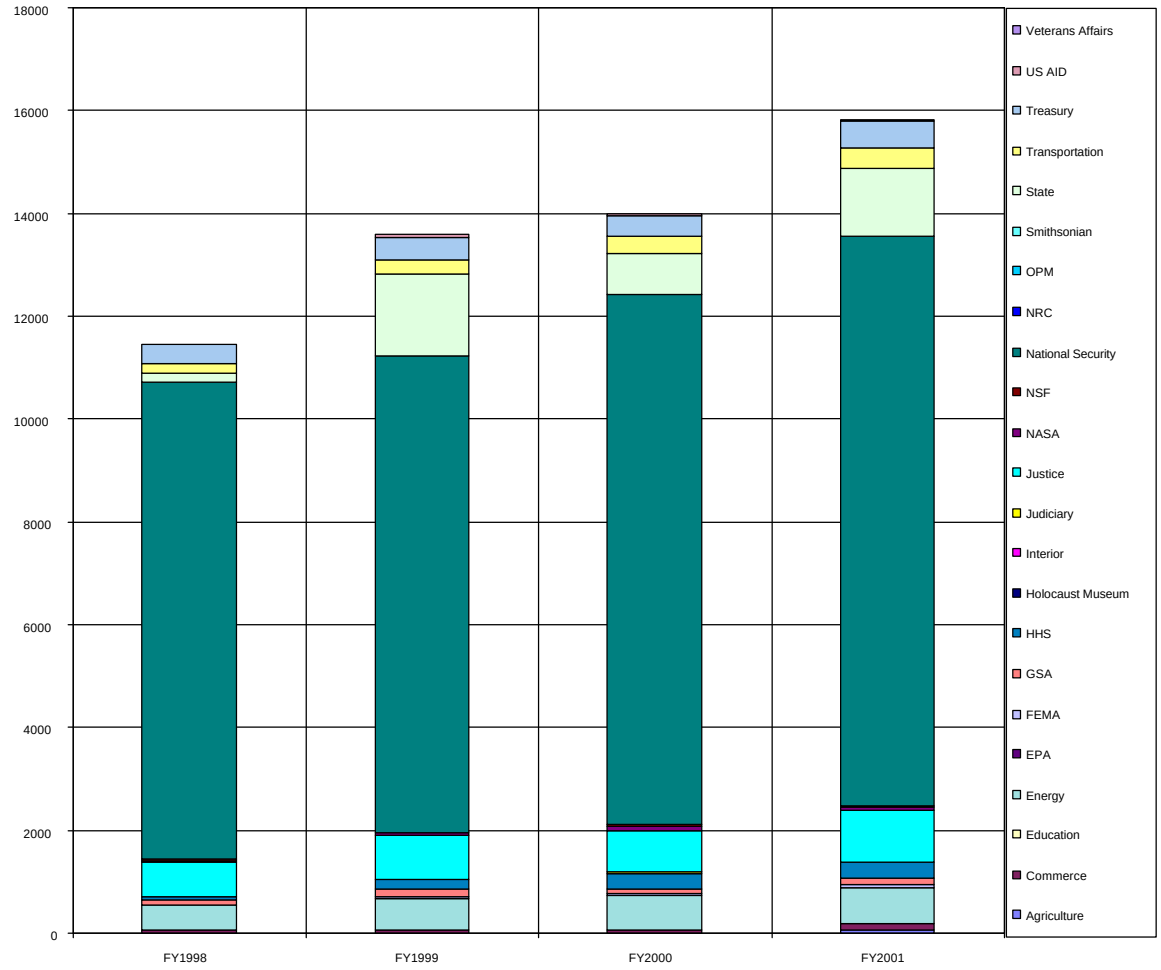


Source: Adapted by Anthony H. Cordesman

Figure 1.3

Federal Spending on NMD, Terrorism, WMD, and CIP by Agency: FY1998-FY2001 – Part One

(Current $US Millions)



Source: Adapted by Anthony H. Cordesman

Figure 1.4

Federal Spending on NMD, Terrorism, WMD, and CIP by Agency: FY1998-FY2001 – Part One

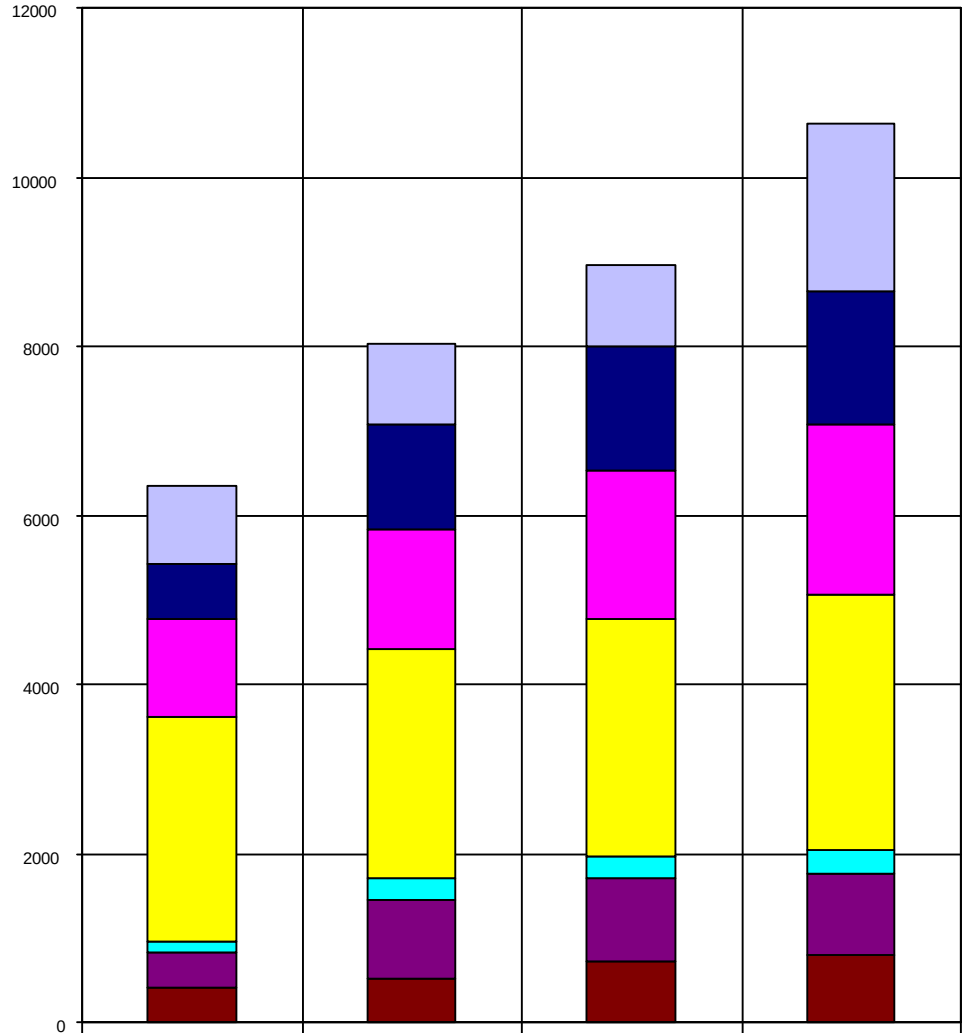
(Current $US Millions)

	FY1998	FY1999	FY2000	FY2001
Agriculture	10.9	12.92	14.84	59.17
Commerce	38.89	53.66	40.15	125.7
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	5.5
FEMA	5.92	17.61	31.57	35.99
GSA	89.60	136.50	92.80	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	9270.68	9266.73	10326.14	11,073.62
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	416.9	424.21	527.24
US AID	5.68	54.89	5.83	5.01
Veterans Affairs	0.01	0.04	17.33	17.39

Figure 1.5

Core Federal Spending on NMD, Terrorism, WMD, and CIP by Activity: FY1998-FY2001

(Current $US Millions)

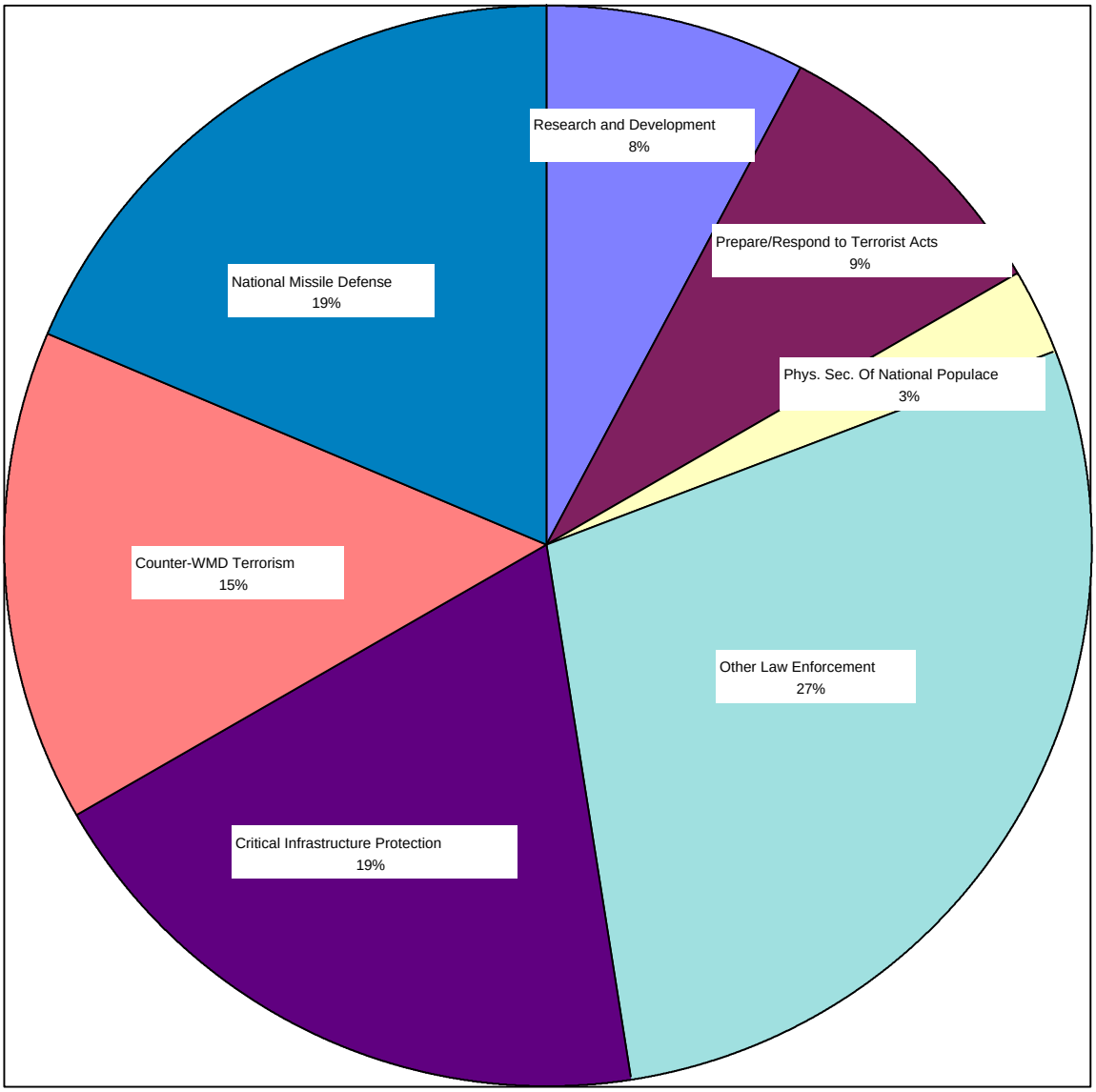


	FY1998	FY1999	FY2000	FY2001
National Missile Defense	936	946	965.25	1,990.90
Counter-WMD Terrorism	645.32	1,238.44	1,453.74	1,554.96
Critical Infrastructure Protection	1142	1428.57	1759.42	2027.25
Other Law Enforcement	2654.72	2686.777	2,820.44	3,025.51
Phys. Sec. Of National Populace	146.66	256.83	248.86	266.76
Prepare/Respond to Terrorist Acts	417.84	930.21	984.41	947
Research and Development	403.14	527.01	727.91	812.79

Source: Adapted by Anthony H. Cordesman

Figure 1.6

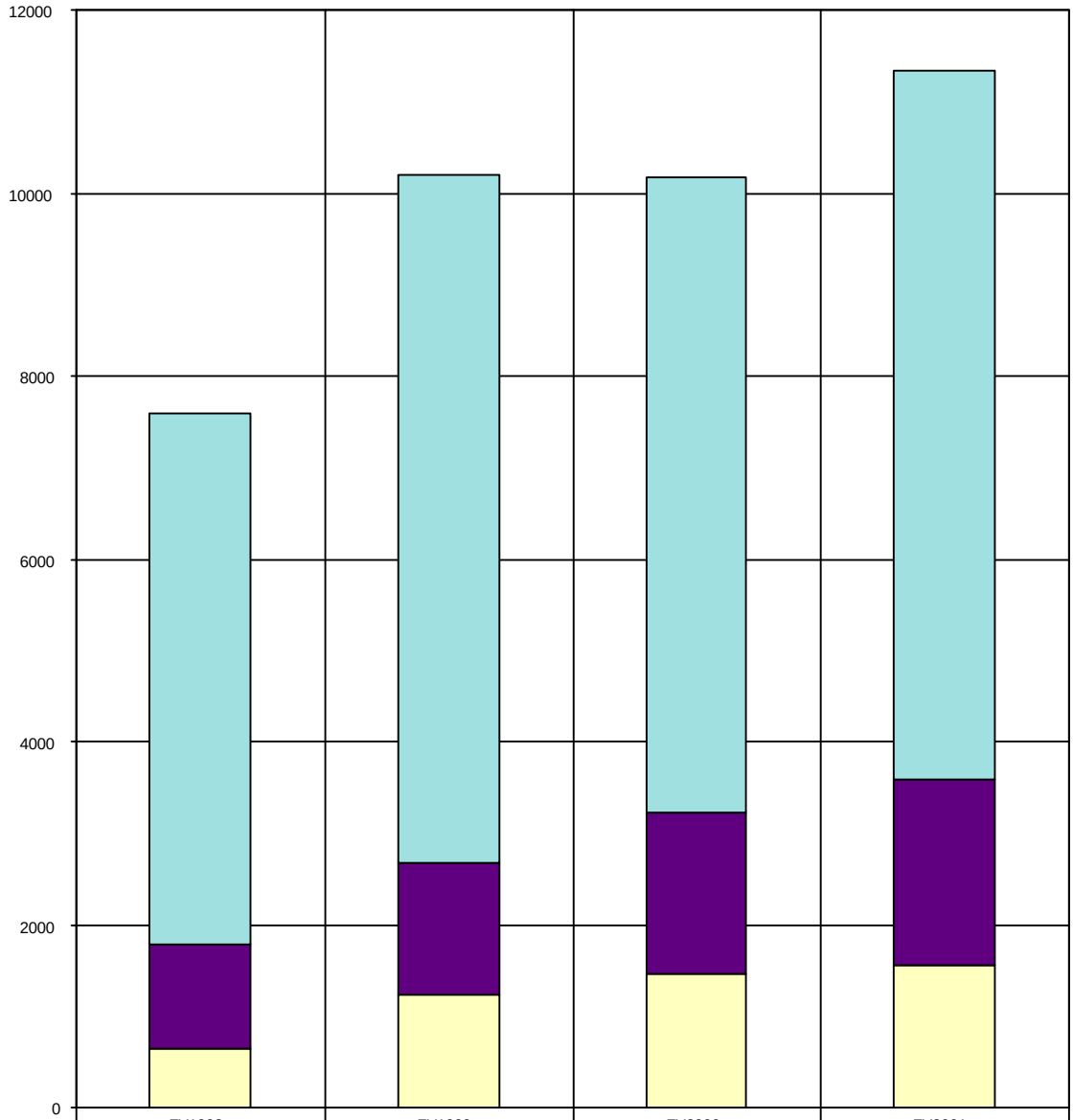
Distribution of Core Federal Spending on NMD, Terrorism, WMD, and CIP by Activity: FY2001
(Current $US Millions)



Source: Adapted by Anthony H. Cordesman

Figure 1.7

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



	FY1998	FY1999	FY2000	FY2001
Other Terrorism	5,810.74	7518.81	6965.98	7756.33
CIP	1142	1428.57	1759.42	2027.25
WMD	645.32	1,238.44	1,453.74	1,554.96

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

in every category.

II. Past, Current, and Projected Spending on National Missile and Ballistic Missile Defense

Cost estimates of NMD differ radically from those for counterterrorism and CIP in that there is a long history of clearly costable efforts by a single Department. The current US program is the result of 17 years of effort to shape a political consensus around the program the US should fund, deploy, and sustain. This effort has had five major phases, which have been summarized in Table 2.1.[1]

During this time the NMD program has evolved from the goal of providing a comprehensive shield against the largest scale of missile attacks on the American homeland to the far more limited defense described earlier. In the process, it has evolved from one oriented towards the Cold War threat by using extremely advanced space-based missile weapons to a one oriented towards defending against “rogue states” using land-based interceptors similar in concept to the defenses the US examined in the era before the ABM Treaty.

Equally important, the overall US investment in the ballistic missile defense program has evolved from one focused on the defense of US territory to one that invests more in theater missile defense than national missile defense. NMD is now only part of a far more comprehensive effort to develop a family of missile defenses.

The SDIO Era

The first phase of the US program took place during 1987-1989, and involved total Department of Defense expenditures of roughly $21.2 billion. It grew out of President Reagan’s original “star wars” speech in 1983 – a speech that led to the creation of the Strategic Defense Initiative Organization (SDIO) within the Department of Defense in April 1984. The new SDIO was devoted to developing the technologies needed to create a comprehensive land and space-based strategic defense against inter-continental ballistic missiles (ICBM's) and similar submarine-launched ballistic missiles. Its budget was structured to respond to “existing and

emerging threats from missile warfare towards the United States, and its forward deployed forces, allies, and friends around the world." In practice, however, its primary orientation was to defend against the Cold War threat from the Soviet Union. [2]

From the start, the program exposed deep divisions over the technical feasibility of such a program, its impact on the arms race, and its impact on arms control. There were those who argued that such a program could be deployed in the near-term and those who argued that the technology involved could never be cost-effective and would be relatively easy to defeat. There were also those who argued for a nearly leak-proof shield over the American homeland -- although the official rationale for the program evolved into one whose mission was described in much more modest terms and as to "enhance deterrence of a Soviet first strike," although this still meant the future deployment of 1000's of space-based interceptors. The Department of Defense history of the program states that, "At the inception of SDIO, the vision of BMD embraced by President Ronald Reagan of eliminating the threat of nuclear attack by use of space-and ground-based interceptors needed tremendous amounts of research to become a reality."

As a result, SDIO devoted virtually all of it initial efforts and budget resources to developing the technologies necessary to deploy a comprehensive ballistic missile defense system. This effort focuses on three main technology programs: Surveillance, Acquisition, Tracking, and Kill Assessment (SATKA), Directed Energy Weapons Technology (DEW), and Kinetic Energy Weapons Technology (KEW). The SATKA programs pursued signal processing, ground and space-based sensors and surveillance systems, and microwave radar technology. The DEW programs included various laser programs and neutral particle beam technology. The KEW programs included Brilliant Pebbles, Space-based Interceptor, and interceptor integration technology. Systems Analysis/Battle Management (SA/BM) programs were concerned with systems engineering,

While SDIO examined a wide range of possible deployment concepts, it was not concerned with the actual procurement and deployment of weapons, and the programs

summarized in Table III.8 were devoted to developing the technologies necessary for missile defense.

Table 2.1

The Cost of the First Phase of the National Missile Defense Program: 1985-1991

(In millions of then year $US dollars

Program	1985	1986	1987	1988	1989	1990	1991
SATKA	546	844	926	936	1083	1238	719
DEW	378	796	853	935	869	695	351
KEW	256	596	723	771	752	785	996
SA/BM	100	212	385	461	486	525	504
SLKT	108	214	375	430	414	328	292
Mgmt HQ	9	14	18	20	23	--	--
TMDI	--	-	-	-	-	-	226

Source: “Ballistic Missile Defense Organization Budgetary History,” Ballistic Missile Defense Office, BMDO Fact Sheet PO-99-02, April 1999.

The second major phase of the NMD effort took place during 1989-1992, during the end of the Cold War. The focus of the US ballistic missile defense program changed from comprehensive defense to Global Protection Against Limited Strikes (GPALS). In 1991. This change led to a restructuring of the SDIO budget to reflect the new priorities. The US creased to focus on blunting a massive ICBM attack by the Soviet Union. Instead, it focused on defending against a limited missile strike launched by a rogue state or non-state actor. This meant that the efforts of SDIO toward TMD could be increased, although attention was maintained towards NMD Space Based Interceptors included funding for systems development of Brilliant Pebbles. Other Follow-on Systems included directed energy weapons such as the Chemical Laser.[3]

This phase of the US NMD effort cost roughly $7.64 billion, and the cost of each major program activity is shown in Table 2.2 below. It is important to note that the basic program goal

of Phase II was essentially the same goal the US is now pursuing with its current NMD architecture, although Phase II still involved significant research into space-based weapons, and now included a major dimension for theater defense.

Table 2.2

The Cost of the Second Phase of the National Missile Defense Program: 1992-1993

(In millions of then year $US dollars)

Program	1992	1993
Limited Defense System	1482	1675
Space Based Interceptors	434	211
Other Follow-on Systems	528	300
Research & Support	666	418
Theater Missile Defense	797	1028
Procurement	25	75
Total	3,932	3,707

Source: “Ballistic Missile Defense Organization Budgetary History,” Ballistic Missile Defense Office, BMDO Fact Sheet PO-99-02, April 1999.

The Impact of BMDO

The third phase of the NMD program, or “technology readiness” phase, took place during 1993-1995, and its goal was to reduce the deployment time for a ground based system. The scope of the NMD effort was further narrowed, and more emphasis was placed on theater missile defense which led to another reorganization of the management of the US missile defense effort in 1993. As a result, SDIO became the Ballistic Missile Defense Office (BMDO).

This reorganization led to a further major restructuring of the program. The missile defense effort now had three major areas of activity and objectives. The first was theater missile defense and supporting the deployment of a robust TMD capability as soon as possible, This

effort has addressed the widely dispersed theater ballistic missile threats with ranges under 1,200-kilometers that already existed, and involved development and flight testing of THAAD, PAC-3, and Navy systems. The second phase was national missile defense and to position the United States to be ready to defend against a limited ballistic missile threat. The third was Advanced Technology effort which supports both TMD and NMD in an effort to continue to advance US capabilities to counter future and possibly more complex threats. During this phase, the work in all three areas of program activity focused on research and development. This activity had a total cost of roughly $9.2 billion during 1993-1995. It also shifted resources from an NMD dominated program to one where about 70% of the costs went to theater missile defense.

In April 1996, the Department of Defense changed the purpose of the NMD program from a technology readiness program to a deployment readiness program and designated NMD as a major defense acquisition program and sought matured technologies for possible use in a NMD system. This fourth "deployment readiness" phase lasted during 1996-1999, and had a total cost of roughly $14.2 billion. It continued to put the bulk of its resources into theater missile defense, but focused on the NMD as a Major Defense Acquisition Program and Deployment Readiness Program. This program, also called "3+3," sought to develop a NMD system capable of being deployed within three years after a deployment decision at a Deployment Readiness Review (DRR) in 2000. The initial goal of the NMD 3+3 program was to develop and demonstrate, by fiscal year 2000, an initial, limited capability that could be deployed by fiscal year 2003. The DRR criteria were stated to be the existence of the necessary threat and technological capability to proceed.

When the NMD program was changed to a deployment readiness program in April 1996, plans and requirements were not sufficiently defined to allow the development of a reliable cost estimate. The Fiscal year 1996 and 1997 budget requests were submitted to Congress before the program was changed to a deployment readiness program. In late 1995 and early 1996, DOD conducted a "Program Update Review" to determine how to proceed with the NMD program.

The review considered a number of options for NMD. The option selected included an integrated test in fiscal year 1999 and a possible deployment decision in fiscal year 2000. DOD estimated that research, development, and test and evaluation costs for this option would total about $2.3 billion for fiscal years 1998 through 2003. According to program office officials, this update review was based on a "rough order of magnitude" cost estimate derived from engineering judgment and field estimates. Detailed system requirements had not been established from which to make a formal, documented cost estimate.

Once NMD became a deployment readiness program in 1996, the focus changed from technology and component development to development and testing of a system that could be quickly deployed. One of the first steps was to define operational requirements for the system. U.S. Space Command defined broad requirements for an NMD system in August 1996. This was followed by NMD's first system requirements review held in November 1996.

Once these requirements were known, they had to be defined in sufficient detail so that the contribution of each system component to the requirement could be determined. According to DOD officials, it was only after these detailed requirements were established that detailed cost estimates could be produced. The NMD program office used the requirements data to prepare a new, more rigorous cost estimate. DOD's Office of Program Analysis and Evaluation also prepared an independent cost assessment. These estimates were not completed in time to affect the fiscal year 1998 President's budget request.

The program office estimated that about $4.6 billion would be required for research, development, test and evaluation—about $2.3 billion higher than previous projections. The independent assessment confirmed the program office's projection of research, development, test and evaluation costs. As a result of these estimates, it was apparent to DOD officials that the NMD program was significantly under funded. According to DOD officials, these were the first disciplined, system-level cost estimates based on requirements necessary to field an NMD system.[4]

The Quadrennial Defense Review, which was underway at the time the estimates were prepared, examined three options for the NMD program:[5]

- The first option was to keep NMD within its current budget, which would mean that system deployment would be delayed by at least 3 years or that the program would once again become a technology readiness program.
- The second option was to increase program funding to the levels indicated by the new estimates—an increase of about $2 billion in fiscal years 1998 through 2003--in order to maintain the 3+3 program schedule. Even with the additional funding, however, schedule risks were predicted to remain high.
- The third option was to increase program funding by up to $1.5 billion but also extending the schedule by about 3 years.

The review recommended the second option—increased funding to maintain the option to make a deployment decision in 2000. The Secretary of Defense asked Congress to increase the fiscal year 1998 budget request for NMD by $474 million. Congress appropriated the requested additional funds. DOD estimated that an additional $1.8 billion would be needed for fiscal years 1999 through 2003, bringing the total increase to about $2.3 billion. The amount of increased funding was based on the Office of Program Analysis and Evaluation's independent cost assessment.

As a result, BMDO shifted the initial deployment of NMD to 2005 rather than 2003 in order to reduce program risks. The GAO provides the following summary of these reasons for these decisions:[6]

> DOD significantly increased its NMD funding requirements in May 1997 because more rigorous cost estimates, based on more detailed program requirements and plans, showed that the program could not be accomplished within previously projected funding levels…the 3+3 NMD program was not sufficiently defined for detailed cost estimating when it initially changed from a technology readiness program to a deployment readiness program, and was designated a major defense acquisition program in April 1996; (3) the May 1997 Quadrennial Defense Review included the first program estimate based on detailed system descriptions, requirements, and plans; (4) funding increases provided by Congress in fiscal years 1996 through 1998 were used for risk reduction activities, such as: (a) retaining competition in the development of the exoatmospheric kill vehicle, considered one of the most technically challenging components of the system; (b) increasing the number of planned tests; and © purchasing additional spare hardware; (5) Congress increased funding for NMD because of concerns about the adequacy of funding to support the program; (6) the Ballistic Missile Defense Organization (BMDO) Director acknowledged in an April 1996 testimony that an additional $350 million a year could be used to reduce program risks; (7) future NMD funding requirements will depend in large part on the system design and architecture, and when and where it is deployed; (8) details on the specific system and location are not expected for some time; (9) program life-cycle costs ranged from $18.4 billion by fiscal year 2003 to $28.3 billion by fiscal year 2006; (10)

since GAO's December 1997 report, DOD has increased funding and revised NMD program plans to mitigate schedule and technical risks; (11)however, program officials told GAO that even with the mitigation actions resulting from the increased funding, schedule and technical risks associated with a 2003 deployment remain high; (12) according to a February 1998 report of a panel of former senior military, government ,and industry officials, successful execution of the 3+3 program on the planned schedule is highly unlikely; and (13) this panel concluded that the program would benefit from the earliest possible restructuring to contain the risk.

The details of the program changes during this period provide a good picture of the real-world problems in developing such a complex system. A historical analysis by the GAO shows the allocations of Congressional authorization during FY 1996 through FY 1998. Over 80 percent of additional funding was allocated to six program areas—the ground-based interceptor; ground-based radar; system integration; battle management, command, control, and communications system; systems engineering; and test and evaluation. According to NMD officials, these funding increases were used for risk reduction activities and to execute the 3+3 program. Table 2.3 shows how the funding increases for the 3-year period, fiscal year 1996 to 1998, were allocated.[7]

Table 2.3

Allocations of Congressional Funding Increases for Fiscal Years 1996 Through 1998

Funding increase by Program Area	Dollars in Millions	Percent of total
Ground-based interceptor	$434	37
Systems integration	159	14
System test and evaluation	149	13
Ground-based radar	107	9
Battle management, command, control, and communications	72	6
Systems engineering	57	5
Other	196	17
Total	$1,174	100

Note: totals may not add due to rounding.

The largest increase, $434 million (over one-third of the 3-year total), was allocated to the ground-based interceptor. Most of these funds were used to maintain competition in the design and development of the interceptor's kill vehicle. The original plans were to select a

single kill vehicle design and contractor at the end of 1995 before either of the two competing designs had been fully tested—even though the kill vehicle was one of the most complex parts of the NMD system. The additional funding allowed the program to preserve the kill vehicle competition through actual intercept tests in fiscal years 1998 and 1999. Some of the increased funding was also needed to cover the costs of a schedule slippage due to the failure of a flight test in January 1997, purchase a spare kill vehicle from one of the contractors, and upgrade launch capabilities at the test range. Because of subsequent funding reductions, and a decision to incorporate the ground-based interceptor into a lead system integration contract, program officials decided not to begin development of a booster for the interceptor.

Increases totaling $159 million allocated to systems integration were used to obtain a prime contractor for the system. BMDO decided in the summer of 1996 that a prime contractor would be needed to manage the remaining design and development effort and to integrate and test the complete NMD system. Two competitive concept development phase contracts were awarded in fiscal year 1997. One of two concept development phase contractors, Boeing North American Company, won the Lead System Integrator (LSI) contract on April 30, 1998. The LSI serves as the prime contractor for NMD system development. The LSI contractor will be responsible for integrating the elements of NMD (radar, interceptors, and the BMC3). In addition, the LSI will demonstrate the system capability through integrated ground and flight testing, and will serve as the key player in developing the necessary plans for fielding the system, should the decision be made to do so.

In December 1998, Boeing selected Raytheon as the EKV contractor. A Boeing designed EKV is to be held in abeyance, as a risk reduction activity, until completion of data reduction of Integrated Flight Test-4. Plans for this kill vehicle are undefined at this time. The other major team members included Raytheon (ground based interceptor kill vehicle and NMD radars), TRW (BMC3), and Lockheed Martin (payload launch vehicle for initial tests).[8]

An increase of $149 million in the system test and evaluation effort was used in part for additional test targets. Some of the increased funding has also been used to develop an

integrated system test capability needed for ground tests of the various elements of the NMD system. The added funding also permitted increased testing such as using targets of opportunity to test ground-based system elements and a Midcourse Space Experiment designed to obtain information on viewing targets against earth and space backgrounds—a critical capability in identifying and tracking threatening warheads.

Funding increases amounting to $107 million allocated to the ground-based radar have been used to enhance realism in and to accelerate development of the radar that will be used in testing. Original plans were to conduct the tests with a radar technology demonstrator. However, with the increased funding, BMDO decided to construct a ground-based radar prototype to be used in the testing program. The prototype has a larger face than the demonstrator and more closely resembles the radar to be deployed. Additionally, the radar development was accelerated.

After NMD became a deployment readiness program, BMDO found that that a more extensive battle management, command, control, and communications effort was needed to support an NMD system. This effort sought to provide engagement planning and execution, allow human-in-control of the NMD system, and interface with external command, control, and communications systems. With $72 million in additional funding allocated to this element, BMDO was able to begin development of five capability increments of a prototype battle management, command, control, and communications system. The first three increments were completed by April 1998. BMDO also added a NMD communication network and a system that will be used to communicate with the NMD interceptor in-flight.

The originally planned funding levels for systems engineering were sufficient only to support a technology readiness program. Funding for this effort was increased by $57 million mostly in order to prepare and update documents required for a system deployment. BMDO reported that without the additional funding, it would not have been able to baseline the NMD system architecture, and, thus, there would not be a NMD system.

The remaining $196 million of the increases was allocated in smaller increments to a number of areas. The largest of these was an increase of about $50 million for program management support. The increase paid for personnel and contractor support for the joint program office as well as for systems analyses and small business innovative research. Personnel costs previously spread through all the projects were rolled up into one project management line item.

These changes in the program during 1996-1999 did not represent unusual cost escalation or delays for a program of the complexity of an NMD system. They also ensured that NMD research and defense activity was successful in a number of areas, and resolved many of the remaining development and systems integration issues affecting the deployment of a limited ground-based system. As a result, the Secretary of Defense announced in January 1999 that the threat criteria would soon be met, and funds were programmed to move NMD from the development phase to a deployment phase should BMD be directed to do so.

The NMD Acquisition Phase of NMD Activity

The fifth phase of the NMD program began in 2000, although the preliminary NMD system design underwent a successful System Preliminary Design Review (PDR) as early as July 1999. [9] The US State Department announced for the first time in September 1999 that it had selected Alaska as the first interceptor site. This announcement was not picked up in the public literature provide on the system by BMDO, which still refers to a deployment near Grand Forks in North Dakota.[10]

The fifth phase focuses on “NMD acquisition,” and its goal is to prepare for the initial deployment of a limited NMD system by 2005. The BMDO describes this phase as follows: “The current NMD Program is structured to develop, demonstrate and present at a Deployment Readiness Review in FY2000, an integrated system designed to meet the threat requirement. The Development Phase is currently underway and an Integrated System Test is planned for FY2000, prior to the Deployment Readiness Review. Subsequent to FY2000 Review, and if directed to do

so, the Program will complete system development and field an initial capability, designed to protect the 50 States from a limited attack, by FY2005. “

It is important to note, however, that this NMD system is ground-based only and currently budgets for only 20 interceptors. Furthermore, more BMDO resources were devoted to theater than national missile defense, and a major research effort remained underway to develop defenses considerably more advanced than the ones the US currently plans to deploy as part of its nominal NMD architecture.

The current theater missile defense effort focuses on the deployment of the US Army Theater High Altitude Area Defense (THAAD), the US Aegis Navy Area theater ballistic missile defense (TBMD), and Patriot Advanced Capability 3 (PAC-3) programs as part of a “new organizational focus concentrating on providing theater missile defense to troops stationed overseas and to any emerging threats to U.S. territory.” The Advanced Technology program is a “third priority,” which is “intended to provide technology options for improvements to planned and deployed defenses, operational support costs and command facilities. Survivability, Lethality, and Key Support Technologies (SLKT) involved countermeasures integration, lethality and target hardening, and new concepts development.” Recent BMDO spending on these efforts is shown in Table 2.4.

Table 2.4

Recent BMDO Spending on Missile Defense

Appropriation	FY1998 Appropriated	FY1999 Appropriated	FY2000 Requested
RDT&E			
Navy Area TBMD	290	245.8	268.4
Navy Theater Wide	410	368.4	328.8
PAC-3	206	322.3	29.1
THAAD System	406	445.3	611.6
NMD	978	1550.5	836.6
Other	1,095	972.2	868.9
Total	3,385	3,904.5	2944.4
Procurement			
PAC-3	349	248.2	300.9
Navy Area TBMD	15	43.3	55.0
BMC3	20	22.8	0
Total	385	314.3	355.9
MILCON	3	10	1.4
TOTAL	3,773	4,228.8	3,301.7
% Directly on NMD	26%	23%	25.3%

Source: BMDO, Department of Defense, March 1999.

Jacques S. Gansler, the Under Secretary of Defense for Acquisition and Technology provided the following additional details on the FY2000 missile defense program in his testimony to the House Armed Services Committee on February 25, 1999:

> "Of the $6.6 billion in new funds programmed for national missile defense, $600 million will be provided using the FY 1999 Emergency Supplemental for Ballistic Missile Defense. These supplementary funds permit additional risk-reduction efforts, as well as activities needed to ensure a smooth transition to deployment should a decision be made in FY 2000 to begin deploying the system. Previous plans for testing national missile defense components and the system prior to the deployment decision remain unchanged. In June 1999, the performance of the exo-atmospheric kill vehicle will be demonstrated in the first national missile defense intercept attempt. Subsequent tests, to be conducted before the June 2000 decision point, will further evaluate the system's performance, culminating in an "end-to-end" systems test in the second quarter of FY 2000.
>
> "To maximize the probability of programmatic success and be able to deploy a technologically capable system as quickly as possible, key national missile defense decisions will be phased to occur after critical integrated flight tests. As a result, instead of projecting a deployment date of 2003 with exceedingly high risk, the Department now projects a deployment date of 2005 with much more manageable, although still high, risk. The funds added to the national missile defense program in FY 2001-2005 support a deployment in FY 2005. The majority of national missile defense funding through FY 2000 is in the RDT&E

appropriation; procurement funding would begin in FY 2001. Military construction funds are programmed in FY 1999 for design, while construction is funded in FY 2001-2005.

“If testing goes flawlessly, and there is a willingness to accept higher program risk, we could seek to deploy sooner. But independent analysts have expressed concern that the Department’s fast-paced schedules for ballistic missile defense programs have sometimes represented a "rush to failure." Given the reality of the threat, the national missile defense program cannot afford to fail.

“The Air Force’s Space Based Infrared System (SBIRS) system is an important element of our BMD program. Both components of the SBIRS program, SBIRS-High and -Low, have seen significant cost growth and technical challenges during the past year. The President’s Budget restructures both components of the SBIRS program to make optimum use of available Defense Support Program satellites, yet provide timely support to the ballistic missile defense mission.

In that regard, we are rescheduling the SBIRS-High program’s first launch of its geosynchronous satellite to FY 2004. We currently have five Defense Support Program satellites awaiting launch, and the Department, in executing its stewardship responsibilities, must make full use of those satellites before launching a replacement system. The new SBIRS-High schedule synchronizes well with the new national missile defense schedule in that the required number of SBIRS-High geosynchronous satellites (two) will have been launched in time to support a national missile defense deployment in 2005. It should be noted that, although SBIRS-High will provide improved performance compared to its predecessor in all mission areas, the Defense Support Program is adequate for the strategic warning mission. And the Defense Support Program can support the initial deployment of the national missile defense system, with only a very slightly reduced confidence level of successful defense.

“We are also restructuring the SBIRS-Low component, resulting in a planned first launch in FY 2006. This change is driven primarily by the technical challenges and complexities inherent in the system. As part of the SBIRS-Low restructure, after the formulation of the FY 2000 President’s Budget, we cancelled the two flight demonstration experiments that were part of our earlier-conceived risk reduction effort. Much has already been learned and significant risk has been mitigated through the design, fabrication, assembly, and integration accomplished to date. Continuation of the flight experiments is not critical to SBIRS-Low, and the remaining program risk is best addressed in the now more robust Program Definition studies that will constitute the next phase of the SBIRS-Low acquisition. We intend to pursue the SBIRS-Low program in a manner consistent with program risk and the need to support our BMD programs.

“Activities in the missile defense technology base are key to countering future, more difficult threats. The technology base program underpins the theater ballistic missile defense, cruise missile defense, NMD, and Space Based Laser programs. It will enable the Department to provide block upgrades to baseline systems, perform technology demonstrations, reduce program risk, accelerate the insertion of new technologies, and develop advanced technologies to provide a hedge against future surprises. Advanced technologies are also being exploited to reduce the cost of future missile defense systems.

“In the past, BMDO explored many potential solutions to ballistic missile defense, including exotic or leap-ahead technologies (X-ray lasers, neutral particle beams, Brilliant Pebbles). Today's thrust is to provide research and development in technical areas that support our missile defense programs. Three programs in particular illustrate BMDO's current thinking: 1) the Atmospheric Interceptor Technology program, which develops advanced missile technologies for PAC-3, THAAD, and Navy Theater Wide to address advanced threats and reduce cost, 2) the Exoatmospheric Interceptor Technology program, which is developing and demonstrating advanced seeker concepts, as well as advanced materials, to provide upgrades to both NMD and TMD interceptors, to counter the evolving threat and reduce cost, and 3) the Advanced Radar Technology program which improves signal processing capabilities and reduces key component costs. We

expect these programs to provide useful hardware and data to the TMD and NMD programs.

"Recently, BMDO and the Air Force had an Independent Review Team of laser, operational, and programmatic experts examine the Space Based Laser program. They proposed that any orbital flight experiment be preceded by extensive integrated ground demonstrations of key technologies and flight system elements. The subsequent orbital spacecraft experiment they envision would demonstrate large, lightweight deployable optics, a new concept in very large mirrors that could enable dramatic savings in vehicle weight and attendant cost.

"We have developed a laser technology program that balances long-term research and development goals with a nearer-term goal to demonstrate the basic feasibility of a system. The total outlay for the program will be $139 million in FY 1999 and $139 million per year through FY 2000-2005. The technology program, jointly funded by BMDO and the Air Force, will fund a ground demonstration and permit a subsequent decision to increase funding enroute to orbiting a spacecraft. Affordability--both of a demonstration flight and of an eventual operational system--is a key concern on which we intend to focus."

The Clinton Administration's 2000 budget request for the Ballistic Missile Defense Organization totalled $3.3 billion. This included $2.9 billion for RDT&E, $355.9 million for procurement, and $1.3 million for military construction activities. Combining these three budget categories, the Theater Air and Missile Defense programs accounted for $1.9 billion or roughly 60 percent of the budget. National Missile Defense represented $836.6 million or 25 percent of the budget. The Administration requested $65.3 million for Applied Research and $173.7 million for Advanced Technologies, together, these programs represented about 7 percent of the budget. BMD Technical Operations accounted for $192.0 million and is about 6 percent of the budget. The Administration requested $16.5 million for Threat and Countermeasures efforts and $36.6 million for International Cooperative Programs. Together, these programs represent 2 percent of our overall budget.

The Congress chose to appropriate more money for FY2000 than the Department of Defense requested. The Department requested $3,672,822,000 for all ballistic missile defense programs. The bill provided for a total of $3,899,543,000 for all ballistic missile defense programs. It included $3,669,543,000 in new appropriations and $230,000,000 to be derived from funds previously provided in Section 102 of division B, title I, chapter 1 of Public Law 105-277. A total of $2,970,009,000 was provided for research and development; $355,900,000 was provided for procurement within the Ballistic Missile Defense Organization (BMDO) budget; and, $343,634,000 was provided in Air Force research and development programs to

include $308,634,000 for the Airborne Laser and $35,000,000 for the Space-Based Laser. The bill provided the budgeted amount for the joint U.S.-Israel ARROW anti-tactical ballistic missile development program, and provides for $45,000,000 to support deployment of a third ARROW battery. The recommended amounts represented an increase of $226,721,000 over the budget request of $3,672,822,000 for these programs.

The FY2000 Authorization Act authorized a net increase of $403.0 million for ballistic missile defense programs, $169.5 million for military space programs and technologies, and $201.6 million for strategic nuclear delivery vehicle modernization. It authorized an increase of $212.0 million for the Patriot PAC-3 system, $90.0 million for the Navy Upper Tier (Theater Wide) and $92.0 million for the Space Based Infrared (High) program. It authorized an increase of $90.0 million for the Navy Upper Tier (Theater Wide) theater missile defense program, of which $50.0 million was for continuation of advanced radar technology development and $40.0 million is for program acceleration. It authorized an increase of $30.0 million for the Atmospheric Interceptor Technology program, an increase of $15.0 million for the Arrow Deployability Program, an increase of $10.0 million for the Tactical High Energy Laser Program, an increase of $10.0 million for the Space-Based Laser program and an increase of $92.0 for the Space Based Infrared (High) program.

The Congress also called for a report on the risks in the NMD deployment program and directed that with the submission of the Fiscal Year 2001 budget, the Secretary of Defense shall submit to the congressional defense committees a report that contains an assessment of the advantages or disadvantages of deploying a ground-based National Missile Defense system at more than one site. It include a version of the National Missile Defense Act of 1999 in the FY2000 Defense Authorization Bill which declares that it is U.S. policy to: (1) deploy as soon as technologically possible a National Missile Defense (NMD) system capable of defending U.S. territory against limited ballistic missile attack (whether accidental, unauthorized, or deliberate), with funding subject to the annual authorization of appropriations and the annual appropriation of funds for NMD; and (2) seek continued negotiated reductions in Russian nuclear force. The

key portions of the text read as follows:[11]

> "It is the sense of Congress that--
>
> (1) because technology development provides the basis for future weapon systems, it is important to maintain a healthy balance between funding for the development of technology for ballistic missile defense systems and funding for the acquisition of ballistic missile defense systems;
>
> (2) funding planned within the future-years defense program of the Department of Defense should be sufficient to support the development of technology for future and follow-on ballistic missile defense systems while simultaneously supporting the acquisition of ballistic missile defense systems; and
>
> (3) the Secretary of Defense should seek to ensure that funding in the future-years defense program is adequate both for the development of technology for advanced ballistic missile defense systems and for the major existing programs for the acquisition of ballistic missile defense systems.
>
> Not later than March 15, 2000, the Secretary of Defense shall submit to Congress the Secretary's assessment of the advantages or disadvantages of a two-site deployment of a ground-based National Missile Defense system, with special reference to considerations of the world-wide ballistic missile threat, defensive coverage, redundancy and survivability, and economies of scale."

The NMD Program Before President Clinton's Decision to Defer Deployment

The Department indicated in early 2000 that its strategy retained a two-phased approach: (1) development; and (2) possible deployment, based on the threat and the demonstrated technological feasibility of the system to defeat that threat. A decision to deploy, based on the recommendation of the Deployment Readiness Review (DRR), was planned for June 2000, to allow the program to plan for the fielding of a Capability 1 architecture by 2005 instead of 2003.

The specific decisions to be made at the DRR were the commitment to deployment, element site selection, and authorization to proceed to contract award for site construction. Two other key decision points were added on the path to the 2005 deployment. An FY2001 decision was to consider the building and/or upgrading of required ground radar systems and the integration of command and control software into the Cheyenne Mountain Operations Center. An FY2003 decision was to determine if the weapon system is ready for limited production and deployment. If no deployment decision is made, the program will still continue development with an eventual focus on a more capable NMD (Capability 2) system.[12]

The Secretary Cohen also directed the Department to take no programmatic steps that would preclude the potential to deploy earlier than FY05. As part of the NMD redirection, more than $6 billion in additional funding was programmed to support development and initial deployment. The Department of Defense estimated that the life cycle cost of the program would be $26.6 billion as of February 2000. This estimate was based on deployment of the first interceptor site in Alaska, and an initial force of 20 interceptors – at a cost of $1.105 billion each. (Assuming an FY2005 deployment. The figure quoted includes the cost of operating the system for 20 years as well as development, production, and construction costs.)[13]

Secretary Cohen described the NMDO program as follows in his FY2000 annual report to the President and Congress in February 2000,

> "The submission of the FY 2000 budget request marks a major change in the Administration's funding commitment to National Missile Defense. The addition of $6.6 billion in new funding brings total FY 1999-2005 resources for NMD to $10.5 billion, of which $9.5 billion is allocated in FY 2000-2005. The added funds include those that would be required through FY 2005 to deploy an NMD system. No decision for deployment has been made. However, a decision regarding deployment is planned for June 2000 that will be based primarily on the maturity of the technology as demonstrated by progress in development and testing.
>
> The NMD program has been geared for some time to the possibility that a rogue nation could—perhaps sooner than intelligence has projected—come to possess intercontinental ballistic missiles that could threaten the United States. This possibility was underscored by the August 1998 North Korean attempt to launch a satellite on a Taepo Dong-1 (TD-1) missile. The test demonstrated that North Korea continues to be interested in developing long-range missile capabilities and that it has made considerable progress. That launch demonstrated some important aspects of ICBM development, most notably multiple-stage separation. While the intelligence community expected a TD-1 launch for some time, it did not anticipate that the missile would have a third stage or that it would be used to attempt to place a satellite in orbit.
>
> The intelligence community's current view is that North Korea would need to resolve problems with the third stage prior to being able to use the three-stage configuration as a ballistic missile to deliver small payloads to intercontinental ranges (that is, ranges in excess of 5,500 kilometers). Nonetheless, a three-stage variant of the TD-1, if successfully developed and deployed, could pose a threat to portions of the United States sooner than estimated previously. The TD-1 launch demonstrates the very type of potential near-term threat that led the Administration to propose the NMD deployment readiness program in 1996.
>
> The NMD system being developed would have as its primary mission defense of the United States—all 50 states—against a small number of intercontinental ballistic missiles launched by a rogue nation. Such a system would also provide some capability against a small accidental or unauthorized launch of strategic ballistic missiles from China or Russia. It would not be capable of defending against a large-scale, deliberate attack.
>
> Of the $6.6 billion in new funds programmed for NMD, $800 million will be provided from the FY 1999

> Emergency Supplemental for Ballistic Missile Defense. These funds permit additional risk-reduction efforts, as well as activities needed to ensure a smooth transition to deployment should a decision be made in FY 2000 to begin deploying the system. Previous plans for testing NMD components and the system prior to the deployment decision remain unchanged. In June 1999, the performance of the exoatmospheric kill vehicle will be demonstrated in the first NMD intercept attempt. Subsequent tests, to be conducted before the June 2000 decision point, will further evaluate the system's performance, culminating in an end-to-end systems test in the second quarter of FY 2000. The FY 2000 request includes no procurement funding associated with deployment. The funds added to the NMD program in FY 2001-2005 support a deployment in FY 2005.
>
> To maximize the probability of programmatic success and be able to deploy a technologically capable system as quickly as possible, key decisions will be phased to occur after critical integrated flight tests. As a result, instead of projecting a deployment date of 2003 with exceedingly high risk, the Department now projects a deployment date of 2005 with much more manageable risk. If testing goes flawlessly, the system might be ready for deployment sooner. But independent analysts have expressed concern that DoD's fast-paced schedules for ballistic missile defense programs represent a rush to failure. Given the reality of the threat, the NMD program cannot afford to fail. The approach the Department has adopted is the optimal one to provide a capable NMD system as soon as possible.
>
> The NMD development program will continue to be conducted in compliance with the Anti-Ballistic Missile Treaty. NMD deployment may require modifications of the treaty, and the Administration is working to determine the nature and scope of these modifications. Environmental surveys for potential basing sites in both Alaska and North Dakota have begun, and Russian officials have been briefed on these activities. If deployment requires an amendment to the treaty, the United States will negotiate with the Russians in good faith."

The President's FY2001 budget was submitted to Congress in February 2000. The Department of Defense summarized its request for missile defense funds as follows:

> The FY 2001 budget continues the marshalling of the technology and funding needed to deploy a National Missile Defense (NMD) system to defend all 50 states against a limited ballistic missile attack. Later this year the President will decide whether to deploy such a system based on four criteria: threat, cost, technical feasibility, and overall security implications including arms control. The budget for FY 2001-2005 includes sufficient NMD funding to achieve a 2005 initial capability if deployment is ordered. FY 2001-2005 NMD funding totals $10.4 billion—reflecting the addition of $2.3 billion since last year's request. The budget will allow DoD to upgrade early warning radar facilities, build a radar complex in Alaska, provide 100 ground based interceptors, and fund additional systems testing.
> Also a top DoD priority is a strong theater air and missile defense program—aimed at meeting current regional threats. The budget continues to advance the goal of deploying systems that can protect forward-deployed U.S. forces, as well as allies and friends. To defeat shorter-range missiles, key lower-tier programs currently are the Patriot Advanced Capability-3 (PAC-3) and Navy Area Defense systems. Key upper-tier programs are the Theater High Altitude Area Defense (THAAD) and Navy Theater Wide systems. To defeat theater-range missiles during their boost phase, development of the Airborne Laser and Space-Based Laser is continuing.

Lt. General Ronald T. Kadish, the Director of BMDO, provided a detailed summary of the FY2001 program to the Senate Appropriations Committee, Defense Subcommittee, on April 12, 2000.[14]

The total Fiscal Year (FY) 2001 budget request for the Ballistic Missile Defense Organization is $4.5 billion. This includes $3.9 billion for research, development, test, and evaluation (RDT&E), $444 million for procurement, and $103.5 million for military construction (MILCON) activities. Combining these three budget categories, National Missile Defense represents $1.92 billion, or 43 percent of the budget. Theater Air and Missile Defense programs account for $1.95 billion, also roughly 43 percent of the budget. We request $37.7 million for Applied Research and $93.2 million for Advanced Technologies, which together represent about 2.9 percent of the budget. BMD Technical Operations accounts for $272.6 million and is about 6 percent of the budget. We request $22.6 million for Threat and Countermeasures efforts and $117 million for International Cooperative Programs, which together represent 3 percent of our overall budget. The following chart breaks out the Fiscal Year 2001 budget request by program element for BMDO-managed programs.

… Based on recent threat assessments, my program guidance is to be in a position, technologically, to support a decision later this year on whether to deploy a National Missile Defense (NMD) system capable of defending all 50 states against limited ballistic missile attack from states that threaten international peace and security. Recent intelligence estimates indicate that we must be concerned about the possibility that ballistic missile threats from states that threaten international peace and security will increase as they acquire a capability to launch more and longer range missiles with simple countermeasures in the 2005 to 2010 timeframe. As a result, we are enhancing the NMD program beyond the original Capability 1, or "C1," architecture by developing an "Expanded C1" architecture to meet this expanded threat. The Expanded C1 architecture will be capable of defending all 50 states against expected near-term threats larger than the initial C1 architecture was designed to handle.

The Expanded C1 deployment option builds on revised program guidance announced last year by the Secretary of Defense. For planning purposes, the Expanded C1 system will incorporate 100 ground-based interceptors based in Alaska and an advanced X-Band radar based at Shemya Island, also in Alaska. Our NMD architecture plans incorporate upgrades to the existing ballistic missile early warning radars and, for the purposes of initial launch detection, use the Space Based Infrared System (SBIRS) High, which eventually will replace the existing Defense Support Program satellite constellation. Initial Operational Capability (IOC) for the C1 architecture, consisting of 20 interceptors, still can take place in 2005. The full 100 can be deployed by Fiscal Year 2007. Since the President submitted the FY00 budget to Congress, the NMD program has been increased by $2.3 billion over FY01-05. Between Fiscal Years 2001 through 2005, we have programmed $10.375 billion (in then year dollars) for the NMD program.

In 1999, BMDO commissioned a second independent panel headed by retired General Larry Welch to review the National Missile Defense (NMD) program in light of the program's new structure. The panel's charter was to determine the effects of extending the NMD program by two years and to review the adequacy of the resulting test program. The panel concluded that, although the revised NMD program reduced program risk, it remains a high-risk program. The panel made 18 specific recommendations to reduce program risk further. I support the panel's recommendations and have added $285M across FY01-05 to augment the NMD testing program. This funding will pay for additional hardware for the NMD Kill Vehicle, additional test equipment and testing.

… We plan to conduct a Deployment Readiness Review (DRR) in July of this year. We recently adjusted the schedule for the DRR, delaying this technology readiness assessment of the NMD program by approximately one month. The DRR is a review internal to the Defense Department that will be led by the Under Secretary of Defense for Acquisition, Technology & Logistics. We think the delay is prudent given our rescheduling of Integrated Flight Test 5 (IFT-5) to take place on June 26 of this year. We do not believe moving the DRR to July will materially affect the current schedule which supports fielding an initial capability in Fiscal Year 2005.

Although the DRR starts a key decision process, it is the first of at least three decision milestones in the program over the next five years. The technological assessment of the NMD program will take place at the Defense acquisition executive level - with full participation from all Department of Defense stakeholders. The DRR will not constitute the actual decision to deploy the NMD system. Rather, it will assess the technological progress to support a deployment decision. The Administration's decision will be based on an assessment of four factors: (1) the nature of the threat; (2) the status of the technology based on an initial series of rigorous flight tests, and assessment of the proposed system's operational effectiveness; (3) system affordability; and (4) assessments of the impact of NMD deployment on the overall strategic environment and U.S. arms control objectives, including efforts to achieve further reductions in strategic nuclear arms under START II and START III.

If a decision is made to deploy, we will simultaneously seek approval for our recommended NMD site and award of the construction contract for that site. A decision to deploy would lead us to conduct a Defense Acquisition Board review to assess the status of the program in late Fiscal Year 2001. Based on program performance, we would seek approval to initiate upgrades to the current early warning radars, begin building the missile site, and start integrating the Battle Management/Command, Control and Communications (BM/C3). In Fiscal Year 2003, we would conduct a second Defense Acquisition Board review to seek approval to procure and deploy the ground-based interceptors as well as the necessary spares and test rounds. All of these decisions will depend on an assessment of our technical and programmatic progress.

…While we have been developing and testing the system elements, we also have been proceeding vigorously on deployment planning activities. We have conducted fact-finding and siting studies for two potential site locations - Alaska and North Dakota. We have initiated site designs for the X-band radar, weapon sites, and BM/C3 facilities. On October 1, 1999, we published in the Federal Register a Notice of Availability of the NMD Program's Deployment Draft Environmental Impact Statement (EIS), inviting the public to review and comment on that document. The public comment period ended on January 19, 2000. In October and November of last year, over 650 people attended public hearings on the draft EIS in Alaska, North Dakota, and Washington, D.C. We are considering the input received as we prepare the Program's Final Environmental Impact Statement, which we have scheduled for completion later this spring. As required by law, the results of the EIS will represent one of many inputs into the deployment decision process.

We initiated ground-based element facility planning and design in FY99 and have completed the 65% design for the weapon system and X-band radar facilities. We will start the design of the BM/C3 facilities later this year. For FY01, we are submitting a request for construction of the tactical and support facilities for an Expanded C1 capability. This will consist of an X-Band Radar Complex, a Ground-Based Interceptor Missile Launch Complex, and a series of dispersed facilities for Battle Management/Command, Control, and Communication. We request a FY01 MILCON appropriation of $101.6M to begin construction of the X-band radar, conduct site preparation of the interceptor site, and continue planning and design work.

In accordance with budget guidance, we will further define the facility and systems requirements associated with potential deployment of 100 interceptors in an Expanded C1 architecture by FY07, including the installation of 80 additional missile silos and non-tactical facilities. In order to remain on schedule for the deployment of the first 20 missiles in FY05, we plan to issue a Request for Proposal and award the contract(s) this fall, if approval for deployment is given.

We have made important technical progress in many areas in the National Missile Defense program. Nevertheless, this is an extremely complex program and we still have many significant challenges ahead of us.

The Senate voted on July 14, 2000 to authorize a total of $1.9 billion for NMD in FY2001. It approved the budget by a 52-48 vote. The defense authorization bill for fiscal 2001 passed by a 97-3 vote. The bill authorized $310 billion for defense, $4.5 billion more than President Clinton requested, and a 4.4 percent increase over last year's funding. The bill also included a 3.7 percent pay raise for military personnel, effective January 1, 2001, and by allowed veterans age 65 and older to buy prescription drugs at discount prices.[15]

The projected budget for all of BMDO and for the NMD program is shown in Table 2.5 below:

Table 2.5

The BMDO Budget Request for FY2000 and FY2001 in Then Year $US Millions

	FY2000	FY2001
National Missile Defense		
NMD Dem/Val*	950.248	1,740.238
NMD Procurement	0.000	74.530
NMD Milcon	15.000	101.595
Theater Air and Missile Defense		
PAC-3 EMD	179.139	81.016
PAC-3 Procurement	343.773	365.457
Navy Area EMD	307.274	274.234
Navy Area Procurement	18.143	0.000
THAAD Dem/Val	523.525	0.000
THAAD EMD	79.462	549.945
Navy Theater Wide Dem/Val	375.764	382.671
TMD BMC/3 Procurement	0.000	3.975
Joint TAMD Dem/Val	196.566	0.000
FoS E&I	145.657	231.248
MEADS Dem/Val	48.594	63.175
Support Technologies		
Applied Research	88.365	37.747
Advanced Technology Dev.	212.837	93.249
Boost Phase Intercept	4.961	0.000
Space Based Laser**	0.000	74.537
Organizational Costs		
BMD Technical Operations		
BMD Tech Ops	214.445	270.718
BMD Tech Ops Milcon	1.372	1.923
International Coop Programs	81.560	116.992
Threat & Countermeasures	19.343	22.621

Pentagon Reservation Maintenance Fund	0.000	4.775

* $590M in FY99 funding is being applied to FY00 requirements.
** SBL (included under Advanced Tech Development in FY00), which has a separate PE in the FY2001 PB, represents $74M or 1.7 percent of the budget and represents more than half of the total required funding in partnership with the U.S. Air Force

The Total Cost of the US Ballistic Missile Defense Program to Date

A full breakout of the costs of the first four phases of the US ballistic missile defense effort is shown in Figure 2.1 The direct costs of the NMD program reached $16.9 billion during 1995-1999 – or roughly 30% of the total money the US spent on ballistic missile defense. The total cost of all SDIO and BMDO activity reached over $56 billion in direct costs to the Department of Defense, by the end of the fourth phase in 1999, plus several billion more in costs by other federal agencies.

Secretary Cohen's January 20, 1999, announcement acknowledged and affirmed the emerging missile threat and announced the dedication of an additional $6.6 billion for NMD during fiscal years 1999 through 2005. He also noted that the Administration had begun a dialogue with Russia about the development related to our NMD program and the ABM Treaty. Finally, he recognized that the program was now structured to work towards a key requirement - developing and demonstrating the technological readiness of our system. A later budget statement indicated that the Department intended to allocate $10.504 billion (in then year dollars) for the NMD program between fiscal years 1999 through 2005.[16] As has been noted earlier, the life cycle cost of the program over 20 years was estimated to be $26.6 billion over 20 years, assuming the interceptor force was initially deployed in Alaska and was kept at a force of 20 interceptors.[17]

A White House fact sheet issued the day after President Clinton deferred an NMD deployment decision on September 1, 2000 stated that, "The Clinton Administration has spent approximately $5.7 billion on NMD, and budgeted an additional $10.4 billion in FY 2001-2005 to support possible deployment of the initial NMD architecture. Our current estimate for developing, procuring and deploying our initial system of 100 interceptors, an ABM radar,

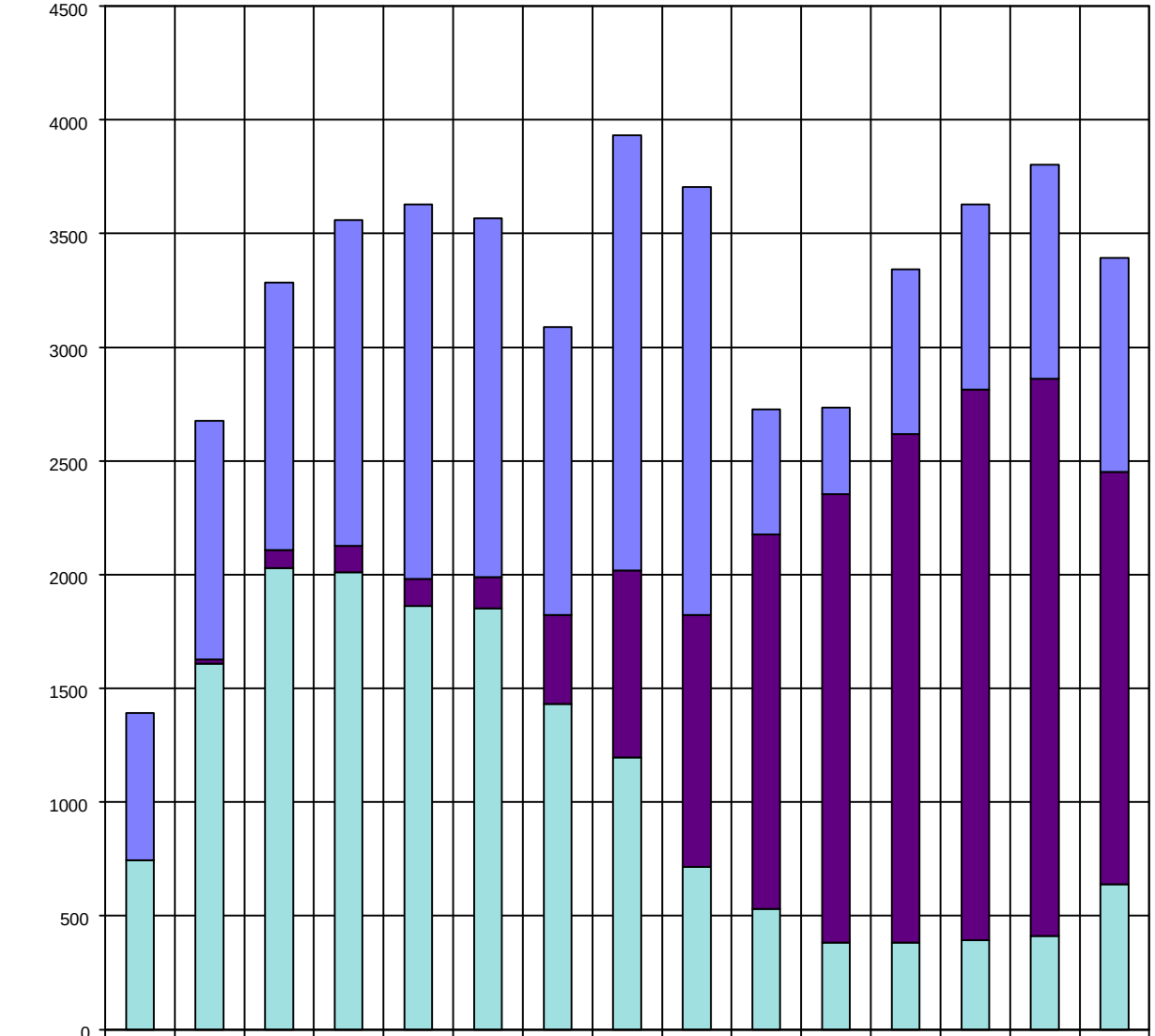
upgrades to 5 early warning radars, and command and control is around $25 billion (Fiscal Years 91-09). But to put that in perspective, it represents less than 1 percent of the defense budget over the coming six years."[18]

Some politicized cost estimates designed to attack NMD include the total cost of all SDIO and BMDO programs in the cost of preparing for the deployment of the current NMD program. This is manifestly unfair, even if one ignores the validity of including the cost of the totally different NMD programs carried out during the Cold War. At the same time, the direct costs of NMD alone understates the fact that the bulk of "other" RDT&E costs are spent on NMD.

The key point is that the US is giving both TMD and NMD high priority and continues to invest in a future capability to deploy a very different kind of NMD program. This is a key point in terms of both program analysis and national priorities. Whatever one may think of the ballistic missile threat to the US homeland, the theater threat is already real. Similarly, it seems hard to deny the need for a robust technology program unless the world becomes a far safer place.

Figure 2.1

BMDO Historical Funding



	85	86	86	88	89	90	91	92	93	94	95	96	97	98	99
NMD/SDI	647	1048	1177	1423	1651	1583	1265	1916	1886	553	387	729	812	936	943
TMD	2	22	78	125	111	131	392	822	1103	1646	1970	2234	2423	2456	1816
Support	748	1606	2025	2006	1865	1857	1431	1194	718	529	382	381	393	408	637
Total	1397	2676	3280	3553	3637	3571	3088	3932	3707	2728	2739	3405	3628	3800	3396

The total program cost through 1999 was $48.527 billion. The total was $16.956 billion for NMD, $15.331 billion for TMD, and $16.179 billion for support technology.

Source: Adapted by Anthony H. Cordesman from Ballistic Missile Defense Organization (BMDO) “Ballistic Missile Defense

Organization Budgetary History, BMDO Fact Sheet PO-99-02, April, 1999.

The CBO Report on Budgetary Implications of National Missile Defense

It must be stressed that the preceding data describe a program that will have to be totally restructure by the next President, Moreover, the Department of Defense has never provided meaningful cost estimates of the price of a mature program. The most detailed report on the risks, costs, and benefits of the NMD program is provided in a report by the Congressional Budget Office (CBO) entitled on Budgetary Implications of National Missile Defense and which was issued in the April 2000.[19]

> The Administration's plan for NMD gives policymakers the flexibility of deploying the system in three phases, each with different capabilities. The Administration could choose to deploy all three sequentially or halt deployment after any one of them. The first phase, known as Expanded Capability 1, would cost nearly $30 billion, the Congressional Budget Office (CBO) estimates. That figure includes one-time costs and operating costs through fiscal year 2015. (By comparison, the Administration's estimate is nearly $26 billion.) Continuing on to the second stage, Capability 2, would cost an additional $6 billion, for a total of nearly $36 billion, CBO estimates. Achieving Capability 3, the most extensive and sophisticated stage of NMD deployment, would add more than $13 billion to the costs of Capability 2. Thus, costs for the entire system would total nearly $49 billion through 2015, in CBO's view. (The Administration has not released estimates for Capabilities 2 and 3.) Those CBO estimates do not include the costs of space-based sensors for NMD because the sensors would be used for other missions as well and their costs are included in separate Air Force programs. CBO's estimates attempt to strike a balance between overestimating and underestimating potential NMD costs.
>
> The Administration's current plan for national missile defense shows Expanded Capability 1 possibly being deployed at the end of fiscal year 2007, Capability 2 at the end of 2010, and Capability 3 at the end of 2011. However, the Administration's current Future Years Defense Program, which runs through 2005, does not include significant funds for those later phases. To begin funding the Capability 2 system after 2005 and still meet the target deployment date of late 2010, CBO estimates would require annual spending that would surpass $3 billion in 2006 and 2007. Moreover, that estimate assumes that the Administration decides not to proceed with Capability 3. If it also attempted to acquire Capability 3 by late 2011—as well as Capability 2 along the way—annual spending would have to exceed $6 billion in 2007 and 2008.
>
> The fact that a number of potentially hostile nations are reported to be developing long-range ballistic missiles has instilled a sense of urgency in the Administration, causing it to propose a very ambitious development schedule for NMD. That schedule is significantly shorter than those of previous missile and satellite programs that CBO examined. The abbreviated schedule raises questions in the minds of some analysts about whether enough tests would be conducted to ensure that the system under development actually worked.
>
> CBO has compared the Administration's flight-test program with those of other major missile development efforts to assess whether the number of proposed test flights is appropriate for a program of this complexity. Unfortunately, the record of past programs is ambiguous. One interpretation of that record—that technological advances in computers and ground tests allow more development to occur with fewer

> flight tests—suggests that the 21 flight tests proposed for NMD might be sufficient. Another interpretation—that missiles developed from existing systems need fewer flight tests but new concepts need more—suggests that NMD would need more flight tests than the Administration has planned. Those tests cost approximately $80 million each.
>
> Another consequence of the shortened schedule for NMD is a large degree of overlap between developing the system, integrating its various components, and producing it. (For example, all of the interceptors for Expanded Capability 1 would be purchased before the first test flight of the initial operational test and evaluation stage of the development program.) Some overlap is not uncommon in missile development efforts. Program managers use concurrent development and production to quickly field weapon systems that are considered vital to the nation's security— which supporters strongly believe NMD to be. However, such overlap can result in both growing costs and, ironically, significant delays in deployment if a system is produced before all of its design problems have been worked out.
>
> Some problems have already occurred in NMD's development. For instance, the system failed to intercept the incoming target during its most recent flight test because of a faulty cooling system in the interceptor. Does that result indicate a serious design problem or a failure in quality control? Both options are potential procurement issues, even if they are not problems with the basic science of the hit-to-kill approach.

The CBO report is the only unclassified US government report which explicitly examines the implications of the cost of an NMD program that goes beyond a limited introductory deployment and it is also certainly correct in warning that even the basic system would cost at least $30 billion, rather than the $26 billion the government budgets, and that a more adequate system would cost at least $50 billion. Given past cost escalations at this level of technical risk, the life cycle cost of a Capability 3 system might well rise to levels around $100 billion.

The Details of the CBO Cost Estimate

The details of the CBO estimate show that little parametric and regression analysis was applied to its cost estimates, and it is vital to understand that even the Capability 3 system still locates interceptors at only one site, and does not plan to deal with a large or extremely sophisticated threat. [20]

> CBO estimates that costs for the Expanded Capability 1 stage of NMD would total $29.5 billion through 2015—$20.9 billion for one-time costs and about $8.5 billion for initial operations (see Table 2.5). That total is $3.9 billion more than the Administration's estimate. Total costs would increase by $6.1 billion if the system progressed to Capability 2 and by another $13.3 billion if it moved to Capability 3—for a total system cost of $48.8 billion. (The Administration has not estimated the additional costs of Capability 2 or 3.)
>
> CBO's estimates of total costs include one-time expenses for such things as design, procurement, and construction as well as operations costs through 2015. The estimates for operations costs cover different periods of time based on when parts of the system would be initially operational. The estimate for operations for Expanded Capability 1 covers 2005 through 2015; the added operations costs for Capability

2 occur in 2010 through 2015; and the additional costs for Capability 3 come in 2011 through 2015. Those estimates assume that the systems complete more rigorous operational test and evaluation programs than those planned by the Administration during their first five years of operation and reach a steady-state level of operations costs in their sixth year. In this paper, annual operations costs after 2015 are expressed in fiscal year 2000 dollars, and all other costs are expressed in the dollars of the relevant year (in other words, adjusted for expected inflation).

Table 2.5.

Total Costs for National Missile Defense by Level of Capability, 1996-2015
(In billions of dollars)

	Administration's Estimate[a]	CBO's Estimates		
Type of Cost	Expanded Capability 1	Expanded Capability 1	Capability 2	Capability 3
Design, Procurement, and Construction				
Interceptors	6.1	7.1	9.5	12.7
X-band radars	1.1	1.2	2.5	4.6
Early-warning radars	1.2	1.3	1.3	1.7
Command and communications facilities	2.0	2.2	2.2	3.6
Test and evaluation	2.2	2.2	2.8	2.8
System integration	5.4	5.4	5.4	5.4
Construction	0.5	1.5	1.8	4.0
Subtotal	18.6	20.9	25.6	35.0
Operations[b]				
Operational tests	2.7	4.2	5.2	5.2
Day-to-day operations	1.9	1.9	2.4	3.4
Operational integration	2.4	2.4	2.4	5.3
Subtotal	7.0	8.5	10.0	13.9
Total	25.6	29.5	35.6	48.8
Memorandum:				
Annual Cost for Operations After 2015 (In 2000 dollars)	0.6	0.6	0.7	1.1
Costs of SBIRS-Low[c]	0	0	10.6	10.6

SOURCES: Congressional Budget Office; Department of Defense.

NOTE: The estimates do not include the costs associated with space-based sensors.

a. The Administration has not released estimates for Capability 2 or Capability 3.
b. These estimates for operations show the costs that would be required through fiscal year 2015. They cover different periods of time based on when each level of capability would be initially operational. The estimate for operations for Expanded Capability 1 covers fiscal years 2005 through 2015; Capability 2, 2010 through 2015; and Capability 3, 2011 through 2015.
c. CBO does not include the costs of the low-Earth orbit satellites of the Space-Based Infrared System (SBIRS) in the costs of national missile defense (NMD) because it believes the satellite program will be deployed—even without NMD—to serve other important missions. Nevertheless, SBIRS-low is critical to the performance of Capability 2, especially in determining how that system is structured. Failure to deploy SBIRS-low would either increase the costs of NMD, reduce its effectiveness, or both.

CBO's estimates for national missile defense do not include the costs of any of the SBIRS space-based sensors because, as noted earlier, those satellites will have other important missions besides supporting NMD. For example, SBIRS-high and SBIRS-low will replace some current aging systems and will contribute new capabilities for theater missile defense, intelligence, and possibly other programs. Those additional missions may be sufficient to ensure that SBIRS is funded and deployed even if a national missile defense is not. However, failure to deploy those space-based sensors would render NMD less effective and possibly lead to changes in the system that would increase its costs.

In determining the potential costs of national missile defense, CBO attempted to strike a balance between overestimating and underestimating. As with any new and complex program, NMD's future costs are uncertain for several reasons, including the usual imprecision that accompanies cost estimates, the chance that the system as currently envisioned will not work as planned, and the likelihood that circumstances will change and call for a major redefinition of the program.

Estimates can and often do go awry for any program (such as development of a weapon system) that depends on technology. But programs that are at the cutting edge of technology (such as NMD) or that employ new methods of production introduce more risk than programs that are based on the use of proven technology and well-established production methods. CBO's estimates of NMD costs have been adjusted to reflect those risks. For example, they include probable cost growth that is common to systems with many sophisticated components, such as interceptors and radars.

Changes in the threat that the national missile defense system is designed to counter may also lead to significant changes in the plans and consequent costs for NMD. If the planned system does not accomplish all of its objectives, engineering and other changes could add to its costs. For example, some defense analysts believe that certain countermeasures could render NMD less effective; should those concerns, or others, prove true, the NMD system will most likely need some design changes or equipment upgrades to improve its effectiveness. As a result, the potential for cost increases may be somewhat greater than the potential for declines in total costs. However, CBO does not yet have a sufficient basis to determine the likelihood of significant design or implementation changes or to estimate the corresponding increase in NMD costs.

Expanded Capability 1

Acquiring the Expanded Capability 1 system would cost about $20.9 billion, CBO estimates. Including operations through 2015—if the NMD system stayed at that capability level for that long—would bring total costs to $29.5 billion. Annual operating costs after 2015 would total $600 million (in 2000 dollars).

As Table 2.6 outlines, CBO's estimate for Expanded Capability 1 is $3.9 billion more than the Administration's estimate for the same period because of different assumptions about procurement of NMD components, construction, and operations.

Differing estimates for procurement arise for two reasons. First, CBO believes that in addition to the 100

deployed interceptors, the system would need 82 additional interceptors to use in testing and to replace ones lost in accidents or engagements. The Administration puts the number of additional interceptors at 47. However, CBO's larger figure is more consistent with the experience of previous missile programs. It includes 20 additional interceptors for operational testing and evaluation because CBO assumes that the system will need a total of 30 tests over its first five years of operations. (The Peacekeeper missile program conducted about 20 tests during its initial five years of operations, and the Navy's Trident missile program conducted about 40 tests in its first five years.) In addition, CBO projects that a greater number of spare interceptors (20 instead of five) will be necessary to replace ones that are destroyed during engagements or tests and to allow for unforeseen events such as damage during maintenance. CBO assumes that the NMD system is more like tactical air defenses than strategic missile systems in that after an attack, it would be restored to its former condition—a task that would require spare interceptors. In all, the 35 additional interceptors that CBO includes in Expanded Capability 1 would cost almost $0.6 billion, or about $18 million apiece.

Second, CBO's estimates for procurement are higher because they assume that the Expanded Capability 1 system will experience cost growth comparable to that of both analogous strategic systems (such as the Air Force's Minuteman and Peacekeeper missiles and the Navy's Trident missile) and various tactical systems (such as the Air Force's Advanced Medium-Range Air-to-Air Missile, the Navy's Standard missile, and the Army's Patriot missile). The average growth of production costs for those programs has been about 20 percent compared with projections made at a point in their acquisition cycle similar to where NMD is now. As a result, CBO estimates that such growth will add $0.4 billion to the production costs of interceptors and another $0.4 billion to the combined production costs of the X-band radar, the upgraded early-warning radars, and the command and communications facilities. (Because the Administration's estimate includes about 5 percent for cost growth, CBO's estimate reflects an increase of about 15 percentage points.)

Table 2.6

Costs for Each Level of Capability in the National Missile Defense System

(By fiscal year, in billions of dollars)

	1996-2005	2006-2010	2011-2015	Total, 1996-2015
Expanded Capability 1				
Administration's Estimate	15.5	6.3	3.8	25.6
CBO's Adjustments				
Interceptors	0.4	0.7	*	1.0
X-band radars	0.1	0	0	0.1
Early-warning radars	0.1	0	0	0.1
Command and communications facilities	0.1	*	0	0.2
Test and evaluation	0	0	0	0
System integration	0	0	0	0
Construction	1.0	0	0	1.0
Operational tests	0	1.2	0.3	1.5
Day-to-day operations	0	0	0	0
Operational integration	0	0	0	0

Subtotal	1.7		1.9		0.3		3.9	
CBO's Estimate	17.2		8.1		4.2		29.5	
Capability 2								
Additions for Capability 2								
Interceptors	0		2.4		0		2.4	
X-band radars	0		1.3		0		1.3	
Early-warning radars	0		0		0		0	
Command and communications facilities	0		0		0		0	
Test and evaluation	0		0.7		0		0.7	
System integration	0		0		0		0	
Construction	0		0.3		0		0.3	
Operational tests	0		0		1.0		1.0	
Day-to-day operations	0		0.1		0.4		0.5	
Operational integration	0		0		0		0	
Subtotal	0		4.7		1.4		6.1	
CBO's Estimate	17.2		12.9		5.5		35.6	
	1996-2005		2006-2010		2011-2015		Total, 1996-2015	
Capability 3								
Additions for Capability 3								
Interceptors	0		3.3		0		3.3	
X-band radars	0		2.2		0		2.2	
Early-warning radars	0		0.4		0		0.4	
Command and communications facilities	0		1.2		0.2		1.4	
Test and evaluation	0		0		0		0	
System integration	0		0		0		0	
Construction	0		2.1		0		2.1	
Operational tests	0		0		0		0	
Day-to-day operations	0		0		1.0		1.0	
Operational integration	0		1.0		1.9		2.9	
Subtotal	0		10.2		3.1		13.3	
CBO's Estimate	17.2		23.1		8.6		48.8	

SOURCES: Congressional Budget Office; Department of Defense.

NOTES: These estimates do not include costs associated with the low- or high-orbit versions of the Space-Based Infrared System.

* = less than $50 million.

In the area of construction, CBO estimates that building the necessary facilities would cost some $1.5 billion—or $1 billion more than the Administration estimates. Those construction costs cover the X-band

radar site, command and communications facilities, 100 missile silos, access roads, housing for personnel, and other infrastructure support. CBO's estimate is based primarily on the cost of constructing the Safeguard missile defense site at Grand Forks, North Dakota, in the early 1970s (about $1.5 billion in today's dollars). It also takes into account similar expenses for land-based ICBMs and planning factors from DoD about relative construction costs in different areas of the country.

CBO expects that operating the Expanded Capability 1 system would cost a total of about $8.5 billion through 2015, which is some $1.5 billion more than the Administration estimates for the same period. All of the difference results from CBO's assumption that 30 operational tests will have to be conducted over the first five years rather than the 10 tests that the Administration now plans.

Eventually, operations costs for Expanded Capability 1 will reach a steady-state level of about $600 million a year (in 2000 dollars). Steady-state operations have three main components: day-to-day costs to run the equipment and keep it ready and to staff the command and communications facilities (a total of about $100 million per year); costs for an operational integration program, which would continually upgrade the NMD system to incorporate new technologies ($300 million per year); and the cost to conduct operational tests (about $200 million per year). Those costs are based on information provided to CBO by the Ballistic Missile Defense Organization.

Capability 2

Although the Administration's plan for NMD indicates possibly upgrading Expanded Capability 1 to a more sophisticated Capability 2 system by the end of 2010, the Administration has not estimated the costs associated with that stage of deployment. However, it has specified what the Capability 2 architecture would consist of as well as the areas in which most of the improvements would be made. Based on that information, CBO estimates that upgrading Expanded Capability 1 to Capability 2 would cost $6.1 billion—for a total cost of $35.6 billion for that level of national missile defense (see Tables 2.5 and 2.6).

Although the number of deployed interceptors would remain the same, improving the ability of the Expanded Capability 1 system to handle complex threats (specifically, ballistic missiles with sophisticated countermeasures) would add more than $2 billion to the cost of the interceptors. (The exact technical details of moving from Expanded Capability 1 to Capability 2 have not been announced, but CBO assumes that the budgetary impact would be comparable to that of upgrading the Standard missile to the Block IVA configuration or improving the Patriot missile to the PAC-3 configuration. When those upgrades are complete they will cost $2 billion and $3 billion, in 2000 dollars, respectively.) Moreover, a further 19 interceptors would be needed for integrated flight tests and operational tests, at a cost of slightly more than $0.3 billion, bringing the total increase in interceptor costs to about $2.4 billion.

DoD has indicated that the hardware for the high-resolution X-band radar and the upgraded early-warning radars would not need improvement for Capability 2. But buying three more X-band radars would cost about $1.3 billion, and constructing radar platforms and domes would cost another $0.3 billion ($100 million per radar).

Additional flights to test the upgrades made for Capability 2 would cost about $0.7 billion, CBO estimates. That figure includes seven additional integrated flight tests during 2008 or 2009 (at a cost of about $80 million each) and engineering support. In addition, CBO estimates, 12 more operational tests—which occur after a system has been deployed—would be needed between 2012 through 2014, at a total cost of about $1 billion. Those tests would allow for a rate of six operational tests per year during the first five years of Capability 2's operations.

Finally, moving to Capability 2 would increase the day-to-day operations costs for national missile defense by nearly $100 million a year (to support the three additional X-band radars), or a total of about $0.5 billion. Annual operating costs after 2015 would total $0.7 billion (in 2000 dollars).

The effectiveness of the Capability 2 system depends on the deployment of the SBIRS-low satellites, which, according to the Air Force, will provide the NMD system with 24-hour coverage of global threats.

As mentioned earlier, CBO's estimates for national missile defense do not include the costs of those satellites, even though they are essential to Capability 2's success. Those costs would total nearly $10.6 billion through 2015, CBO estimates—$4.2 billion for research and development, $2.7 billion for purchase of the initial 24 SBIRS-low satellites (about $100 million apiece), $1.1 billion for operations (about $5 million a year per satellite), and $2.7 billion for purchase of replacement satellites (assuming each satellite has an average mission life of about eight years). If SBIRS-low was unavailable for any reason, Capability 2 could be achieved by using faster interceptors, deploying more forward-based radars, and developing more capable "kill vehicles" (the part of the interceptor that hits the incoming warhead). None of those changes or additions are currently planned.

Capability 3

The Administration's plan for Capability 3 of NMD calls for deploying 125 additional interceptors (with Capability 2 sophistication) by 2011, probably in Grand Forks, North Dakota. It also calls for adding 25 interceptors to the site in Alaska, for a combined deployment of 250 interceptors. CBO estimates that moving from Capability 2 to Capability 3 would cost more than $13.3 billion through 2015—or a total of $48.8 billion for that level of national missile defense.

The additional costs would come from several areas. CBO estimates that purchasing 150 more deployed interceptors and 30 more spares would cost about $3.3 billion (nearly $18 million each). Buying five additional X-band radars, stationed both in the United States and abroad, would cost a total of about $2.2 billion. Constructing the radars' platforms and domes would cost another $0.5 billion. In addition, buying an upgraded early-warning radar and deploying it in Asia would cost about $0.4 billion, and building the command and communications facilities would cost about $1.4 billion. Other construction costs at Grand Forks would total about $1.6 billion (equivalent to the Alaskan site).

Adding a second site to the NMD system would increase the costs of both day-to-day operations and operational integration. CBO estimates that daily operations at Grand Forks would cost a total of about $1 billion through 2015, or an average of about $200 million a year. Operational integration at that site would start in 2008 and would total about $2.9 billion. Those estimates for day-to-day operations and operational integration are comparable to the costs at the Alaskan site. Annual operating costs after 2015 would total about $1.1 billion (in 2000 dollars).

The CBO Analysis of Technical Risks and Test and Evaluation

CBO has also provided an important supplement to the reporting by the Welch Panel and the Director of Operational Test and Evaluation of the Department of Defense. It again describes what seems to be a relatively high risk program.[21]

The Flight-Test Program

Past missile development programs do not provide a clear indication of how many developmental flight tests such a program should have. (Those tests are used to remove design flaws that might, for example, prevent the rockets from firing, the cooling system from pumping fluids, or the thrusters from maneuvering the interceptor.) On the whole, more recent programs appear to have conducted fewer developmental flight tests than earlier programs did (see Table 2.7). One possible interpretation of that trend is that the increasing sophistication of ground tests and computer simulations has allowed those types of testing to be substituted for flight tests.

Alternatively, that trend might indicate that familiarity and increasing expertise have allowed DoD to reduce the number of flight tests it needs when it develops new versions of existing missile systems. For instance, Polaris A-2 had fewer flight tests than Polaris A-1, both of which were single-warhead ballistic

missiles. Polaris A-3, however, was the first U.S. missile to have multiple warheads—a significant advance in sophistication—and its development included considerably more flight tests than even Polaris A-1 had. Intercontinental ballistic missiles deployed after 1960 also saw an increase in the number of flight tests for the first multiple-warhead missile (Minuteman III), but not as marked an increase as with the submarine-launched ballistic missiles.

Other missile programs had substantially more developmental flight tests than either ICBMs or submarine-launched missiles did. That fact is particularly striking given that many of those programs also flew "captive carry" tests, in which a number of the weapon's functions can be tested in a realistic environment without the expense of destroying the missile. For example, the guidance and control system of an antiaircraft missile can be tested (the optical system can sense the target, the computer can decide what maneuvers to make, and the missile's fins can be turned in the right direction) while the missile remains attached to an aircraft that flies toward the target.

If the increasing sophistication of ground-testing and computer capabilities is really the cause of recent declines, the 21 developmental test flights scheduled for NMD would appear to be adequate. If, by contrast, the number of test flights that a missile development program needs is mainly a function of the missile's resemblance to previously developed systems, the 21 test flights might be insufficient. In that case, however, estimating how many test flights the NMD program would actually need on the basis of such simple historical precedents would be impossible.

Table 2.7

Comparison of Test Programs for Various Missiles

		Number of Test Flights for Research and Development	
Missile Program	Year of Initial Operational Capability	Single-Warhead Missiles	Multiple-Warhead Missiles
Intercontinental Ballistic Missiles			
Minuteman I	1961	56	n.a.
Minuteman II	1965	20	n.a.
Minuteman III	1970	n.a.	25
Peacekeeper	1986	n.a.	19
Submarine-Launched Ballistic Missiles			
Polaris (A-1)	1960	42	n.a.
Polaris (A-2)	1962	28	n.a.
Polaris (A-3)	1964	n.a.	55
Poseidon (C-3)	1971	n.a.	25
Trident I (C-4)	1979	n.a.	25
Trident II (D-5)	1990	n.a.	28
Other Missiles			
Safeguard Missile Defense	1975	165	n.a.
Standard Missile 2 Block I & II	1981	88	n.a.

Patriot (Air-defense system)	1985		114		n.a.	
Tomahawk (Navy)	1986		74		n.a.	
Advanced Medium-Range Air-to-Air Missile	1991		111		n.a.	
SOURCE: Congressional Budget Office based on information from the Department of Defense and the Federation of American Scientists.						
NOTE: n.a. = not applicable.						

System Development Time

The historical record provides a more straightforward picture of the length of time needed to develop a new weapon system. Several missile and satellite development projects—the Welch Panel pointed to both types as good historical examples for NMD—that a 1997 report by the General Accounting Office listed had an average duration of nearly 13 years.[22] The recent restructuring of the NMD program to deploy a threshold system in late 2005 gives an expected development time of about 10 years, three years shorter than what a "traditional" program might take. (DoD says the current national missile defense program began in 1996.) Of course, that difference does not indicate how changes in the system's architecture, which have been made frequently during the NMD project, affect the schedule. Some analysts would argue that such changes either slow down the program further or add to costs.

Extending the acquisition schedule for the threshold deployment of Capability 1 to the more traditional 13 years—with deployment by the end of 2008—would have some advantages. Perhaps most important, the technology needed to discriminate between decoys and real warheads would have an additional three years to develop. Currently, the Defense Acquisition Board is scheduled to decide in the middle of 2003 whether to procure the interceptors. Moving that date back to 2006 would allow the board to have information from significantly more developmental test flights. Further, when flight-test failures occurred, the tests could be repeated. Some close observers have stressed the importance of repeating such flight tests, with exactly the same mission profiles, to ensure that changes made in response to failures actually worked.

Another significant advantage gained by extending the acquisition schedule would be improved ground tests and simulations, which are constantly evolving. Currently, system integration for NMD is taking place using computer models of important components. Although that situation is to some extent inevitable given the physical constraints of ground tests, the most recent major ground test (conducted between October 12 and 19, 1999) suffered problems because the computer models—not the components they represented—failed to perform up to expectations in the majority of scenarios tested. Extending the acquisition program would allow more time to improve those simulations and reduce the risk that future integrated ground tests would experience similar problems.

The most expensive aspect of switching to a more traditional acquisition schedule—if policymakers decided to do so—would be the additional test flights. Because of uncertainty about how many test flights a "traditional" NMD procurement path might entail, CBO cannot estimate how much such a path might cost. However, if the program was stretched out to 13 years, there would be at least two alternatives for a new flight-test program. One would be to keep the 21 tests currently planned but increase ground testing to make better use of the data gained. Another possibility would be to launch the maximum number of flight tests during the program extension. (Four per year is the current maximum launch rate at the Kwajalein Missile Range, although that number could increase once a second launch facility being built there is finished.) Conducting four flight tests a year for an additional three years might imply an increase in costs of roughly $1.8 billion (half for the tests and half for the added years of system integration). Of course, that number of additional flights is based on launch capacity rather than known need. But some analysts believe that the NMD program would benefit from more flight tests. However, other analysts believe that the recent restructuring of the NMD flight-test program—which increased the number of developmental flights to 21 from 19—is sufficient given the high cost of each test (roughly $80 million).

Parallel Development and Production

One way to meet an urgent defense need is to overlap the development and production of a weapon system. Building such parallel development and production into an acquisition program can have significant advantages in reducing the time required before deployment, lowering costs, and improving management efficiency. It can also cause significant problems, however.

Design problems that require major alterations can come to light after production has started. That was the case with the B-1B bomber. That aircraft was intended to quickly close a perceived "window of vulnerability" in U.S. strategic forces and was authorized to begin production about three years before its developmental testing was scheduled to be completed. However, serious problems were discovered with the bomber's defensive avionics (a system designed to jam or confuse Soviet radars) several years after production began. Some analysts believe that the development and production overlap might have caused, or at least contributed to, those problems.

National missile defense is a highly concurrent acquisition program. The threshold system of 20 interceptors will become operational before the first of the initial operational test and evaluation (IOT&E) flights takes place in 2006. In fact, the Administration's schedule for NMD would purchase all of the interceptors and boosters needed for Expanded Capability 1 before the first IOT&E flight.

Although national missile defense is an extreme example of production overlapping development, other major missile programs have had significant overlap. For instance, production of the Peacekeeper missile was approved a year and a half before IOT&E started. Furthermore, Peacekeeper became operational only 15 months after that first operational test. Initial deployment of Peacekeeper was followed by more than two years of further initial operational testing. The Trident II missile program was also highly concurrent, with a production decision almost two years before the first performance evaluation test flight. However, Trident II completed those test flights a month before reaching initial operational capability.

Although some analysts would argue that the threat of attack from ballistic missiles justifies such concurrent development and production of NMD, it does entail significant risks. For example, as noted earlier, the Welch Panel says that the booster planned for actual operations will subject the kill vehicle to 10 times more high-frequency vibrations than the rocket used on all of the test flights so far. The increased vibrations could conceivably distort or damage the kill vehicle's optics or electronics, rendering the interceptor impotent.

If that occurred—and it is by no means certain—one possible solution might be to change the structure supporting the kill vehicle on the booster. That in turn could add so much weight that the booster would need to be redesigned. Following that worst-case scenario to a logical conclusion, the silos meant to house the system might also need to be enlarged. However, silo construction would begin in the spring of 2002 to be ready for threshold deployment by the end of 2005. A decision about silo construction in turn is tied to the deployment readiness review scheduled for July.

III. Total Spending on Counterterrorism, Defense Against Asymmetric Warfare, and Critical Infrastructure Protection: The OMB Analysis

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 of 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.[23]

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,[24]

> 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.[25]

The US is also giving significantly higher priority to the full range of threats post 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.

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 reports 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 Rapid Assessment and Initial Detection (RAID), teams throughout the country. 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 25 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 a currently definitional and statistical nightmare, and is filled with conflicting bureaucratic rivalries and priorities.

It is clear, however, that major increases are taking place. 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 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.[26] 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.[27]

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:[28]

> 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:[29]

- *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.[30] . 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.[31]

> 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.[32] 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 Monterrey Institute Estimate

The rise in federal spending has led to something of a feeding frenzy within federal departments and agencies, and is has become the fashion to label programs as counterterrorism,

weapons of mass destruction related, or as critical infrastructure protection. At the same time, few agencies provide any detailed figures on the trends in their budget that allow for independent analysis of where the money is really going, or which permit more detailed breakouts than those contained in the previous White House analysis of the FY2000 request.

It should be noted that this lack of transparency is scarcely unusual. Most federal agencies report a line item budget, and provide little detail on how money is allocated by program or function. Reporting is long on the reason for programs, but short or non-existent on actual expenditure levels, program goals, and program achievements. The use of the Internet has not helped in this regard. Federal web pages are largely an exercise in public relations or vanity that provides little substantive insight into what the federal government is actually doing and spending.

The Monterrey Institute did, however, issued a private estimate of both total federal spending and spending by agency in 1999. The patterns in total federal spending are shown in Table 3.1. These figures differ somewhat from those used by the NSC, but provide useful further background on the level of the federal effort. It shows a growth from $6.7 billion in FY1997 to $10.0 billion in FY2000, a growth of 50% in four years.

Table 3.1

Monterrey Institute Estimate of Total Federal Spending on Terrorism (As of 1999)

Government-wide	**FY 1997[^] ($ million)**	**FY 1998[^] [+] ($ million)**	**FY 1999[^] ($ million)**	**FY 2000[^] (requested) ($ million)**
Federal Government (Total)	**$6,700**	**$6,500**	**$9,647**	**$10,000**
Combat WMD missions (total)			$1,227	$1,385
Law enforcement & investigative activities		$2,357	$2,937	$2,757
WMD figure for the above function			$87	$87
Preparing for & responding to terrorist acts		$654	$1,233	$1,302
WMD figure for the above function			$629	$664
Public health infrastructure/surveillance			$44	$65
Stockpile vaccines, antidotes, antibiotics			$51	$53
Planning/exercises			$24	$22
Training of first responders			$90	$87
Protective equipment for first responders			$101	$95
WMD detection equipment			$105	$128
State & local planning and assistance			$113	$123
Other			$101	$91
Physical security of govt. facilities/employees		$2,978	$4,600	$3,504
WMD figure for the above function			$223	$206
Physical protection of natl. pop/infrastructure		$333	$454	$472
WMD figure for the above function			$30	$28
Research and Development		$197	$423	$577
WMD figure for the above function			$258	$400
Pathogen genome sequencing			$16	$28
Vaccines/Therapeutics			$9	$50
Detection/Diagnostics			$23	$58
Personal & environmental decontamination			$2	$15
Modeling, simulation, systems analyses			$4	$8
Other			$204	$241

Source: http://cns.miis.edu/research/cbw/terfund.htm

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 3.2 and Charts 3.1 to 3.3 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

At same time, a review of Table 3.2, and Thirteen and Charts 3.1 to T3.3, shows the following 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 million to $3.0 billion. This latter rise was still quire 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 the threat posed to the US homeland. As a result, they give a somewhat misleading view of how the US is dealing with 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 can be equally misleading. 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 Clinton Administration has stated that efforts are being made 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 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.

While it is easy to talk about creating a coordinated federal plan, and efficiently programming resources accordingly, 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 from the more detailed analyses of agency and departmental efforts that follows.

More importantly, however, the threat simply is not predictable enough to attempt more than a constantly evolving and extremely 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.

Furthermore, it is far from clear that the federal programs identified as being directly designed to deal with the threat state actors, their proxies, or independent extremists and terrorists pose to the American homeland will always prove to be the most effective programs in

actually improving Homeland defense. This particularly true given the role of US military and intelligence activities overseas play in creating an effective deterrent to foreign attacks on the US.

Table 3.2

OMB Estimate of Total Federal Spending on Terrorism and CIP (As of 6/2000)

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

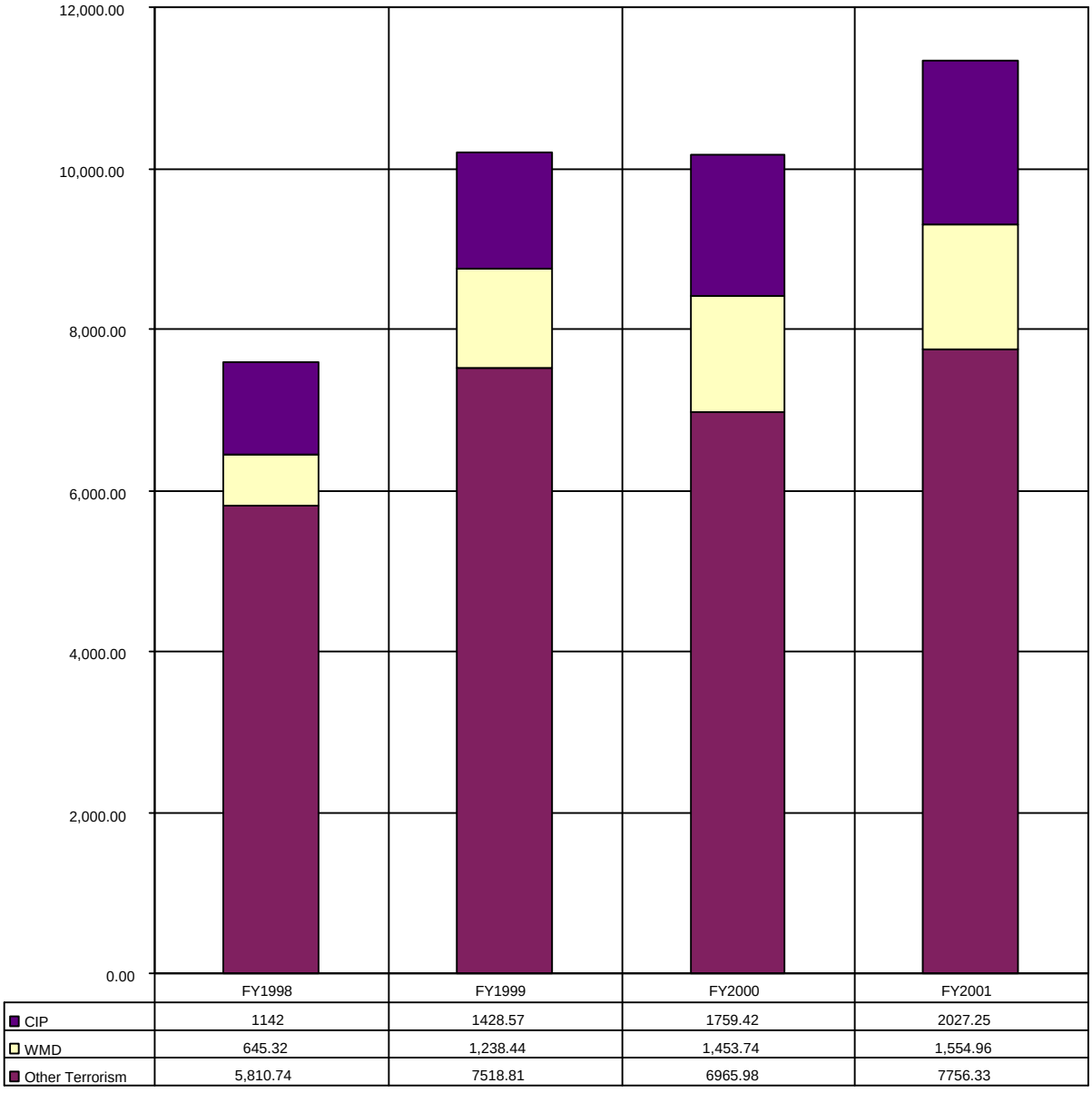
	FY1998	FY1999	FY2000	FY2001
Federal Government	*8,303.40*	*11,424.26*	*11,632.88*	*12,893.50*
Combat Terrorism	6,516.08	8,757.25	8,419.72	9,311.29
Law Enforcement and Investigative Activities	2,654.72	2,686.77	2,820.04	3,025.51
Physical Security of Government Facilities and Employees	2,893.72	4,356.44	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
WMD Preparedness	*645.32*	*1,238.44*	*1,453.74*	*1,554.96*
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
Critical Infrastructure Protection	*1,142.00*	*1,428.57*	*1,759.42*	*2,027.25*
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 3.1

Federal Spending on Terrorism, WMD, and CIP by Category: FY1998-FY2001

(Current $US Millions)



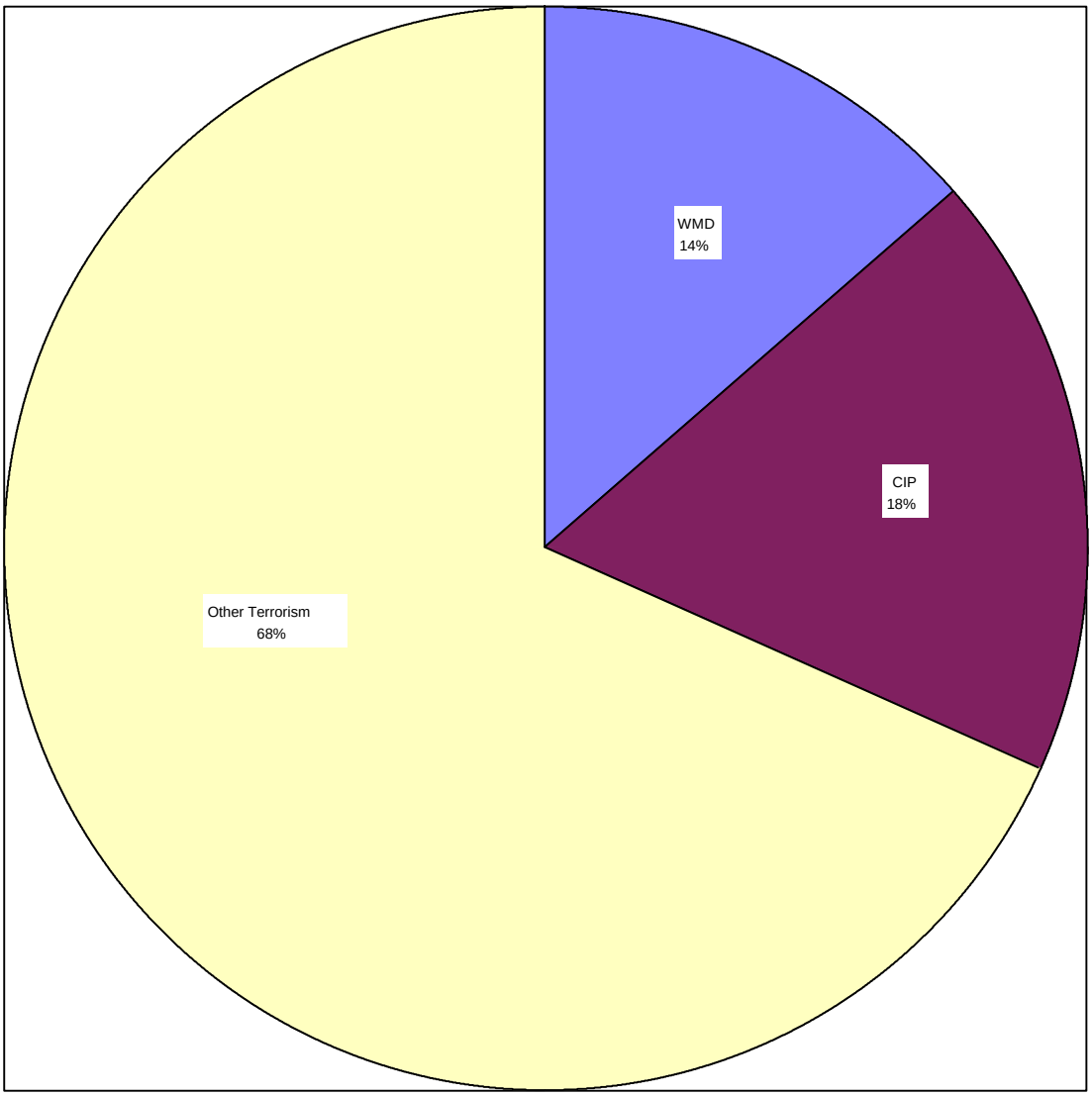
	FY1998	FY1999	FY2000	FY2001
CIP	1142	1428.57	1759.42	2027.25
WMD	645.32	1,238.44	1,453.74	1,554.96
Other Terrorism	5,810.74	7518.81	6965.98	7756.33

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

Chart 3.2

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

(Current $US Millions)

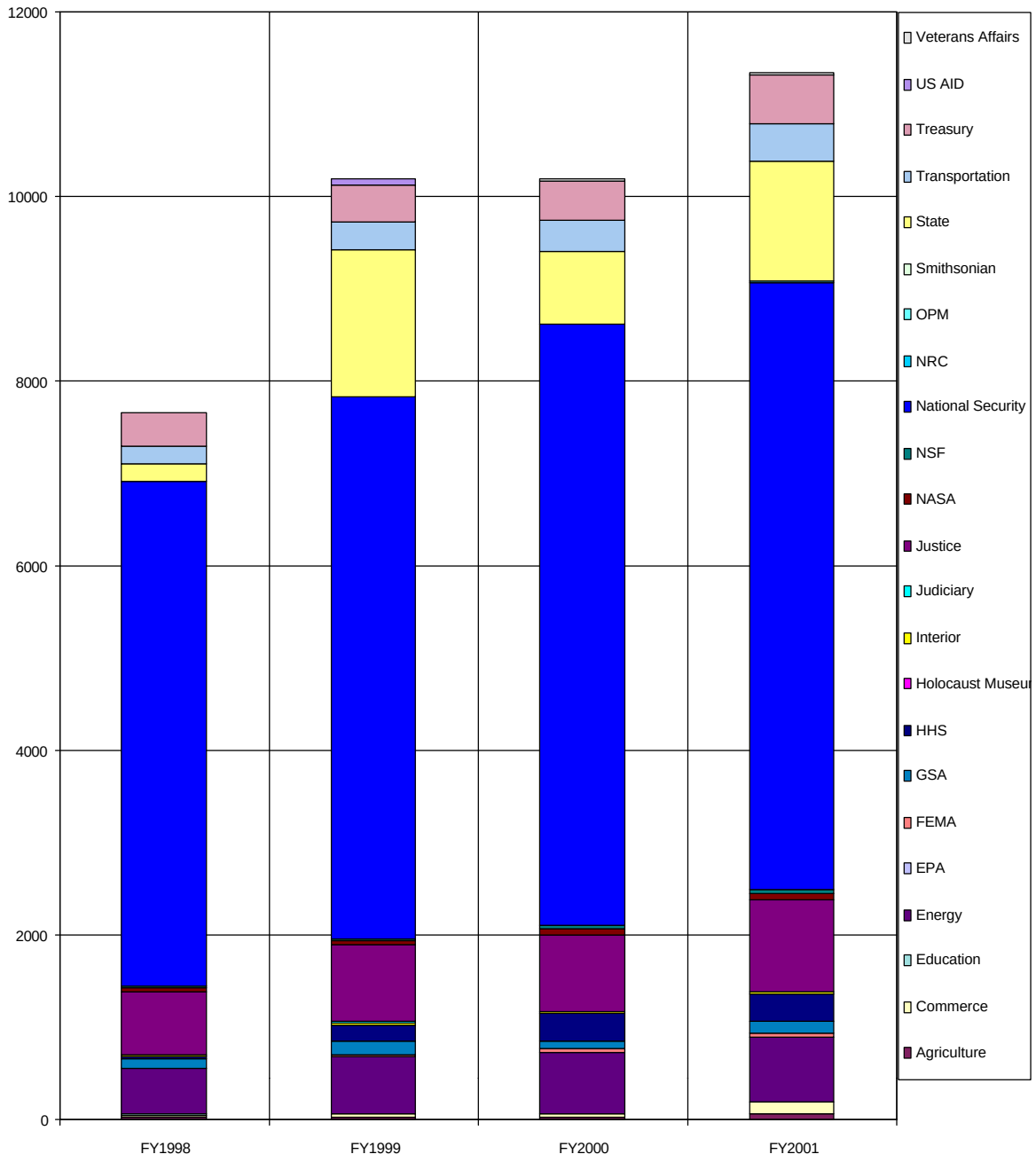


Source: Adapted by Anthony H. Cordesman

Chart 3.3

Federal Spending on Terrorism, WMD, and CIP by Agency: FY1998-FY2001 – Part One

(Current $US Millions)



Source: Adapted by Anthony H. Cordesman

Chart 3.3

Federal Spending on Terrorism, WMD, and CIP by Agency: FY1998-FY2001 – Part Two

(Current $US Millions)

	FY1998	FY1999	FY2000	FY2001
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

Total Spending on State and Independent Terrorism versus Homeland Defense

Nevertheless, the US must try to use those resources it does dedicate to countering terrorism as efficiently as possible. Chart 3.4 shows the patterns in these expenditures, less expenditures on CIP. 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.

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 founding, 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

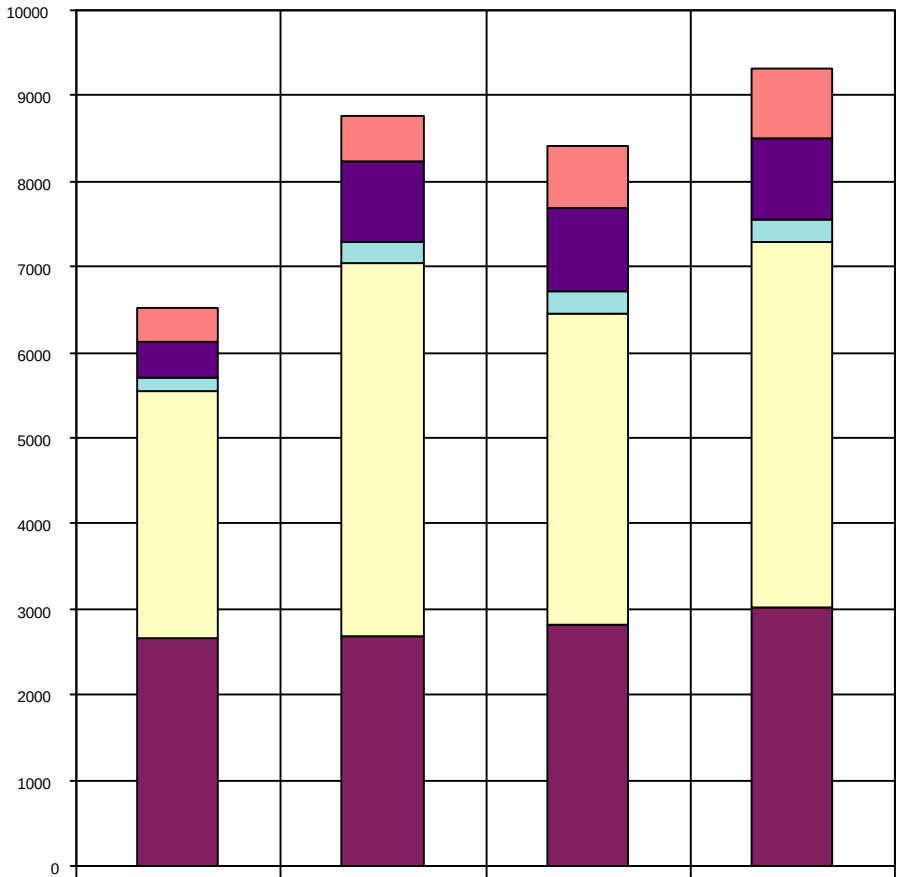
Much of the activity in both anti-terrorism and counter-terrorism affects world wide federal activities. Accordingly, Charts 3.5 and 3.6 provide a different breakout of the patterns in total federal spending on terrorism. They eliminate spending on activities like critical infrastructure protection and 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 shown 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 3.4

Federal Spending on Terrorism and WMD by Category: FY1998-FY2001

(Current $US Millions)



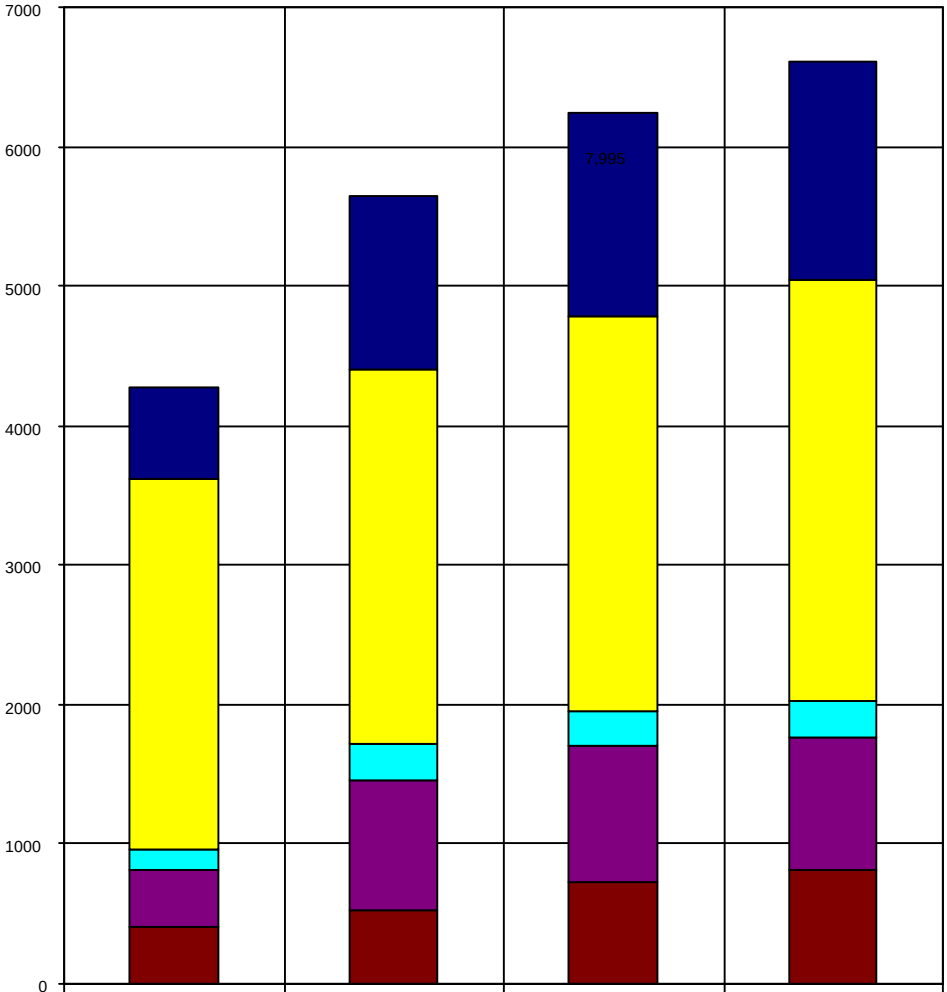
	FY1998	FY1999	FY2000	FY2001
Research and Development	403.14	527.01	727.91	812.79
Preparing for and Responding to Terrorist Acts	417.84	930.21	984.41	947
Physical Security of National Populace	146.66	256.83	249.96	266.76
Physical Security of Gov. Facilities and Employees	2,893.72	4,356.44	3,637.49	4,259.24
Law Enforcement & Investigative	2654.72	2686.77	2,820.04	3,025.51
TOTAL	*6,516.08	*8,757.25	*8,419.72	*9,311.29

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

Chart 3.5

Core Federal Spending on Terrorism and WMD by Activity: FY1998-FY2001:

(Current $US Millions)

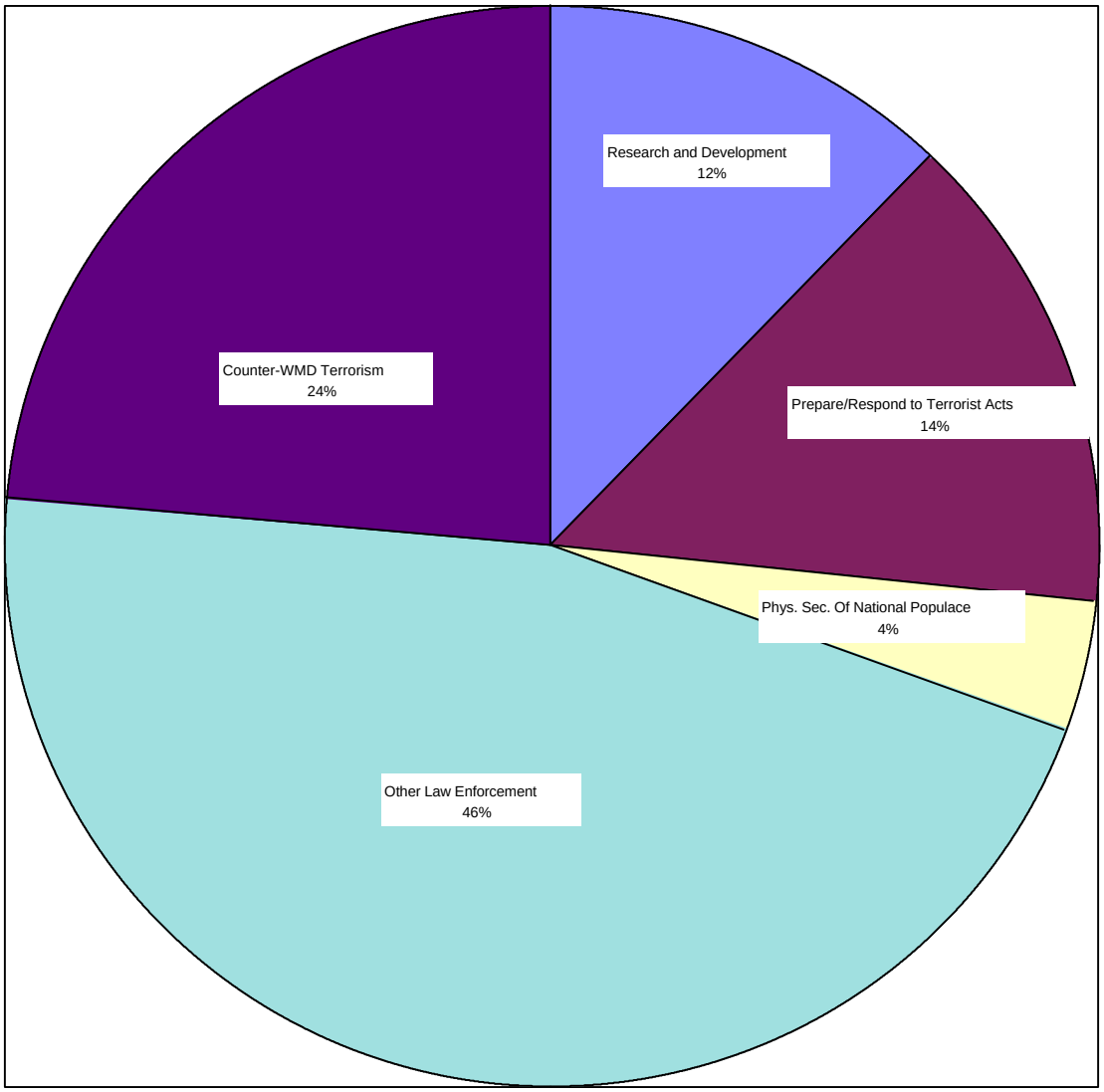


	FY1998	FY1999	FY2000	FY2001
*TOTAL	*4.267.68	*5,639.27	*6,235.36	*6,607.02
Counter-WMD Terrorism	645.32	1,238.44	1,453.74	1,554.96
Other Law Enforcement	2654.72	2686.777	2,820.44	3,025.51
Phys. Sec. Of National Populace	146.66	256.83	248.86	266.76
Prepare/Respond to Terrorist Acts	417.84	930.21	984.41	947
Research and Development	403.14	527.01	727.91	812.79

Source: Adapted by Anthony H. Cordesman

Chart 3.6

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



Source: Adapted by Anthony H. Cordesman

Spending on Preparedness for Attacks Using Weapons of Mass Destruction

Only a relatively small number of federal programs are dedicated specifically to domestic defense and response 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 3.7 and 3.8. 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 3.8 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.

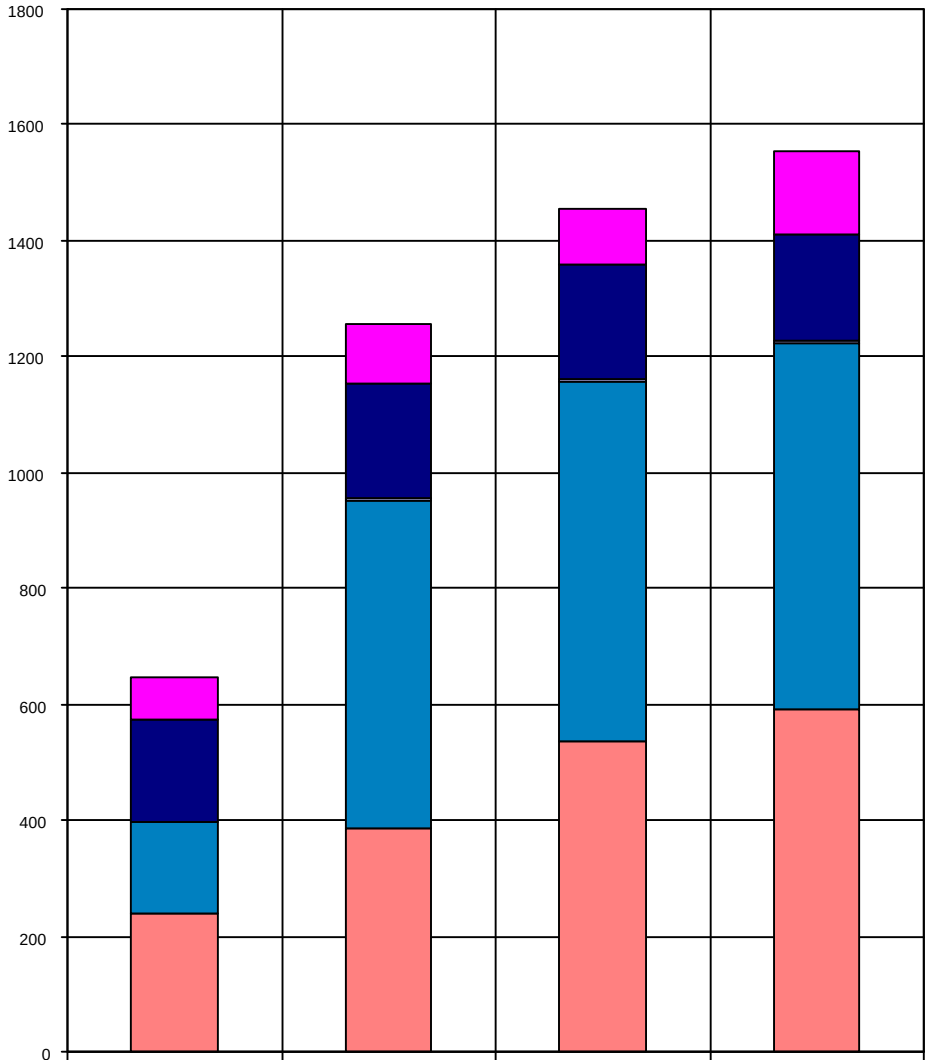
These efforts require an exceptional degree of interagency coordination, which is the responsibility of the White House Office of Science and Technology Policy, and which chairs an interagency working group to determine vulnerabilities and shortfalls in the US effort to mitigate or respond to WMD, determines 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 3.7

Federal Spending on WMD Preparedness by Activity: FY1998-FY20001

(Current $US Millions)



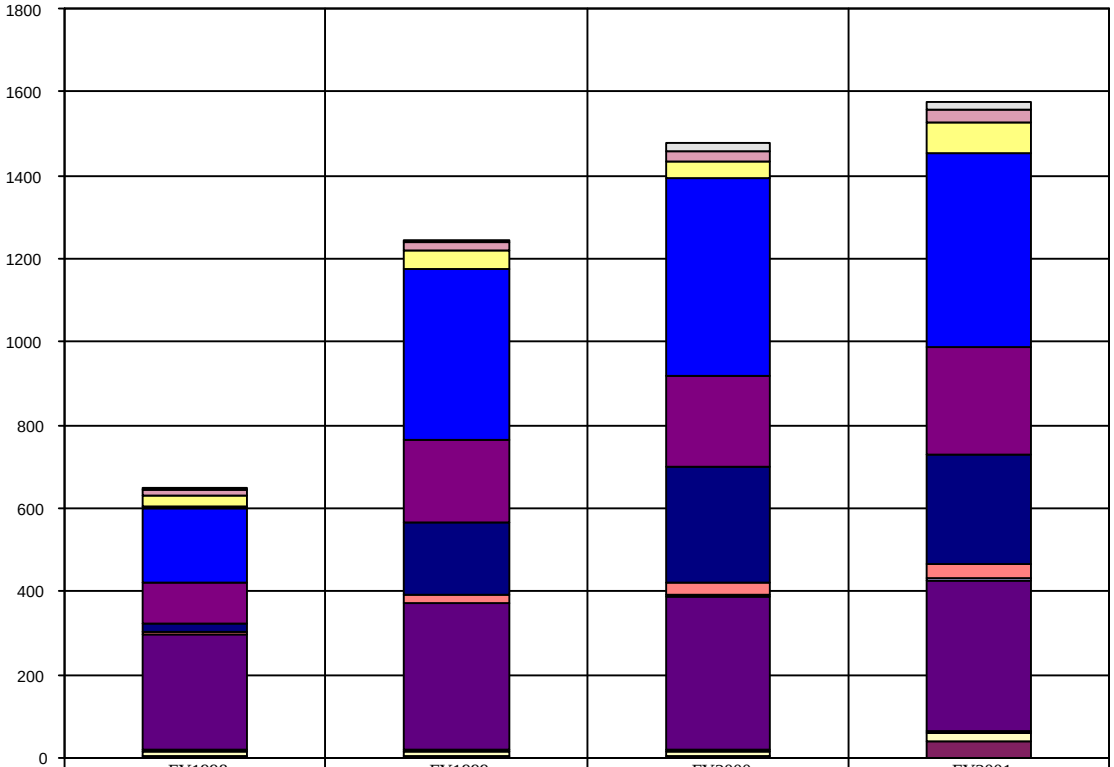
	FY1998	FY1999	FY2000	FY2001
Law Enforcement and Investigation	71.82	102.3	93.77	142.53
Physical Security of Government	175.09	199.35	200.58	185.41
Security of National Populace	3.39	3.83	3.61	3.62
Prepare & Respond to WMD Terrorism	155.26	564.2	618.74	633.48
Research and Development	239.75	386.76	537.04	589.92

Source: Adapted by Anthony H. Cordesman

Chart 3.8

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

(Current $US Millions)



	FY1998	FY1999	FY2000	FY2001
Veterans Affairs	0.1	0.04	17.33	17.39
US AID	3	1.4	1.4	2.35
Treasury	18.01	19.46	25.87	25.87
Transportation	0	0	0.45	2.5
State	23	46	37	72
NRC	3.04	2.79	2.79	2.79
National Security	180.56	408.15	475.82	467.21
Justice	100.8	201.22	217.18	254.66
Interior	0.22	0.25	0.27	0.27
HHS	15.9	173.12	277.56	265.37
FEMA	5.92	17.61	30.77	34.52
EPA	2	2	2	3.2
Energy	275.78	350.75	366.61	364.23
Education	3.59	4.45	5.23	2.51
Commerce	11.9	9	9	20.2
Agriculture	5.2	6.7	7.33	39.8

Source: Adapted by Anthony H. Cordesman

Chart 3.8

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

(Current $US Millions)

	FY1998	FY1999	FY2000	FY2001
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

IV. US Government Efforts to Create a Homeland Defense Capability to Deal with Asymmetric and Terrorist Attacks Using CBRN Weapons

Chart 4.1 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, 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 founding, 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

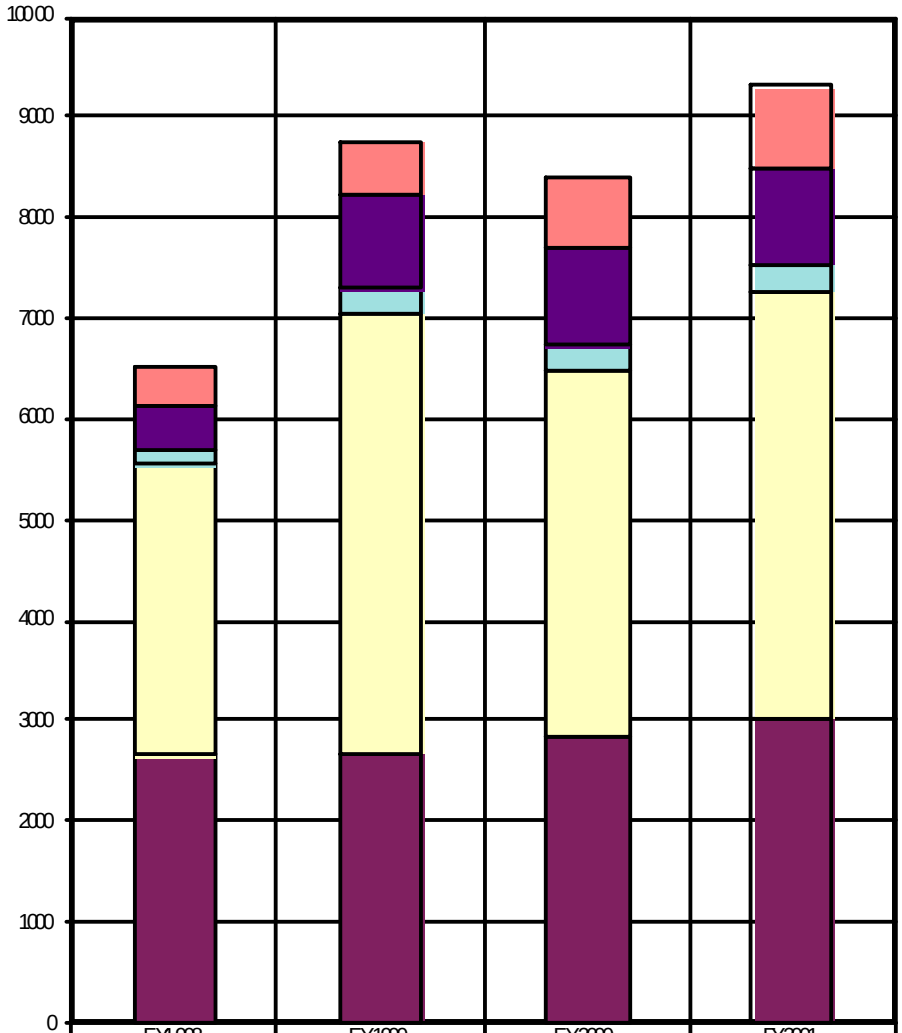
Much of the activity in both anti-terrorism and counter-terrorism affects world-wide federal activities. Accordingly, Charts 4.2 and 4.3 provide a different breakout of the patterns in total federal spending on terrorism. They eliminate spending on activities like critical infrastructure protection and show only the core federal spending on threats by 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 46 percent of the total for CIP, WMD, and other terrorism, and 56 percent of the total for WMD, and other terrorism. At the same time, they are still considerable. "Core spending" increased from $3,797.46 million in FY1998 to $5,237.47 million in FY2001, or by 38 percent. This involved a 141% increase in spending to deal with weapons of mass destruction, and a more than 36% increase in related research and development activity. They also involved a 12% increase in other law enforcement and investigation activities, a 19% 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 4.1

Federal Spending on Terrorism and WMD by Category: FY1998-FY2001

(Current $US Millions)



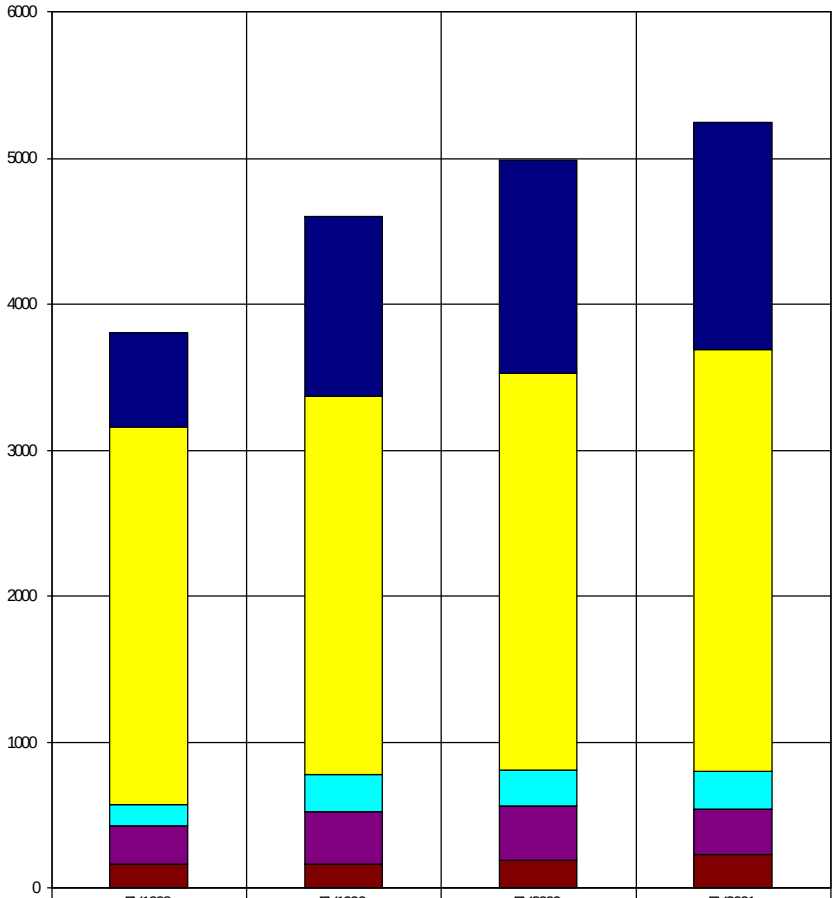
	FY1998	FY1999	FY2000	FY2001
Research and Development	403.14	527.01	727.91	812.79
Preparing for and Responding to Terrorist Acts	417.84	930.21	984.41	9.47
Physical Security of National Populace	146.66	256.83	249.96	266.76
Physical Security of Gov. Facilities and Employees	2,893.72	4,356.44	3,637.49	4,259.24
Law Enforcement & Investigative	265.472	268.677	2,820.04	3,025.51
TOTAL	*6,516.08	*8,757.25	*8,419.72	*9,311.29

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 4.2

Core Federal Spending on Terrorism and WMD by Activity: FY1998-FY2001

(Current $US Millions)



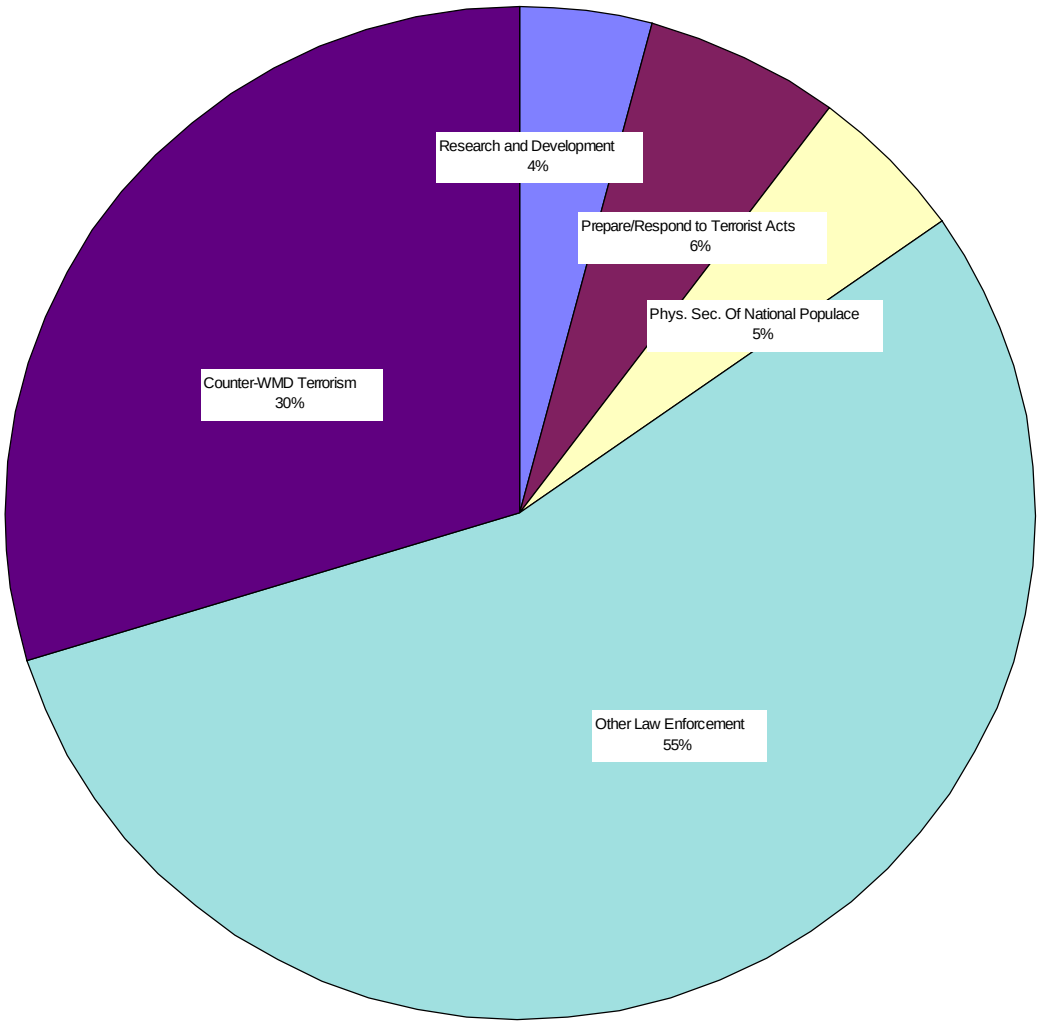
	FY1998	FY1999	FY2000	FY2001
*TOTAL	*3,797.46	*4,600.17	*4,982.80	*5,237.47
Counter-WMD Terrorism	645.32	1,238.44	1,453.74	1,554.96
Other Law Enforcement	2,582.90	2,584.47	2,726.27	2,882.98
Phys. Sec. Of National Populace	143.27	253	246.25	263.14
Prepare/Respond to Terrorist Acts	262.58	366.01	365.67	313.52
Research and Development	163.39	158.25	190.87	222.87

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 4.3

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 are 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 4.4 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. The State Department 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-62 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. There 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 US 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-related materials.

WMD Counterterrorism

The majority of WMD counterterrorism resources fall into two main categories within the national security community. 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, which accounts for most of the increase over FY2001. The other funding in this area is for 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:

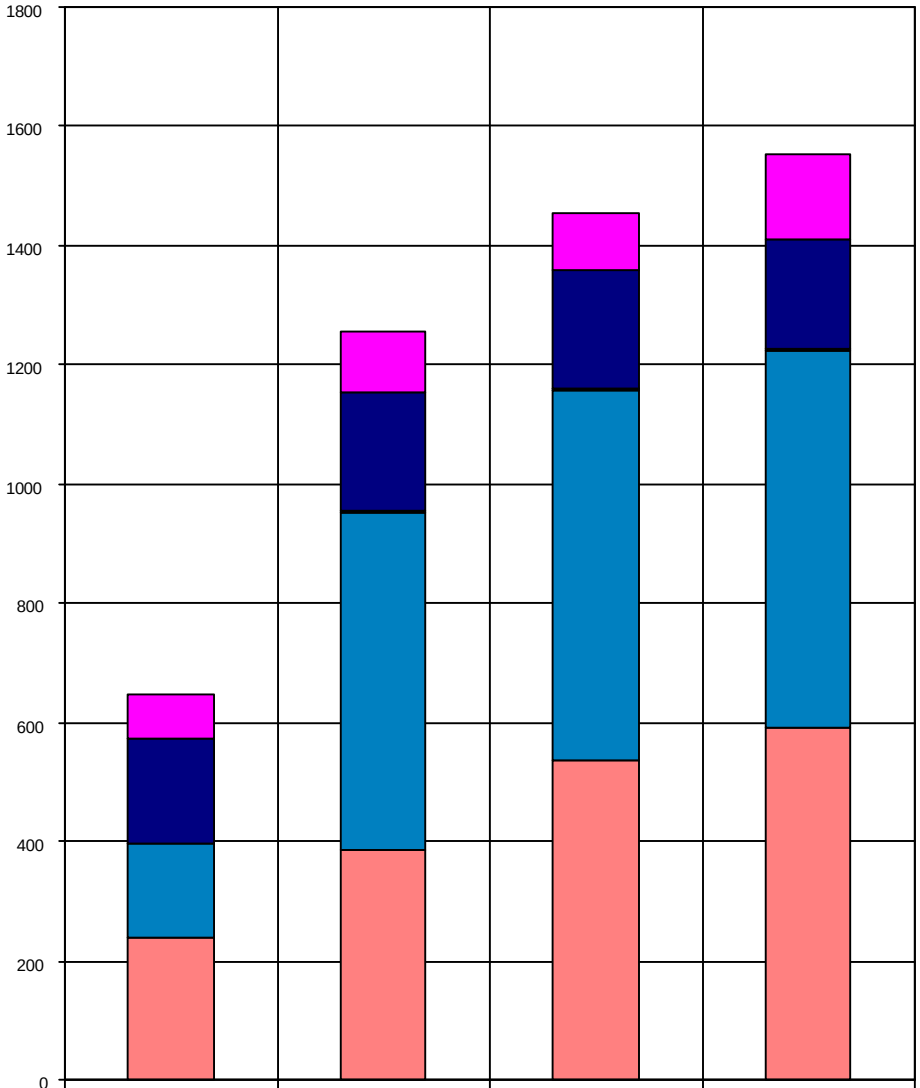
- Preventing or forestalling the release of a WMD payload.
- Detecting and responding to a threatened or actual release.
- Managing the health, environmental, and law enforcement consequences of such an incident.

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

Chart 4.4

Federal Spending on WMD Preparedness by Activity: FY1998-FY20001

(Current $US Millions)

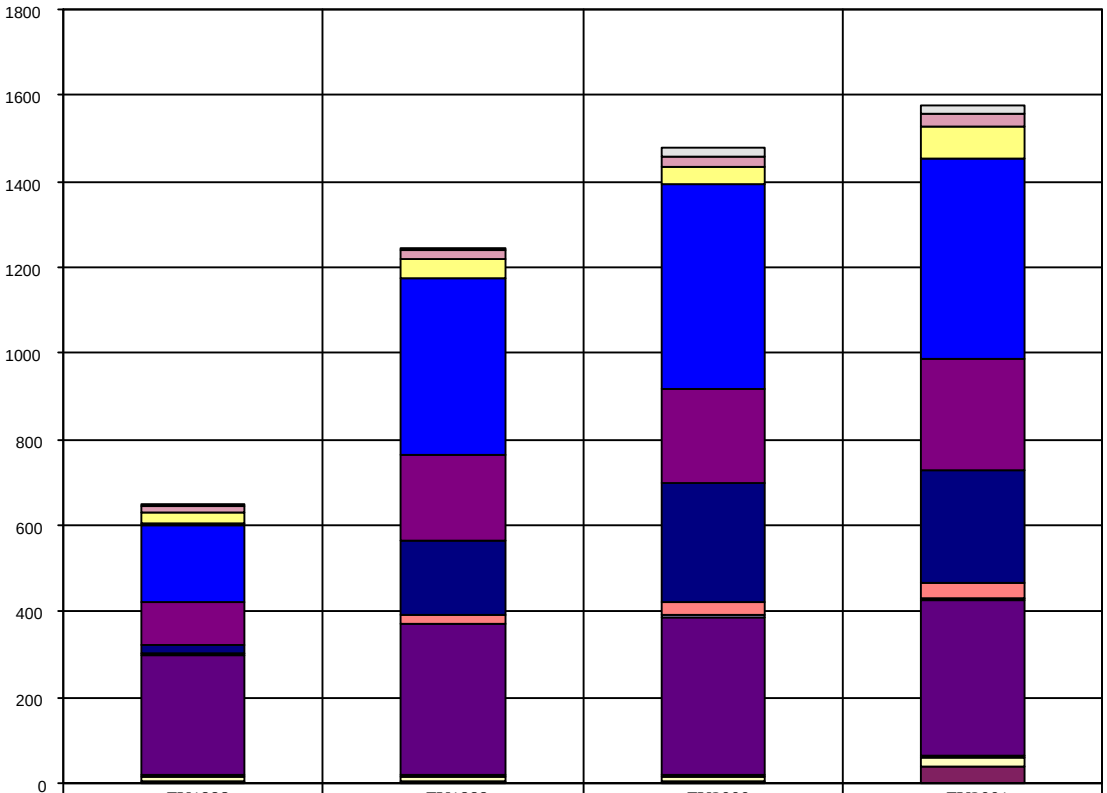


	FY1998	FY1999	FY2000	FY2001
Law Enforcement and Investigation	71.82	102.3	93.77	142.53
Physical Security of Government	175.09	199.35	200.58	185.41
Security of National Populace	3.39	3.83	3.61	3.62
Prepare & Respond to WMD Terrorism	155.26	564.2	618.74	633.48
Research and Development	239.75	386.76	537.04	589.92

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 4.5

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



	FY1998	FY1999	FY2000	FY2001
Veterans Affairs	0.1	0.04	17.33	17.39
US AID	3	1.4	1.4	2.35
Treasury	18.01	19.46	25.87	25.87
Transportation	0	0	0.45	2.5
State	23	46	37	72
NRC	3.04	2.79	2.79	2.79
National Securit	180.56	408.15	475.82	467.21
Justice	100.8	201.22	217.18	254.66
Interior	0.22	0.25	0.27	0.27
HHS	15.9	173.12	277.56	265.37
FEMA	5.92	17.61	30.77	34.52
EPA	2	2	2	3.2
Energy	275.78	350.75	366.61	364.23
Education	3.59	4.45	5.23	2.51
Commerce	11.9	9	9	20.2
Agriculture	5.2	6.7	7.33	39.8

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 4.5

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

(Current $US Millions)

	FY1998	FY1999	FY2000	FY2001
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 to Defend Against Asymmetric and Terrorist Attacks 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. 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 what degree 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 OMB data are shown in Table 4.2. 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 4.2

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				
Combat Terrorism	**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				
Combat Terrorism	**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
WMD Preparedness	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				
Combat Terrorism	**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
WMD Preparedness	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				
Combat Terrorism	**2.00**	**2.00**	**2.00**	**3.20**
Preparing for and Responding to Terrorist Acts	2.00	2.00	2.00	3.20
WMD Preparedness	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				
Combat Terrorism	**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

WMD Preparedness	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				
Combat Terrorism	**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				
Combat Terrorism	**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
WMD Preparedness	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				
Combat Terrorism	**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**
Combat Terrorism	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				
Combat Terrorism	**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				
Combat Terrorism	**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
WMD Preparedness	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				
Combat Terrorism	**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
WMD Preparedness	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				
Combat Terrorism	**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
WMD Preparedness	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
Smithsonian				
Combat Terrorism	**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				
Combat Terrorism	**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
WMD Preparedness	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				
WMD Programs				
Embassy Security	-	-	-	1200.00
Anti-Terrorism Assistance Program	-	-	-	64.00
Terrorism Interdiction Program	-	-	-	4.00

Department of Transportation				
Combat Terrorism	**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
WMD Preparedness	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
*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				
Combat Terrorism	**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				
WMD Programs				
Air Security Protective Operations	-	-	-	16.00
CIP Programs				
Research and Development	-	-	-	4.00
Public Key Infrastructure	-	-	-	7.00
US AID				
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
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				
Combat Terrorism	**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.[33]

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 Operations Center provides leadership for national plant and animal health emergencies.[34]

The following table 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.[35]

Table 4.3

Department of Agriculture Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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				
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

Intelligence plays a critical role in counterterrorism. As Brent Scowcroft, a former national security adviser under Presidents Ford and Bush, has said,[36]

> Prevention, not defense, should be at the heart of any terrorism strategy, and its primary instrument is intelligence operations. If we can penetrate terrorist operations and anticipate their moves, we can at least keep them off balance and frequently prevent terrorist acts. In the end, an offensive strategy designed to prevent and disrupt terrorist activities by funding our intelligence agencies rather than construction contractors is the surest way to provide security for all American citizens abroad--and in the United States as well.

OMB 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:[37]

> 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.

The National Commission on Terrorism, also known as the Bremer Commission, has recommended that the CIA take a more aggressive role in recruiting informants and collecting information. The Bremer Commission criticized 1995 guidelines that set up a complicated approval process to recruit informants whom may have committed human rights violations. The Commission recommended that the CIA stop using the 1995 guidelines and revert to the pre-existing process when recruiting terrorist informants. The Commission also noted that the Counterterrorist Center (CTC) is underfunded. As a result, the CTC has had to cut back planned operations. The Commission recommended that the CIA work with Congress to insure the CTC has adequate resources. The Commission also believed that the CIA, through its Foreign Language Executive Committee, needs the authority to expand the pool of linguists available to the US Government to create a surge capability. The Commission did have praise for the CIA by saying the FBI should have reports officers like the CIA. Reports officers' primary mission is to determine what information should be shared with other agencies.[38]

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 table adapted from the 2000 OMB counterterrorism funding report.[39] FY 2001 requested funding for WMD preparedness includes an increase of $11.2 million towards WMD preparedness.

Table 4.4

Department of Commerce Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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
WMD Preparedness	**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

The current role of the Department of Defense (DOD) in defending and responding to counterterrorism is something of an anomaly, and highlights the gap between classic national defense roles like missile defense and the current approach to counterterrorism. DoD is responsible for the development of a national missile defense system. At present, however, there is no clearly defined mission for the Department in dealing with response to a catastrophic event like a successful missile penetration and strike on a US target. Similarly the Department plans for asymmetric attacks by states, their proxies, and major terrorist groups using nuclear or highly lethal biological weapons, but has largely sought to avoid being integrated into the defense and response effort for such highly level attacks because of its fear that (a) it would be forced to fund the mission with existing resources, (b) would see its primary missions diluted, and (c) would be dragged into a political morass in dealing with the interagency process and Congress.

As a result, the Department is charged with supporting the FBI or FEMA in a terrorism crisis and has no lead designation. This may be appropriate when states or their proxies are not involved in an attack, and when it is an isolated incident that does not require a state of national emergency. It is a potential recipe for failure, however, at higher levels of attack. It highlights the

de facto gap between the current focus civil agencies have on relatively low levels of terrorist attack and the very different threat that could occur from overt or covert state or state sponsored attacks.

It is also unclear that the present arrangements are really adequate even for dealiing with terrorist attacks. The National Commission on Terrorism, also known as the Bremer Commission, recommended that the DOD be the lead agency if a catastrophic terrorist event overwhelms the capabilities of other federal agencies. The Commission advised the creation of contingency plans in case a devastating terrorist event forced the DOD to take the lead and advised the Secretary of Defense to create a unified command structure to prepare the DOD for the lead role. The Commission said:[40]

> 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 Bremer Commission further recommended that increased funding for the National Security Agency to allow the NSA to close technology gaps and to ensure that the NSA has the capability to collect terrorist information.[41] This recommendation not only seems sound, it is crucial if the US is to prepare effectively for the future spectrum of attacks on the US homeland,

close the present gap between NMD and counterterrorism, and prepare for complex forms of asymmetric attack that could combine covert attacks with weapons of mass destruction and new forms of attack like cyberwarfare. It is also essential if homeland defense is to be treated as part of war fighting, rather than a largely passive and defense activity. The failure to plan for events like multiple, near simultaneous biological attacks using multiple agents is one case in point. So is the tendency to limit the examination of cyberwarfare and CIP attacks to limited acts of terrorism rather than fully examine vulnerability and response in the case of large-scale state sponsored attacks or actual war.

Analyzing the Role of the Department of Defense

There are other major problems in analyzing the role of the Department of Defense, and the national security community as a whole. At present, most reporting is designed to cover a highly compartmented definition of counterterrorism activity that excludes three basic elements of the problem. It does not include most counterproliferation activities. It does not include an analysis of asymmetric warfare capabilities. And, it does not include large-scale cyber and information warfare. There also is no way to know what resources the Department is being given that could be used for responding to a large-scale attack or in a national emergency.

In practice, however, the Department must play a critical role in defending the US against foreign attacks, in intelligence, in counterterrorism, and in responding to CBRN attacks. In fact, the Department is anything but consistent in its approach to looking at this aspect of the problem. The Secretary of Defense announced the Defense Counterproliferation Initiative in 1993 to combat the CBRN threat. This Initiative called 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 reported on the progress DOD has made in implementing the Initiative in May 2000:[42]

> 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.

A broader recommendation is needed. Homeland defense is not simply NMD, counterterrorism, and information security. It involves a much broader matrix of national security efforts. Effectively planning and analysis requires a full understanding of the overall nature of DoD and other national security efforts in this area and regardless of past PDDs, and the work of the NSC, the federal government at present lacks even a raw conceptual picture of its current plans, capabilities, and spending.

The Size of the Current Department of Defense Effort

Although the Department of Defense pioneered program budgeting and the development of future year plans, its program is even more opaque and lacking in any public evidence of long term planning than that of any civil agency – although problem far more for security reasons than from a lack of confidence.

The OMB report to Congress on the Federal budget does not provide specific budget figures, or program descriptions, for the Department of Defense. Instead, the DoD is included as part of the OMB totals for "National Security." One major recommendation for improving future efforts to coordinate Homeland defense is that OMB be tasked with providing future reporting by federal agency, and that any sensitive figures on black programs either be rolled into other DoD

programs or put into some general intelligence or “other agency” heading that could include NSA and CIA.

In general, OMB seems to have a tendency to grossly overclassify broad categories of data in the national security area which made little real sense during the Cold War and which make no sense in a context where enough data have to be declassified to allow effective government-wide planning. The present system of OMB reporting almost seems to be designed avoid effective review by the NSC and Congress, much less any outside experts.

Table 4.5

National Security for Combating Terrorism and WMD Preparedness

National Security	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	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
WMD Preparedness	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

The Department of Defense does, however, prepare a separate unclassified report called "combating terrorism activities." This report makes no effort to distinguish between domestic and foreign activities, but it does make an interesting contrast with the OMB report. The DoD estimate of National Security spending is shown in Table 4.6 below. Chart 4.6 shows the trends in total DoD spending by major program activity, and compares them to the OMB estimate of total national security spending for the same activities. It also compares the OMB estimate of total spending on WMD programs against an estimate of similar spending for FY2001 based on

the DoD data.

The Department of Defense report that explains Table 4.6 again seems almost to be designed to be confusing and limit effective review.[43] It provides no future year or program planning data, and covers only three fiscal years, There are no trend analyses, and the resource analysis are heavily concentrated on service and agency data in ways where it becomes almost impossible to distinguish overall activities by function. In fairness, this is almost certainly a response to the Congress's insistence on reviewing a somewhat archaic "line item" annualized budget, rather than programs. The Department also does provide enough functional data to get a rough idea of where the money goes.

Table 4.6

Summary of the Budget Data in the Department of Defense Report on Combating Terrorism

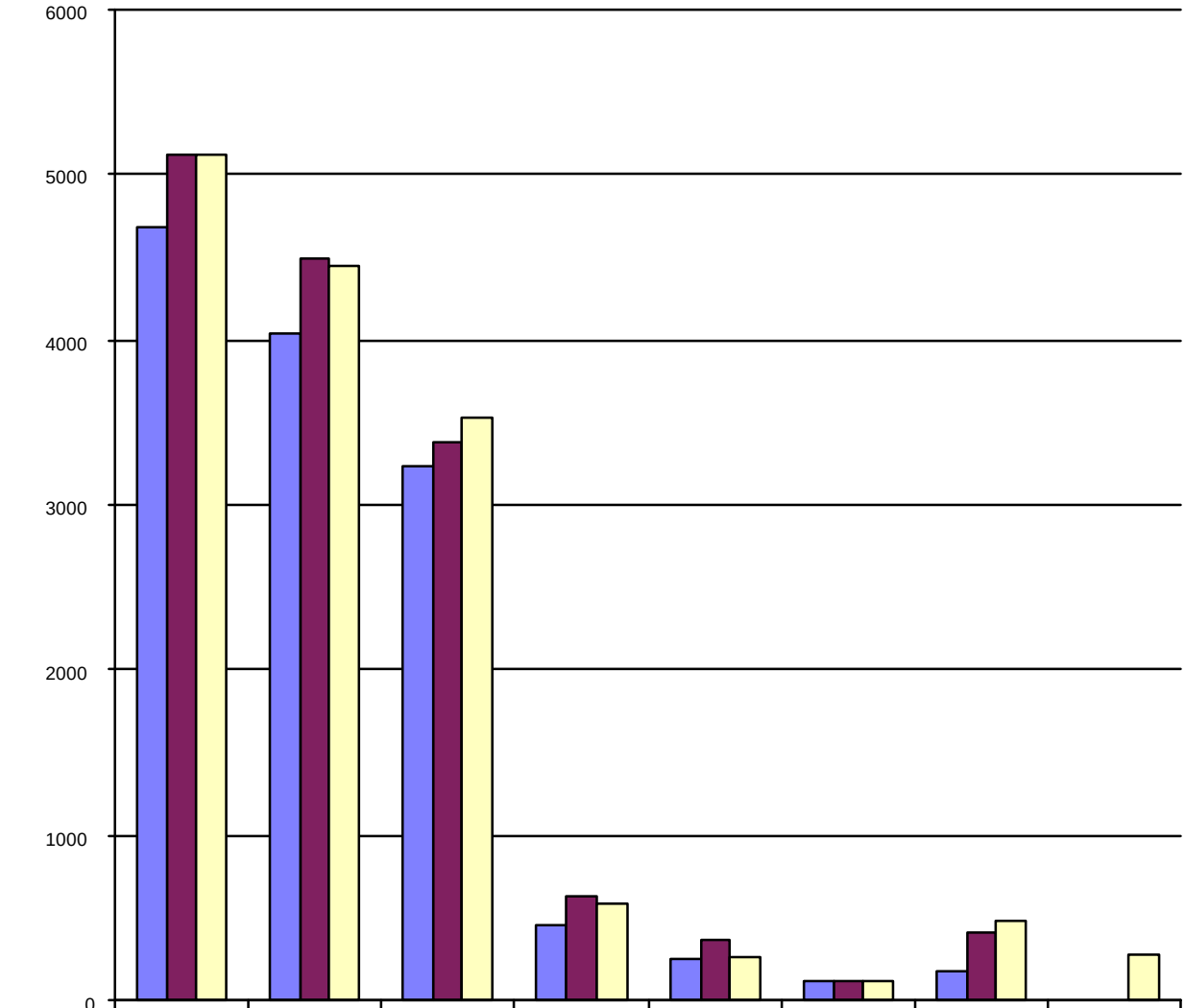
Activities	FY1999	FY2000	FY2001
AntiTerrorism			
Physical Security Equipment	192.4	185.9	205.2
Physical Security Site Improvements	56.4	89.2	57.3
Physical Security Management and Planning	58.3	55.6	58.1
Security Forces and Technicians	1,594.2	1,678.4	1,755.1
Law Enforcement	861.9	884.3	906.8
Security and Investigative Means	428.6	427.3	473.0
Research, Development, Test & Evaluation	48.2	59.6	65.6
SUBTOTAL	3,240.1	3,380.2	3,521.0
Counterterrorism			
Special Operations Command	446.5	620.8	554.9
Research, Development, Test & Evaluation	1.9	3.4	3.0
SUBTOTAL	448.3	634.2	557.9
Terrorism Consequence Management			
Domestic Preparedness Programs	48.9	32.1	10.2
Consequence Management Response	106.4	202.2	90.6
Research, Development, Test & Evaluation	89.0	134.7	164.7
SUBTOTAL	244.3	369.0	265.4
Intelligence			
Counterintelligence	107.1	106.8	106.0
Research, Development, Test & Evaluation	4.1	6.4	5.7
SUBTOTAL	111.2	113.2	111.7
TOTAL	4,044.0	4,486.6	4,455.9
OMB National Security Total	*(4,682.5)*	*(5,117.2)*	*(5,124.1)*
Difference	*638.5*	*630.6*	*668.2*

Source: Adapted by Anthony H. Cordesman from Department of Defense, Office of Combating Terrorism Policy and Support, Combating Terrorism Activities, FY2001, Washington, DC, January 14, 2000.

Chart 4.6

Department of Defense Spending on Combating Terrorism and Counter CBRN Defense

(Current $US Millions)



	OMB National Security	DoD Combat Terrorism	Force Protection	CounterTerrorism/SOF	Consequence Management	Intelligence	National Security WMD	DoD WMD
FY1999	4682	4044	3240	448	244	111	181	
FY2000	5117	4487	3380	634	369	113	408	
FY2001	5124	4456	3521	579	265	112	476	275

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.

The Department of Defense data track broadly with the OMB report in terms of total spending. This does not mean, however, that the differences between the two totals are measures of the money going to the intelligence community – although the DoD report makes no mention of any intelligence money going to CIA, NSA, or DIA. There is no way to correlate the line item data in the OMB and DoD reports and there seem to be a number of differences in the way each agency does the counting.

Several trends are apparent in the Department of Defense data, however, that are not as apparent in the OMB data:

- The vast bulk of spending goes to force and facility protection activities under the heading of "antiterrorism." This has also been the area of the most rapid growth in recent years – rising from $3.2 billion in FY1999 to $3.5 billion in FY2001. In broad terms, protecting US military forces and facilities overseas accounts for roughly 79% of all Department of Defense spending on counterterrorism. There is no way to know, however, what percentage affects DoD activities in foreign countries and DoD activities in the US.

- Another major element is more a matter of accounting than reality. The entire Special Operations Command is stated to be a dedicated counterterrorism activity because the DoD includes are resources dedicated and available to a given activity and personnel who dedicate 51% or more of their time to such efforts. As a result, counterterrorism spending is largely an artificial accounting construct. In FY2001, this included $557.9 million, or about 12% of total DoD spending.

- Terrorism consequence management is not a growth area and shrank from $369 million in FY2000 to $265 million in FY2001, as part of the DoD effort to reduce its responsibilities in this area. It was 5.9 percent of the total DoD effort in FY2001.

    - Between FY1999 and FY2001, the DoD effort in Domestic Preparedness Programs shrunk from $ 48.9 million to $ 10.2 million, or by nearly 80% percent. It was far less than one percent of the total DoD effort in FY2001.

    - The consequence management response effort lost more than 50% of its funding between FY2000 and FY2001. It was 2.0 percent of the total DoD effort in FY2001.

    - In contrast, RDT&E efforts in Terrorism consequence management nearly doubled between FY1999 and FY2001, and rose from $ 89.0 million to $ 164.7 million. It was 3.7 percent of the total DoD effort in FY2001.

- Intelligence spending was nearly static between FY1999 and FY2001, at around $112 million, or 2.5 percent of the total effort. It is obvious that no new programs are underway and no new capabilities are being funded or developed. The funds shown in this heading do not, however, included any activity by NSA or DIA, and virtually all go to the military services. Only about 4% are devoted to the Office of the Secretary of Defense.

- The DoD excludes all counterproliferation activity from its analysis of spending to combat terrorism. It also excludes most capabilities relating to asymmetric warfare.

- The DoD figures are meaningless in terms of measuring overall response capability and costs because these are contingency dependent. For example, any major emergency deployment of the Guard, reserves, or active forces in reaction to a nuclear or large scale biological attack could easily spend multiples of the total funding now shown for counterterrorism.

One key insight is that DoD.s total consequence management effort is now only $265 million and is less than 6% of its total effort. Intelligence, which is not really defined, is static and funded at only $112 million. Reports that imply that there is a massive Homeland Defense effort in DoD relating to CBRN attacks are flatly wrong, while the data that the DoD provides make it impossible to understand what is really happening, and to link counterproliferation and asymmetric warfare capability to Homeland defense

At the same time, there are critical limits to the DoD report. It is currently impossible to produce a valid analysis of the subset of DoD activities affecting the defense against the use chemical, biological, and radiological weapons by states, proxies, terrorists, or extremists, or to tie these aspects of Homeland defense to other aspects of Homeland defense. The figures in excess of $10 billion sometimes associated with such efforts are clearly statistical rubbish, and so are any efforts to associate total DoD spending to combat terrorism with CBRN defense of the American homeland. Only a minor amount of “combating terrorism” money goes to such efforts, and even some of that money actually supports many other functions.

Key Department of Defense Activities

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.

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

- *US Army 52nd Ordnance Group (EOD):* "Provides military explosive ordnance disposal (EOD)/bomb squad units to defeat or mitigate the hazards from conventional, nuclear, or chemical military munitions and weapons of mass destruction (WMD) throughout CONUS as requested by local, state, federal law enforcement or military authorities."[44]

- *US Army Response Task Forces (RTF):* RTF aids the lead agency in consequence management operations by creating a command and control that coordinates all other DoD elements.

- *US Army Medical Research Institute of Chemical Defense (USAMRICD), Medical Chemical Biological Advisory Team (MCBAT):* Is the lead source for medical information for chemical agents.

- *US Army Medical Research Institute of Infectious Diseases (USAMARIID):* USAMARIID is the lead medical research laboratory for the US Biological Defense Research Program. Its role is to protect against bioterrorism and biowarfare with the ideal prevention of immunization. It conducts research to develop technologies, procedures, and training programs for medical defense against biological warfare threats and naturally occurring infectious diseases. It is a tech based research facility that creates countermeasures for biological agents. USAMARIID's facilities include the capability to contain and care for at biosaftey level 3 and 4. It also has an Aeromedical Isolation Team that can respond anywhere in the world and transport back to the center. USAMARIID also provides counterterrorism support with threat evaluation, rapid bio agent identification, and as a general reference to biological agents. USAMARIID is 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.

- *US Army Edgewood Chemical and Biological Forensic Analytical Center Modular On-site Laboratory:* Provides facilities with capabilities to analyze chemical agents.

- *US Army Radiological Control (RADCON):* Supports RTF to provide radiological monitoring.

- *US Army Radiological Advisory Medical Team (RAMT):* Supports RTF and local responders during radiological health situations.

- *Air Force Radiological Assessment Team (AFRAT)*: AFRAT is a response team for nuclear and radiological incidents. Its indirectly funded with O&M funds from the Institute for Environment, Safety and Occupational Health Risk Analysis (IERA), Radiation Protection Division. These funds go towards the equipment and training AFRAT needs to respond to radiological 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.

- *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.

- *Navy Environmental and Preventive Medicine Unit*: This is a Chemical, Biological, Radiological and Environmental Defense Response Team. Teams are created on an *ad hoc* basis suited to the situation. They provided assistance to Chemical/Biological Rapid Response Teams and local responders.

- *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. The DOD reports that the procurement for FY2001 is $1.9 million.

- *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.

- *WMD Civil Support Teams*. There are member teams in 26 states by 2001. The 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.

Antiterrorism and Force Protection

Although anti-terrorism and force protection efforts receive the vast bulk of DoD funding to combat terrorism, they generally have little to do with CBRN attacks. They are designed basically to deal with high explosives and direct assaults, with limited capability to deal with a direct intrusion of a chemical, biological or nuclear weapons.

In fact, one of the more interesting aspects of a detailed review of the service programs in this area is that there is considerable expense on intrusion detection and explosive detection, and blast mitigation, but little on either CBRN detection or cyberattack detection. It is also unclear that the massive number of vulnerability assessments reflected in the FY1999-FY2001 budgets examined these aspects of the problem or any aspect of the possible impact on defense health facilities. It is unclear that current service regulations and technical manuals require such analysis although protection against CBRN attacks is in the charter of each service force protection effort. (The only service to specifically mention this ion its budget justification is the Navy.) Somewhat ironically, DoD law enforcement activities pay far more attention to CBRN attacks than any of the programs related to force and facility protection improvement and design.[45]

Even the DTRA portion of the ongoing force protection effort does not explicitly touch on any CBRN-related effort in the DoD budget justification document.[46] The Joint Staff did, however, developing a WMD Planning Template Annex in FY1999, and directed a program to

educate CINCs and the services in FY2000 and FY2001.[47]

They do, however, have at least some relation to the problem. In brief, DOD has taken action to improve its antiterrorism/force protection (AT/FP) program since the 1995 Riyadh car bomb and 1996 Khobar Towers bombing. The Secretary of Defense chose the Chairman of the Joint Chiefs of Staff to be the principal AT/FP adviser in September 1996, and the Chairman announced DOD's goal of becoming the worldwide AT/FP leader. A July 2000 GAO report describes the DOD AT/FP program:[48]

> The Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict is the principal staff assistant and advisor to the Secretary of Defense for antiterrorism/force protection (AT/FP) policy. While this office focuses on policy, the Chairman of the Joint Chiefs of Staff and the Combating Terrorism directorate within the Joint Staff focus on implementing DOD's AT/FP program. The Joint Staff's responsibilities include reviewing the services' AT/FP budgets, developing standards, managing the Joint Staff Integrated Vulnerability Assessment program, and representing the geographic combatant commanders on AT/FP matters.
>
> DOD policy makes commanders responsible for protecting their forces from terrorist attacks. For forces overseas, the responsibility rests with the geographic combatant commander and the installation commander, with the support of the service headquarters. The geographic combatant commanders are responsible for developing antiterrorism policies that apply at the installations in their areas of responsibility and that take precedence over service or other DOD component AT/FP policies. They are also responsible for determining the threat levels for each country in their area of responsibility, identifying the money and manpower needed to achieve sufficient AT/FP, and working with the services to provide the resources necessary. Finally, because all risks cannot be eliminated, the geographic combatant commanders are responsible for determining the types of risks their forces will face as they undertake their missions.
>
> Installation commanders are responsible for protecting the people, assets, and facilities under their command from terrorist attacks. The installation commander, working with the installation AT/FP manager, is responsible for ensuring that AT/FP standards established by DOD, the geographic combatant commanders, the services, and the service headquarters are implemented. Additionally, because DOD recognizes that not all vulnerabilities can be addressed, installation commanders practice risk management—to decide what risks can be accepted and what risks are too great to be accepted. When the risk is unacceptable, the commander is responsible for taking action to mitigate the risk.
>
> Although geographic combatant commanders have overall responsibility to protect forces assigned to them, individual services are responsible for funding an installation's AT/FP needs and for providing the required number of trained personnel. The majority of funds used for AT/FP activities (excluding the cost of military personnel) are located in the services' Operation and Maintenance appropriations. Operation and Maintenance appropriations are generally used to fund readiness activities, equipment maintenance, recruiting, pay for civilian employees (including contract security guards), and the everyday costs of running an installation. A number of subactivities within this appropriation fund specific expenses. Examples of the subactivities include real property maintenance, depot maintenance, and base operating support. The base operating support subactivity pays for expenses such as utilities, communications, security, building repair, and maintenance. Traditionally, the services have included funds for AT/FP in the base operating support subactivity, and AT/FP activities must compete against other activities for the same

limited funding.

Shortly after the Khobar Towers bombing, the Secretary of Defense established the Chairman of the Joint Chiefs of Staff's Combating Terrorism Readiness Initiative Fund.4 The Fund, which is managed by the Joint Staff, was not intended to relieve the services of their responsibility to fund AT/FP projects; rather, it was intended to provide funding for emergency or other unforeseen high-priority, combating terrorism needs. In fiscal year 2000, the Fund totaled $15 million—$10 million of Operation and Maintenance funds and $5 million of procurement funds. This level of funding is scheduled to continue through fiscal year 2002. In fiscal years 2003 through 2007, the Fund will be reduced to a total of $10 million a year according to DOD.

The GAO did criticize the DOD for underfunding AT/FP programs, for inadequately training AT/FP managers, and for incompletely assessing vulnerabilities. The GAO said:[49]

Overall, military forces stationed overseas are better protected today than they were 3 years ago. The Joint Staff has developed DOD-wide construction standards to ensure that antiterrorism/force protection measures are included in new construction. In addition, DOD has signed agreements with the Department of State and U.S. ambassadors or chiefs of mission to protect DOD personnel not under the jurisdiction of commanders. Geographic combatant commands have created permanent antiterrorism/force protection offices, hired permanent antiterrorism/force protection staff, and developed systems to monitor progress to correct vulnerabilities. Installation commanders are more aware of their responsibility to protect their forces from terrorist attack and, despite funding constraints, have addressed many security vulnerabilities. However, significant security and procedural antiterrorism/force protection problems continue at many installations. For example, some installations have not developed plans to deal with terrorist attacks, others have no effective means of stopping unauthorized vehicles from entering the installation, and some lack secure access to important intelligence information.

Commanders are better able to determine their vulnerability to terrorist attacks than when we last reported. Vulnerability assessments are now being conducted more routinely and are based on a defined set of criteria. However, vulnerability assessment reports do not provide specific actions to rectify problems mentioned in the reports. Additionally, there is no comprehensive method in place to share solutions to common problems among different installations.

Limited antiterrorism funding and trained staff have affected the ability of commanders to correct known vulnerabilities. Funding for antiterrorism protection has been, and will likely continue to be, significantly less than what installation and geographic combatant commanders have determined they require, despite the fact that senior DOD leaders have designated antiterrorism/force protection as a high priority item. For example, some overseas service commands have repeatedly received less than 50 percent of the money the commands believe they require to correct or mitigate vulnerabilities. According to antiterrorism/force protection managers, this level of funding has limited their ability to address vulnerabilities. Congress requires DOD to provide information on proposed antiterrorism/force protection funding and projects as part of its consolidated combating terrorism budget submission; however, it does not require DOD to provide information on the number of projects that remain to be funded. Without information on the types of projects that need funding, Congress does not have an accurate picture of the extent of the risk that U.S. forces face from terrorism. In addition, installations we visited did not have adequately trained personnel dedicated to managing and implementing antiterrorism solutions.

The GAO never explicitly addressed CBRN vulnerabilities. It did report, however, that

all services will face a shortage of AT/FP funding in FY 2001. It estimated that the services' required $274.5 million and estimates that the proposed budget is only $141.3 million, or 51% of the need. The Joint Staff also estimated that AT/FP programs need an extra $700 million over current FY 2002-2005 spending plans. The GAO made the following recommendations to improve AT/FP:[50]

> To improve the effectiveness and increase the impact of the vulnerability assessments and the vulnerability assessment reports, we recommend that the Secretary of Defense direct the Chairman of the Joint Chiefs of Staff to improve the vulnerability assessment reports provided to installations. Although the Joint Staff is planning to take some action to improve the value of these reports, we believe the vulnerability assessment reports should recommend specific actions to overcome identified vulnerabilities. In addition, the Joint Staff should develop an antiterrorism/force protection best practices or lessons learned program that would share recommendations for both physical and process-oriented improvements. The program would assist installations in finding answers to common problems—particularly those installations that do not receive Joint Staff Integrated Vulnerability Assessment reports or others who have found vulnerabilities through their own vulnerability assessments.
>
> To provide Congress with the most complete information on the risks that U.S. forces overseas are facing from terrorism, we recommend that the Secretary of Defense direct the services to include in their next consolidated combating terrorism budget submission information on the number and types of antiterrorism/force protection projects that have not been addressed by the budget request and the estimated cost to complete these projects. Information on the backlog of projects should be presented by geographic combatant command.
>
> To ensure that antiterrorism/force protection managers have the knowledge and skills needed to develop and implement effective antiterrorism/force protection programs, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict to expeditiously implement the Joint Staff's draft antiterrorism/force protection manager training standard and formulate a timetable for the services to develop and implement a new course that meets the revised standards. Additionally, the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict should review the course content to ensure that the course has consistency of emphasis across the services.

As is the case with the OMB data, there is no way to tie the GAO estimates to the DoD reporting on such activity. The DOD reports that the AT/FP budget for FY2001 is $3.5 billion. There is a large discrepancy between the GAO estimate with the DOD estimate.

Counterterrorism

As is noted earlier, the DoD budget category for counterterrorism is essentially the budget for the US Special Forces Command and includes the US Army Special Forces Command, Naval Special Warfare Command and SEALS, US Air Force Special Operations

Command, and Joint Special Operations command. This effort does have a heavy RDT&E element ($87 million in FY20001), but most of the spending is on operating and procurement spending. The budget increased from $446 million in FY1999 to $621 million in FY2000, but dropped to $555 million in FY2001. Virtually all of the shift was procurement related.[51]

Much of this program is black, but there are no indications of CBRN dedicated programs in the DoD reporting, and little to indicate that spending really goes to combat terrorism as distinguished from all types of special forces missions. It is not clear that this budget category makes any functional sense.

Terrorism Consequence Management

Virtually all dedicated DoD activity related to CBRN threats is funded as part of the Terrorism consequence management program. As has been touched upon earlier, this is not a growth area. Total funding shrank from $369 million in FY2000 to $265 million in FY2001, largely because of a DoD effort to reduce its responsibilities in this area. The spending in this category is divided into three major program activities:

- Domestic Preparedness Programs which shrunk from $ 48.9 million to $ 10.2 million between FY1999 and FY2001, the DoD effort in, or by nearly 80% percent. These programs train emergency responders, support Rapid Response Teams, and a Chemical-Biological Emergency Response Team (CBERT). It funds an interagency FBI, FEMA, DOE, EPA, USPHS, and DoD coordination group.

- Consequence management response programs which rose from $106 million in FY1999 to $202 million in FY2000, and than dropped to $91 million in FY2001. These efforts lost more than 50% of their funding between FY2000 and FY2001.

- RDT&E efforts in terrorism consequence management, which nearly doubled between FY1999 and FY2001, and rose from $ 89.0 million to $ 164.7 million.

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. This is why the DOD established the Domestic Preparedness Program to train local and state first responders for a

CBRN attack. The program is supposed to 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 Army's Soldier and Biological Chemical Command is the organization within the DOD that administers the Domestic Preparedness Program.[52] The OMB reports that the total funding for the program during fiscal years 1997-99 was $66.9 million. Funding for fiscal year 2000 was $12.6 million, and the funding request for FY2001 is $31 million.[53] The DoD report states that funding for the same heading was $48.9 million in FY1999, $32.1 million in FY2000, and $10.2 million in FY2001.[54] The difference between the OMB and DoD costing seems to be largely the result of the fact that the OMB report did not take account of plans to transfer much of the DoD activity to the Department of Justice.

In FY2000, the Administration proposed to transfer the Domestic Preparedness Program to DOJ on October 1, 2000, and DOJ will complete DOD's commitments to the 120 cities.[55] The current DoD budget plan will complete this transfer management of the Domestic Preparedness Program to the Department of Justice in FY2001. The DOD will retain management of some programs that utilize DOD resources. The DOD will still fund the Chem-Bio Database development component of the Rapid Response Information System and also the equipment-testing program.

This transfer makes only tenuous sense. DoD may not like the responsibility, but transfer to a civil agency only seems suitable if the program focuses on incidents of the kind that can be dealt with by normal civil defense and response agencies, and DoD and civil agencies are not called upon to deal with a major nuclear or biological incident or a series of asymmetric attacks by a foreign power, proxy, or highly sophisticated terrorist agency. Even then, it is not clear what DOJ would be chosen instead of FEMA.

A March 2000, GAO report summarized progress in the Domestic Preparedness Program as follows:[56]

> 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 4.7

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	[a]1,600
Hospital provider	2,800
Military	850
Other [b]	4,350
Total	**19,000**

.

There have been problems in the program. The lack of interagency coordination in 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 GAO made the following comments,[57]

> 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.

More generally, serious questions arise as to whether the present training and equipment activity in this area of activity are really suited to deal with large nuclear and biological attacks or incidents, and realistically examine DoD-civil federal, state, local, and private sector needs and capabilities for more than low to mid-level terrorism. There seems to be a great deal more emphasis on counting training activity in most reporting on this aspect of the DoD program than to assess whether the training is realistic and adequate.

Consequence Management Response Program

The Consequence Management Response Program is the largest operational component of the overall Terrorism Consequence Management Program, with a total budget of $90.6 million in FY2001. This efforts attempts to integrate the reserves into the response effort, and functions include detection, decontamination, supporting the civil authorities, ordnance disposal, chemical and biological field sampling and characterization. It includes activities like the Civil Support (formerly Rapid Assessment Initial Detection or RAID) teams. It also includes the efforts of the US Army response task forces, and support from specialized US military institutes and facilities like the US Army Research Institute of Chemical Defense (USAMRICD), US Army Medical Research Institute of Infectious Disease (USAMIIRD), US Army Edgewood Chemical and Biological Forensic Analytic Center Modular On-Site Laboratory, US Army Radiological Control (RADCON) Team and US Navy Radiological Control (RADCON) Team, and US Army Radiological Advisory Medical Team (RAMT).

Many of the cutting edge US capabilities for chemical and biological defense outside the CDC and the DARPA research program are concentrated into this area. Unfortunately, the DoD budget reporting does not provide an adequate description of their activity and how much can be ascribed to Homeland defense. There is also a strong tendency to use imply large capabilities and

fund relatively small ones.

Assistant to the Secretary of Defense for Civil Support

The Secretary of Defense appointed the Assistant to the Secretary of Defense for Civil Support (ATSD-CS) to serve as the primary coordinator of DOD's WMD consequence management programs. The ATSD-CS coordinates by chairing the DOD's WMD Preparedness Group, which ensures the DOD's consequence management capabilities and resources are efficiently used.

The WMD Preparedness Group is comprised of the Assistant Secretaries for Health Affairs; Reserve Affairs; Special Operations/Low Intensity Conflict; Command, Control, Communications, and Intelligence; and Legislative Affairs; the General Counsel; the Deputy Under Secretaries for Comptroller and for Acquisition, Technology, and Logistics; and senior representatives from the Joint Staff, the Department of the Army, and the Defense Threat Reduction Agency. The ATSD-CS also represents the DOD in the interagency task force chaired by the President's National Coordinator for Security, Infrastructure Protection, and Counterterrorism.[58]

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 managed by DTRA with oversight from the Deputy Assistant to the Secretary of Defense for Chemical and Biological Defense.

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.[59]

This led to a steady increase in many expenditures unrelated to Homeland defense. For example, funding for e chemical agents and munitions destruction, defense category of Defense-wide Procurement Appropriations Account increased $24 million from $979 million for the 2000 FYDP to $1,004 million for the 2001 FYDP.[60]

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:[61]

- 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 goal of the program is to "develop and demonstrate technologies to thwart the use of biological warfare agents (including bacterial, viral, and bioengineered organisms and toxins) by both military and terrorist opponents. DARPA's primary strategy for accomplishing this goal is to create technologies applicable to broad classes of pathogens and toxins."[62] DARPA focuses on detection, defense, and response of biological weapons. The DOD reports that funding for DARPA has increased every year from $84 million in FY 1999 to $162 million for FY 2001. The largest area

of funding has been Sensors, which deal with the development of technology able to discern the type of bio agents used.

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 FY 2000-2001 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.[63] Virtually all of this funding, however, goes to improve warfighting capability for conflicts overseas. The part of the Chemical and Biological Defense Program that relates to Terrorism Consequence Management has been sharply cut. The DoD budget document indicates that funding dropped from $14.9 million in FY1999 to $9.2 million in FY2000 to $1.2 million in FY2001.[64]

This has been a troubled program in a number of ways. 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:[65]

> 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 recommended in March 2000 that CBDP be coordinated with the other non-medical chemical and biological research programs:[66]

> 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

One of the original purposes of the CBDP is to provide WMD civil support teams with equipment adequate in a response to a chemical/biological incident under the National Guard (NG) and Reserve Component (RC) Equipment program. The WMD Civil Support Teams represent the first military responders and have a goal of reaching a WMD scene within four hours. Ten teams have already been established and are stationed in the ten FEMA regions around the country.[67]. 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 state and federal support. A team is comprised of seven cells: command and control, reconnaissance, medical support, security, logistics, air liaison, and communications.[68] Each team has 22 members, and the governors of the states they are deployed have command and control of the team.[69]

The program was supposed to provide 15 WMD Civil Support Teams with equipment, with 10 equipped in FY 1999 and 5 in FY 2000. The DOD has since called for the establishment

of 17 new WMD Civil Support Teams in addition to the sustainment of the 10 already established in FY2000. Funding for the Consequence Management Program has dropped from FY 2000 of $107.2 million to $76.4 million in FY 2001, however, and most is spent on sustainment of the teams instead of initial fielding of new teams. There are no plans to field new WMD CS Teams in FY 2001 and by the end of 2000, there will only be 27 WMD CS Teams of the originally planned 44 WMD CS Teams. According to DoD, it plans to retain one WMD rapid response team in addition to 17 Civil Support Teams.

Chemical Biological Response Force (CBIRF)

The CBIRF is a 373 man Marine Unit established to provide a chemical-biological incident capability, Funds were provided to stand it up in FY1999 and FY2000, and its equipment has been steadily improved. Most funding, however, has gone for chemical warfare related equipment, and the CBIR only begins to acquire extensive amounts of biological warfare equipment in FY2001. Even then, most of its capability depends on the success of RDT&E activities described in the FY2001 program, but which have no clear deployment date.[70] The CBIRF has limited technical expertise and manning and the DoD budget report indicates is sized as a one medium incident chemical attack response force with limited biological incident capability.

US Air Force Radiological Survey Team (AFRAT) and Foreign Emergency Support Team (FEST)

The US Air Force Radiological Survey Team (AFRAT) is a small 43-man team funded with discretionary funding. It is one of the few teams with dedicated capabilities that could respond to a serious radiological incident.[71]

The USAF 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.[72] The DOD reports that there is no planned funding for FEST in FY2001. The

replacement aircraft will be used.

Counterterror Technical Support Program

The OASD (SO/LIC) is responsible for the oversight of the Counterterror Technical Support Program (CTTS), which will be renamed the Combating Terrorism Technology Support Program in 2001. The CTTS helps fund the R&D for The Technical Support Working Group (TSWG) under the Interagency Working Group on Counterterrorism (IWG/CT). The CTTS develops technology to detect chemical and nuclear threats. The OASD (SO/LIC) also coordinates WMD Terrorist Consequence Management. "Activities funded consist of interagency user requirements related to the personal protection, detection, identification, containment, mitigation and disposal of terrorist-employed chemical, biological, radiological, and nuclear materials."[73] The goal is to develop protective equipment and early warning devices for WMD incidents. The funding for the CTTS has decreased slightly for FY 2001 because of the completion of various projects.

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.[74] $5 million has been requested for FY 2001 for the Joint Task Force.

Defense Logistics Agency

One of the DLA's responsibilities is the procurement of protective equipment and training for DLA agents to plan and react during a chemical/biological incident. Of the $2,246,000 appropriated to the DLA in 2001, however, only $66,000 will go towards chemical/biological incident protection for the procurement of protective suits and masks and

crisis management training.

Defense Threat Reduction Agency

DTRA is a Combat Support Agency directed by the Chairman, Joint Chiefs of Staff, made up of military and DoD civilians to provide vulnerability assessment to better protect military and civilian personnel. DTRA also manages the Chemical/Biological Defense Program. The DOD has appropriated $11,442,000 for DTRA in FY 2001.

The Chemical/Biological Defense program includes the development of materials for training, exercises, force protection installation planning, first response, vulnerability assessment, and detection gear. The program has, however, had only limited funding for Antiterrorism and Force Protection: $2,841 million in FY1999 declining to $458 million in FY2001. This aspect of DTRA activity is heavily oriented toward chemical as distinguished from biological warfare. In contrast, defense-wide RDT&E in more conventional counterterrorism activity increased from $25.0 million in FY1999 to $35.1 million in FY2001.[75] An additional $30 million in RDT&E was programmed in FY2001 for SOLIC RDT&E, all of which is described as related to attacks using conventional explosives. This illustrates the heavy emphasis DoD places on conventional, versus CBRN counterterrorism.

The DTRA Consequence Management Response Program has been larger, because DTRA has provided chemical and biological defense equipment for several of the field teams discussed earlier. These have include the WMD Civil Support Teams, but the number of teams funded has dropped from 10 in FY1999 to five in FY2001, and funding for these teams has dropped from $14.6 million to $1.2 million.[76] The FY2001 submission does not call for funding any teams beyond the 15 already equipped. It is also important to note that the equipment provided is not particularly advanced, and has comparatively limited capability for biological warfare.

DTRA supports several other team efforts:

- *Joint Staff Integrated Vulnerability Assessments Teams (JSIVA):* The operational teams that assess "facility vulnerability to terrorist operations and the means of reduction mass casualties. These assessments include: (1) Terrorist Options; (2) Physical Security; (3) Structural Engineering and Response; (4) Infrastructure Engineering; and (5) Operations."[77] The budget of the DTRA for FY2001 is $7.6 million, which will be spent on the salaries and expenses of the JSIVA teams.
- *Consequence Management Advisory Team (CMAT):* The CMAT is the team that satisfies the DTRA's responsibility for aiding other DoD organizations with WMD and radiological incidents. It "provides technical, consequence management planning, weapons effects modeling, general counsel, public affairs, and health physics expertise to augment CIMC staffs."[78] The funding for the CMAT for FY 2001 is $300,000.

A detailed review of the Department of Defense budget document reveals a number of other DTRA activities. One thing is all too clear, however, and affects much of the intellectual underpinning of the DoD planning effort. A total of $11,4 million does not come close to the amount needed to carry out adequate assessment of the effects of CBRN weapons in a wide range of different attacks, to support net technical assessment efforts, to improve other aspects of planning or response, or to assist broadly in training. At present, DTRA simply is not funded to take on a mission of the scale required.

Research and Development

DARPA is the core of the independent research and development funding identified in the DoD budget analysis for Terrorism Consequence Management. The RDT&E activity in this category is funded at $89.0 million in FY1999, $134.7 in FY2000, and $164.7 million in FY2001. The DARPA portion is funded at $84.0 million in FY1999, $131.7 in FY2000, and $162.1 million in FY2001. It is a relatively robust effort, and reflects a realistic emphasis on RDT&E in an area where the existing threat is limited, but major advances in technology are needed to defend against future threats like genetically engineered biological weapons.

The DARPA Biological Warfare Defense program covers a wide range of efforts to create new characterization systems and defenses against bacterial, viral, and bioengineered organisms and toxins and address both full-scale and terrorist attacks. It involves major advances in detection and characterization technology to reduce the false alarm rate, increase speed, and deal with complex attacks. The program also involves consequence management and external protection technology, asymmetrical protocols for biological warfare defense, and genetic

sequencing research.

It is important to note that this RDT&E program does not have strong service counterparts, and seems to be the only major US government effort seek major new solutions to the threat posed by biological attacks. The military service and CDC efforts have an RDT&E component, but funding is comparatively limited and is concentrated on improving detection and response through the growth of existing technologies.

At the same time, the DARPA program is not described in ways that show any great consistency of effort from year-to-year, or which give any evidence of a coherent future year program. Such planning may exist, but it is not described in unclassified DOD or DARPA literature. No timelines or cost estimates seem to exist for deployment of most of the technologies involved, which generally are designed to fill critical ongoing gaps in the present US government effort to deal with the threat posed by biological weapons.

Intelligence

Virtually all funding in the intelligence category reported by the Department of Defense goes to counterintelligence activity, with very limited funding for research and development. The counterintelligence effort is funded at $107 million in FY1999 and FY2000, and $106 million in FY2001.The RDT&E effort is funded at $4.1 million, $6.4 million, and $5.7 million respectively. Total intelligence funding is $111.2 million in FY1999, $113.2 million in FY2000, and $111.7 million in FY2001.

In practice, the budget description of this activity indicates that virtually all of the intelligence activity involved is designed to support the force protection mission at the tactical level. None goes to developing new intelligence methods or broader intelligence efforts to deal with emerging threats or asymmetric warfare. Any funding of improved CIA, NSA, and DIA efforts is funded under other aspects of the national security budget. The independent RDT&E effort does, however, fund a limited program to support the Vice President’s Task Force on

Terrorism for pre-incident intelligence gathering and operations.

The Possible FY2001 DoD Budget for CBRN/WMD Homeland Defense

Another way to look at Department of Defense activities is to search out only those activities to combat terrorism which can be clearly and openly identified as directed toward CBRN attacks and WMD, and which might have direct relevance to Homeland defense.. Any such estimate using the DoD report on Combating Terrorism must be tenuous at best. Table 4.8 does, however, provide a rough indication of just how small the dedicated effort may really be. While the total for combating terrorism is well in excess of $4 billion; the figure for core DoD activities that broadly affect the defense and response against CBRN attacks on the American homeland is less than $300 million. This does, however, account for a major part of the $467 million that OMB estimates is spent by all National Security agencies on such programs.

Table 4.8

Core Department of Defense Efforts in Combating Terrorism that Broadly Affect CBRN-Related Homeland Defense Against State, Proxy, Terrorist, and Extremist Attacks on Targets Other than DoD Facilities and Forces

WMD Preparedness	
Preparing for and Responding to WMD Terrorism	
DLA	.066
DTRA	11.422
Subtotal	11.488
First Responder Training	10.2
Air Force First Responder	2.700
Subtotal	12.9
Other Planning and Assistance to State/Locals	
Navy – Support to Civil Authorities/TCM	5.574
Special Response Units	
Consequence Management Program	76.4
CBIRF	4.369
Subtotal	80.769
TOTAL	*110.731*
R&D	
Basic Research, incl. Gene Sequencing	
DARPA – Genetic Sequencing of Biological Warfare Agents	12.5
Detection/Diagnostics	
CTTS	
DARPA – Advanced Diagnostics	19.350
DARPA – Sensors	24.056
Subtotal	46.454
Modeling, Simulation, System Analysis	
DARPA – Consequence Management	10.0
Personal/Collective Protection	
DARPA – Bio/Chem Defensive Systems	10.0
Personal/Environmental Decontamination	
DARPA – External Protection	21.0
Therapeutics/Treatments	
DARPA – Multipurpose	22.2
Vaccines	
DARPA – Anti-Virals/Immunizations	21.3
DARPA – Anti-Bacterials/Anti-Toxins	21.658
Subtotal	42.958
TOTAL	*165.112*
Grand Total	275.843

*R&D calculated is the total of R&D from Antiterrorism, Counterterrorism, Terrorism Consequence Management, and Intelligence categories from p. 78.

Department of Defense, Office of Combating Terrorism Policy and Support, Combating Terrorism Activities, FY2001, Washington, DC, January 14, 2000

Conclusions

There is little publicly apparent coordination or policy within the Department of Defense that deal with Homeland Defense against CBRN attacks and WMD Preparedness in ways that go beyond a relatively small core of activities to combat terrorism. This is best exemplified by (a) the failure to tie together all of the key activities relating to homeland defense, (b) a narrow and often dysfunctional definition of counterterrorism, (c) the discrepancies in the DOD and OMB estimates of funding to combat terrorism, and (d) the lack of any apparent dedicate future year planning and programming effort. There is a clear lack of focus, sense of mission, and overall organization of the DOD's efforts against WMD defense in the DOD's Combating Terrorism budget as described in its *public* reporting.

These problems point to obvious solutions. Counterterrorism is only a subset of a much broader problem that affects by Homeland Defense and a world in which the risk of asymmetric conflicts and attacks force us to rethink our entire approach to national security. There is a clear need for a dedicated and more open PPB and FYP effort that covers all of the aspects of the problem and which allows the Executive Branch, Congress, and outside analysts to understand which programs and money is going, our current and planning capabilities, and the balance between different kinds of defensive activity.

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.[79] 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-terrorism 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 $1.42 billion:[80]

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. It 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.[81]

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.[82]

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.[83]

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."[84] CBNP's funding has grown from $17 million in FY 1997 to a projected $63 million in FY 2001.[85]

Total Program Spending

The following table on DOE counterterrorism spending adapted from the 2000 OMB counterterrorism funding report shows no significant increases in funding since FY 1999. The requested FY 2001 budget is $663.53 million.[86]

Table 4.8

Department of Energy Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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
WMD Preparedness	**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:[87]

- 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.[88]

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.[89] 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.[90]

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 the 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

The Federal On-Scene Coordinator (OSC) 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).[91] The FY 2001 budget request for these activities is $3.2 million.[92]

Current Budget

The following table on EPA counterterrorism spending adapted from the 2000 OMB counterterrorism funding report shows there has been an increase of $1.20 million in funding for FY 2001 requested. All EPA counterterrorism funding has gone towards WMD special response units.[93]

Table 4.9

Department of Energy Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**2.00**	**2.00**	**2.00**	**3.20**
Preparing for and Responding to Terrorist Acts	2.00	2.00	2.00	3.20
WMD Preparedness	**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.[94] Initially, the FBI maintains command until the Attorney General transfers the lead agency role to FEMA.[95] 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.[96] The Center for Nonproliferation, Monterey Institute of International Studies has **summarized** FEMA's counterterrorism efforts as follows:[97]

- 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

This office 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.

FEMA also maintains the Rapid Response Information System *(FEMA)*. The Rapid Response Information System (RRIS) can be used as a reference guide, training aid, and an overall planning and training resource for response to a chemical, biological and/or nuclear terrorist incident. The RRIS is comprised of several databases, consisting of chemical and biological agents' and radiological materials' characteristics, first aid measures, Federal response

capabilities, Help Line, Hotlines, and other Federal information sources concerning potential weapons of mass destruction. It is accessible on the Internet at http://www.rris.fema.gov/.

United States Fire Administration

The US 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.[98] A March 2000 GAO report provides a program description:[99]

- 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; (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 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.[100]

The following table 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.[101]

Table 4.10

Federal Emergency Management Agency Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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
WMD Preparedness	**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 table on GSA counterterrorism spending report adapted from the 2000 OMB counterterrorism funding report shows that no money is being spent specifically on CBRN threats.[102]

Table 4.11

General Services Administration Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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

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.[103] 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.

The National Commission on Terrorism, also known as the Bremer Commission, has recommended that the HHS strengthen controls of pathogens and other biological materials at laboratories and during transport. The Bremer Commission observed that the current controls are designed for accident prevention, not to stop theft. The Commission noted that biological controls are not are rigorous nuclear controls. The Commission also recommended regulation of sophisticated equipment necessary for the weaponization of pathogens to hinder the ability of terrorists to acquire the equipment.[104]

Metropolitan Medical Response Systems

HHS is 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) were created under HHS' Office of Emergency Preparedness. In 1999, MMRS were in 27 cities and consisted of trained and equipped local emergency teams. The Systems also participate in DOD's Domestic Preparedness Program.[105] 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.[106] The end goal of HHS is to have MMRS for the 120 most populous cities.

The HHS released a fact sheet in May 2000 describing the MMRS:[107]

> 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.[108] 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:[109]

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. 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:[110]

> 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

fo 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.[111]

The National Commission on Terrorism recommended that the HHS take further steps in enhancing surveillance capability by working with the Department of State to develop an international surveillance system that would serve as an early warning system for infectious disease outbreaks as well as a monitoring system to detect potential terrorist experimentation. The Commission noted that the US has some domestic surveillance capabilities but said the international community is behind US efforts.[112]

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 **the** Secretary for R&D on improved civilian stockpiles of Anthrax and smallpox 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 table 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.[113]

Table 4.12

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

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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
WMD Preparedness	**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 4.13 shows Holocaust Memorial Museum counterterrorism spending adapted from the 2000 OMB counterterrorism funding report, which shows that $2 million was appropriated in

FY 1999 for the physical security of government facilities and employees.[114]

Table 4.13

Holocaust Memorial Museum Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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 averages around $10 million.[115] The vast majority of the money goes to physical protection of government facilities and employees.

Table 4.14

Department of the Interior Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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

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

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.[116] The FBI is responsible for preventing and responding to domestic terrorism.[117] It gathers and assesses intelligence on domestic threats.[118] Its Criminal Division is tasked with all criminal investigations not specifically given to another division. 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 created 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.

The National Commission on Terrorism, also known as the Bremer Commission, has

made many suggestions of how the DOJ and FBI could improve counterterrorism information collection and dissemination. The Commission thought that the guidelines for opening an inquiry or investigation on terrorism need to be clarified. The Foreign Intelligence Collection and Foreign Counterintelligence Investigations guidelines cover international terrorism and the Attorney General guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations cover domestic terrorism. The Commission said field agents are hindered in their investigations because they were unsure if guidelines had been met. The Bremer Commission also recommended streamlining the process for obtaining a court order for electronic surveillance and physical searches of international terrorists. The Office of Intelligence Policy and Review (OIPR) reviews the FBI's application of a Foreign Intelligence Surveillance Act (FISA) order before the FISA order is sent to a FISA court for approval. The Commission recommended that OIPR work more efficiently with the FBI and require no more than what FISA statute requires before submitting application to the FISA court. The Commission supports the FBI's efforts to update information technology capabilities, including counterencryption equipment and data storage and retrieval systems. However, the Commission recommended that the FBI establish reports officers similar to the ones in the CIA to determine what terrorist-related information would be useful to other agencies and policymakers. The Commission said:[119]

> Law enforcement agencies are traditionally reluctant to share information outside of their circles so as not to jeopardize any potential prosecution. The FBI does promptly share information warning about specific terrorist threats with the CIA and other agencies. But the FBI is far less likely to disseminate terrorist information that may not relate to an immediate threat even though this could be of immense long-term or cumulative value to the intelligence community, in part because investigators lack the training or time to make such assessments. The problem is particularly pronounced with respect to information collected in the FBI's field offices in the United States, most of which never reaches the FBI headquarters, let alone other U.S. Government agencies or departments.

The Commission also recommended that the DOJ prosecute terrorists in an open court when possible and protect the rights of the accused:[120]

> The 1993 World Trade Center bombing brought to light the problem of international terrorists entering and operating in the United States and illustrated the importance of removing suspected terrorists from the United States.

> In 1996, Congress established the Alien Terrorist Removal Court (ATRC). The legislation authorized use of classified information in cases involving the expulsion of suspected terrorists, but the law provided several protections for the accused, including the requirement that the alien be provided an unclassified summary of the classified evidence and appellate review by federal courts. For aliens legally admitted for permanent residence, the law allowed the use of special attorneys who hold security clearances (cleared counsel) who are permitted to review secret evidence on behalf of an alien and challenge its veracity.
>
> The ATRC has never been used. Rather, pursuant to other statutes and case law, the Immigration and Naturalization Service (INS) has acted to remove aliens based on classified evidence presented to an immigration judge without disclosure to the alien or defense counsel.
>
> The U.S. Government should not be confronted with the dilemma of unconditionally disclosing classified evidence or allowing a suspected terrorist to remain at liberty in the United States. At the same time, resort to use of secret evidence without disclosure even to cleared counsel should be discontinued, especially when criminal prosecution through an open court proceeding is an option.

The GAO has suggested that the FBI conduct a national threat and risk assessment. The FBI has begun these assessments, as reported in a July 2000 GAO report:[121]

> Regarding our recommendation for a national level threat and risk assessment, the FBI has agreed to lead such an assessment, using the following process: (1) identify initiatives that identify critical and high threat chemical and biological agents, (2) identify federal agencies and personnel to participate, (3) determine classification requirements, and (4) identify specific inquiries appropriate for participating experts, and compile responses and compare agents. The goal is to provide policy makers with "understandable and discriminatory" data to set funding priorities. The FBI has noted some limitations to its methodology. For example, as a law enforcement agency, it has strict legal limitations on the collection and use of intelligence data. FBI officials told us that the state and local assessments represent a thorough nationwide planning process that will compliment national-level threat and risk assessments and related policy making.

National Domestic Preparedness Office (NDPO)

There is 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:[122]

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:[123]

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: [124]

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.

The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, otherwise known as the Gilmore Commission, also recognized the need for a single agency to simplify the process for local and state responders seeking assistance and supports the concept of the NDPO:[125]

> …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 NDPO is also planning to develop a national counterterrorism strategy. However, the GAO has voiced concern that other agencies were creating a national strategy as well. These multiple strategies could create more confusion, as the GAO reports in July 2000:[126]

> Of additional concern to us is the potential development of additional national strategies by other organizations. In addition to the existing Attorney Generals' 5-year interagency plan, the National Security Council and the FBI's National Domestic Preparedness Office are each planning to develop national strategies. The danger in this proliferation of strategies is that state and local governments—which are already frustrated and confused about the multitude of federal domestic preparedness agencies and programs—may become further confused about the direction and priorities of federal programs to combat terrorism. In our view, there should be only one national strategy to combat terrorism. Additional planning guidance (e.g., at more detailed levels for specific functions) should fall under the one national strategy in a clear hierarchy.

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."[127] 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. Equipment that can be bought with the grant money is stated on NDPO's Standardized Equipment List.[128] In FY 1999, $51.8 million was available, $8 million for state planning and $43.8 million for equipment purchases. The FY 2001 requested budget is $78 million.[129] 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:[130]

> 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 another $2 million to work with DOD to create distance learning material.[131]

A March 2000 GAO report provides the following program description:[132]

> 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.[133]

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.[134]

- 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.[135]

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.

A July 2000 GAO report noted **OSLDPS's** progress in developing local threat and risk assessments:[136]

> Regarding local threat and risk assessments, Justices' Office for State and Local Domestic Preparedness Support and the FBI have worked together to provide a threat and risk assessment tool to state and local governments. This tool includes a step-by-step methodology for assessing threats, risks, and requirements. It also includes information on how to prioritize programs and project spending amounts.

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 in spring and summer of 2000. 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 threats and effects, neither 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.[137]

> 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 the exercises are not required on a regular basis.[138]

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.[139] The other four Consortium members received a total of $2 million and $12 million for FY 1998 and 1999 and will receive $14 million for FY 2000. In FY 1999, the Consortium trained about 3,000 individuals.[140]

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:[141]

> 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.[142]

Total Department of Justice and FBI Funding

Table 4.15 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.[143]

Table 4.15

Department of Justice Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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
WMD Preparedness	**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 CBRN terrorism.[144] 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.[145] Table 4.16 summarizes National Security Community counterterrorism spending. It is adapted from the 2000 OMB counterterrorism

funding report.[146]

Table 4.16

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

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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
WMD Preparedness	**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

Nuclear Regulatory Commission

The following table on Nuclear Regulatory Commission counterterrorism spending adapted from the 2000 OMB counterterrorism funding report shows that most of the money is going towards WMD preparedness, and specifically towards protecting the populace from attacks using nuclear and radiological materials, or strikes on nuclear facilities:[147]

Table 4.17

Nuclear Regulatory Commission Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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
WMD Preparedness	**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

Smithsonian

Table 4.18 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.[148]

Table 4.18

Smithsonian Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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

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.[149]

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 billion[150] 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. $200 million will

go towards new protective measures for embassies such as alarms and perimeter barriers, an increase of $200 million from FY 2000. $342 million will go towards high security readiness, $74 million above FY 2000. $68 million will go towards the State Department's Anti-Terrorism Assistance (ATA) Program, an increase of $35 million from FY 2000. 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:[151]

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).

The State Department also designates Foreign Terrorist Organizations (FTO). The Antiterrorism and Effective Death Penalty Act of 1996 directed the Secretary of State to designate groups that are a threat to the US. The National Commission on Terrorism, also known as the Bremer Commission, asserted that FTO designations are not as credible as they could be because some terrorist organizations are left off the list. The Commission said:[152]

> The FTO designation makes it a crime for a person in the United States to provide funds or other material support (including equipment, weapons, lodging, training, etc.) to such a group. There is no requirement that the contributor know that the specific resources provided will be used for terrorism. In addition, American financial institutions are required under the law to block funds of FTOs and their agents and report them to the government.
>
> The FTO designation process correctly recognizes that the current threat is increasingly from groups of terrorists rather than state sponsors. In addition to deterring contributions to terrorist organizations, FTO designation serves as a diplomatic tool. It provides the State Department with the ability to use a "carrot and stick" approach to these groups, providing public condemnation and a potential for redemption if the groups renounce terrorism.
>
> There is little doubt that all groups currently on the list belong there. But the exclusion, for example, of the Real Irish Republican Army, which carried out the Omagh car bombing in Northern Ireland in 1998 killing 29 people and injuring more than 200, raises questions about completeness of the list. This diminishes the credibility of the FTO list by giving the impression that political or ethnic considerations can keep a group off the list.

However, Ambassador Michael Sheehan, the Coordinator for Counterterrorism, testified before the Senate Foreign Relations Committee explaining why more organizations were not designated FTO. The process of FTO designation is a long one requiring many resources, and the Office of the Coordinator for Counterterrorism is working hard to review more organizations.

Ambassador Sheehan said:[153]

> The Commission observes that it is necessary to sustain credibility and dynamism in the Foreign Terrorist Organization (FTO) process, and I am committed to doing just that--not only with regard to FTOs, but with all of our counterterrorism policy tools. Congress has given us a very effective tool in the Secretary's authority to designate FTOs. Designations under the 1996 law criminalize financial support to a FTO, require U.S. financial institutions to block funds of FTOs and their agents, and render representatives and certain members of the FTO ineligible for visas and admission to the United States. State leads this work in consultation with the Departments of Justice and Treasury and with the intelligence community. In 1997, we designated 30 organizations as FTOs, allowing us to deter terrorist fundraising more effectively. As important, the FTO list has proved invaluable as a diplomatic tool to stigmatize and punish terrorist groups and their supporters around the world.
>
> In 1999, we re-designated 27 FTOs (designations expire after 2 years unless renewed), dropped three groups, and added Usama Bin Ladin's al-Qaida organization. Dropping three FTOs (the Democratic Front for the Liberation of Palestine, the Khmer Rouge, and the Manuel Rodriguez Patriotic Front of Chile) from the list sent an important signal that if you are out of the terrorism business by the standards of U.S. law, you will be dropped from the list.
>
> Because of the significance of FTO designations and because they can be challenged in court, the designation process is painstaking and we are very careful about assembling the evidence that goes into making the case. A single designation consumes hundreds of hours of work carried out by my staff as well as by lawyers and analysts from Justice, Treasury, and the intelligence community. Because of the quality of this effort, we have won all court challenges (for example from the MEK and LTTE) to our designations, thereby further bolstering the credibility of the FTO process.
>
> But sustaining credibility and dynamism in the FTO process is an ongoing challenge, constrained mainly by limited personnel resources. We constantly review and assess various potential groups for addition to the list of FTOs--this can be done at anytime, not just every 2 years. I have directed my staff to review some 10 to 12 new groups before the year is out. We have already added a new officer for 1 year to work on this and would like to bolster our capabilities by adding another fulltime lawyer. But undoubtedly there are some groups that will not be reviewed as soon as I would like. I am not satisfied with the pace of the FTO review process, and will continue to keep pushing my staff and the interagency team that processes these designations.

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 **(TSWG)** is an 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 million 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.[154] 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:[155]

> 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 table on State Department counterterrorism spending adapted from the 2000 OMB counterterrorism funding report shows huge increases in appropriations, mostly to go towards embassy security.[156] The WMD preparedness spending has increased over 210% from FY 1998 to $72 million for the FY 2001 request.

Table 4.19

Department of State Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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
WMD Preparedness	**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 for 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.[157]

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, and the FY 2001 request is $18.6 million.[158]

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 $296.8 million.

Table 4.20 shows total DOT counterterrorism spending. It is adapted from the 2000 OMB counterterrorism funding report, which shows that most of the funding is for the protection transportation systems from conventional attacks and not towards WMD preparedness.[159]

Table 4.20

Department of Transportation Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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
WMD Preparedness	**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

Department of Treasury

The Treasury has responsibility for a number of counterterrorism functions. 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 at major bombing and arson sites within 24 hours. 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 National Commission on Terrorism, also known as the Bremer Commission, suggested that the Treasury Department could be more effective in combating terrorism. The Commission recommended that the Office of Foreign Assets Control (OFAC), which administers economic sanctions, create a unit dedicated to tracking terrorist assets. The Commission recognized OFAC has the capabilities and expertise but has resource constraints. The Commission also suggested that Customs and the Internal Revenue Service have information that could thwart terrorist fundraising. However, the Commission realized there is no agency that analyzes all the data available to the US Government to distribute to the relevant officials.[160]

The following table 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.[161]

Table 4.21

Department of Treasury Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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 4.22 shows counterterrorism spending by US AID. It is adapted from the 2000 OMB counterterrorism funding report and shows over $50 million went towards preparing for and responding to terrorist acts in FY 1998.[162] Virtually all AID spending affects foreign countries, however, and not homeland defense.

Table 4.22

US AID Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
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
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

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

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 of 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 table 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.[163] It should be noted that some experts 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 4.23

Department of Veterans Affairs Spending for Combating Terrorism and WMD Preparedness

	FY1998	FY1999	FY2000	FY2001
Combat Terrorism	**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

V. Costing the Federal Critical Infrastructure and Cyberdefense Program

There is no clear way to cost the federal critical infrastructure program, and only speculative data seems to be available on the efforts being made at the state and local levels, and by the private and civil sector. In the case of governments, there are great many law enforcement, intelligence, counterterrorism, and emergency response efforts that are not dedicated to critical infrastructure per se, but which play an important role in shaping the nation's capabilities.

The Department of Defense and intelligence community's offensive information warfare programs may have a powerful retaliatory and deterrent effect, but are not part of the CIP program. At the same time, a number of departments and agencies seem to have recast programs to take advantage of the funding available as CIP funding, and some have blurred the line between ongoing MIS activity and CIP activity.

There are, however, two major sources of data on dedicated critical infrastructure programs and expenses. One is the National Plan for Information Systems Protection. The other is an analysis of the FY2001 budget performed by OMB. While these two analyses overlap, they both provide different insights into the current federal effort.

The National Plan for Information Systems Estimate

According to the "National Plan for Information Systems Protection" the FY2000 Budget provided a $1.737 billion for government efforts to protect critical infrastructure, a 20 percent or $300 million increase from FY1999. This budget included "funding for new programs to address key vulnerabilities, as well as for ongoing efforts to assure the security of interconnected infrastructures such as telecommunications, banking and finance, energy, transportation, and essential government services." These spending trends are summarized in Table 5.1

Table 5.1

Funding for Critical Infrastructure Protection (in millions of dollars)*

Agency	FY 1998 Actual	FY1999 Actual	FY2000 Enacted
National Security	975	1,185	1,403
Treasury	23	49	76
NASA	41	43	66
Transportation	20	25	51
Justice	26	54	46
NSF	19	21	27
Commerce	9	22	18
HHS	22	12	13
Other	9	18	37
Total	1,144	1,429	1,737

Source: "National Plan for Information Systems Protection" Page 121

CIP spending is divided into three major headings; research and development, federal (non-national security) program operations, and national security program operations. These can be broken down into smaller program operations which encompasses the following areas: vulnerability assessment, risk management, protection and mitigation, intrusion detection, incident response and reconstitution, and education and awareness.[164]

Government spending for CIP by sector weighs heavily in favor of government and emergency services as can be seen in Table 5.2.

Table 5.2

Critical Infrastructure Spending by Sector

	FY1998 Actual	FY1999 Actual	FY2000 Actual
Government and Emergency Services	1042	1282	1565
Information and Communications	41	57	58
Transportation	25	32	57
Electric Power, Oil and Gas Production and Storage, and Water Supply	22	35	30
Banking and Finance	12	17	15
Interdependencies	0	0	8
Total	1,144	1,429	1,737

The plan also provided the following description of how the funding is executed for the

critical infrastructure sectors, the interdependency initiative, and ISACs.

- *Government and Emergency Service*s. Funds for this sector increased by more than 20 percent over the previous Budget, the majority of which support national defense Agencies' efforts to protect critical infrastructures.

- *Information and Communication*s. $33 million is provided to seven Agencies for computer security research and development proposals.

- *Transportatio*n. To address Federal Aviation Administration facilities and information systems, and for programs to reduce vulnerabilities in the National Airspace System and surface transportation systems, the Budget significantly increases funding for this sector from $32 million to $57 million.

- *Electric Power, Oil and Gas Production and Storage, and Water Supply*. The $30 million budgeted for this area supports ongoing programs in the Department of Energy, Department of Interior, and Environmental Protection Agency to advise energy companies and metropolitan water agencies in CIP planning, and for basic research. These efforts advance the goal of public-private partnerships to meet common CIP needs.

- *Banking and Financ*e. The Treasury Department received $16 million to coordinate protection of critical facilities, equipment, and operations in the banking and finance sector. As directed by the PDD, Treasury actively leads sector CIP efforts as well as serving as a model for other sectors.

- *Interdependencie*s. The Budget provides $5 million to DoD, Commerce, and the National Science Foundation to study relationships among infrastructures, and to build up our capability to ensure a reliable, interconnected, and secure information system infrastructure.

- *Information Sharing and Analysis Center*s. $8 million for sector liaison Lead Agencies is provided in the Budget to help establish Information Sharing and Analysis Centers (ISAC). ISACs are designed to foster private sector development and to share recommended practices and standards.

The plan also discussed the new initiatives that advance the goals of the Presidential Decision Directive to protect critical infrastructure. The initiatives listed below may support several critical infrastructure sectors. These initiatives represent only a portion of the total of the $1.737 billion CIP program.

- *Computer Security Research and Development Initiativ*e. $80 million is allocated for R&D to study safeguarding networks and databases, and detection of anomalous activities, "trap doors," Trojan Horses, and other malicious code.

- *Information Sharing and Analysis Center*s. As noted earlier, ISACs are designed to foster private sector development and share recommended practices and standards. $8 million is set aside in the Budget to help establish ISACs.

In addition to these new programs, the plan continued to support the following ongoing

efforts:

- *National Defense Infrastructur*e. The Budget increases resources to protect critical infrastructures that support national security requirements, bringing this funding to over $1.4 billion.

- *Federal Aviation Administration and National Airspace Syste*m. FAA funding for CIP doubled, from $23 million to almost $50 million, to better protect FAA facilities and information systems, and for programs to reduce vulnerabilities in the National Airspace System.

- *Fighting Cybercrim*e. The Budget provides $46 million to enhance the investigative and prosecutorial efforts of the FBI, the U.S. Attorney, and the Justice Department's Criminal Division.

- *Critical Infrastructure Assurance Office (CIAO*). The CIAO received $3 million to support efforts to develop a national infrastructure assurance plan and coordinate a national education and awareness program.

The OMB Analysis

OMB has found it difficult to create an accurate analysis of the budgetary data on CIP programs because of the lack of any clear definition of what programs should be included, and the difficulties this has caused for the collection of data. The government is experiencing what the Plan calls " a precipitous learning curve" in its attempts to provide consolidated data and adequate descriptions and data presentations. To deal with this matter the OMB and the National Security Council developed a process to review high-priority national security programs that cross Agency lines. The process calls for program recommendations "being made on a Government-wide context rather than Agency by Agency."

There are four phases in this new approach:[165]

- *Program Revie*w. Interagency working groups, chaired by the National Security Council or the Office of Science and Technology Policy, review the crosscutting issues in a Government-wide context. The groups identify gaps and duplications in the national effort and develop detailed programmatic initiatives to increase our effectiveness in countering unconventional threats.

- *Budget Revie*w. For each issue area, a budget subgroup consisting of Agency program staff, Agency budget staff, and OMB examiners develop budget-quality cost estimates for the programmatic initiatives. This

phase is not an endorsement of funding for the initiatives, but instead is an effort to provide realistic, well-justified cost estimates.

- *Agency Action on Recommendation*s. The working groups then prioritize the initiatives and transmit them as funding recommendations to the Agencies. Agencies will address the recommendations in the context of other priorities and fiscal constraints in their fall budget submissions to OMB.

- *Review of Agency Actio*n. OMB will review Agency action on the recommendations and make any necessary course corrections in Passback based on information from the working groups, other Agency priorities, and available resources.

These efforts to improve collection and analysis of CIP data were evident in the development of the President's Proposed Budget for FY2001. The process was completed under an accelerated schedule for the FY2001 budget, and will be used to develop the FY2002 budgets for crosscutting issues. Figure 5.1 depicts that schedule.

To expedite these efforts to improve data on CIP the process for the President's Proposed Budget for FY2001 were placed and completed under an accelerated schedule. Programmatic Recommendations were to be completed by the end of March. The developments of IWG budget recommendations were to begin in March and be completed by the end of April. From May through July IWG recommendations were to be integrated into Agency budgets. August through October Agency actions were to be reviewed and October through December outstanding concerns were to be resolved.[166]

Annual Report to Congress on Combating Terrorism

As required by Section 1050 of FY 1998 National Defense Authorization Act, the Administration provided information on Executive branch funding efforts to combat terrorism. Following legislation required an additional annex report on domestic preparedness.[167] The 2000 report combines information on programs funded to combat terrorism, enhance WMD preparedness and protect critical infrastructures. The report also focused on the government wide review process launched in the "National Plan for Information Systems Protection" discussed in the aforementioned section.

It should be stressed, however, that the report does not include any aspects of offensive

information and cyberwarfare that could be used to deter or respond to attacks. It also seems to omit any investment in designing less vulnerable systems, and may ignore many investments in back-up or alternative systems. These problems are characteristic of all unclassified reporting on the nature and cost of federal critical infrastructure protection efforts.

According to the report the FY 2001 budget calls for $2 billion for critical infrastructure protection/cybercrime.

> The budget proposes over $2 billion for critical infrastructure protection. These funds support a national effort to assure the security of infrastructures in both the Government and the private sector that are necessary to ensure our national security, national economic security, and public health and safety. The proposed funding for FY2001 represents a 15% increase over the FY2000 enacted level. It includes a 31% increase for R&D programs to develop the tools needed for effective infrastructure protection, bringing CIP R&D to a total $606 million. Of the total CIP budget, $1.7 billion protects Federal systems and ensures our ability to provide essential government services to the public. About $300 million fund agency efforts to provide assistance to the private sector, where most of the Nation's critical infrastructure resides.[168]

For information and telecommunication portions of infrastructure protection the report states that the administration has only begun encouraging "the operational changes necessary" for the protection of information systems. The Report points to the National Plan for Information Systems Protection as the guide for both government protection of its own infrastructures and outreach to the private sector.[169]

> This sector is arguably the most critical in the CIP effort, because almost all other sectors depend to some extent on computers and other information networks. The Administration has had considerable success in reaching out to industry associations to establish public/private partnerships and for input into our R&D agenda, but we have only begun to encourage the operational changes necessary for effective protection of this sector. The National Plan for Information Systems Protection is intended to provide strategic guidance for government protection of its own infrastructures as well as for outreach to the private sector. The Administration is committed to implementing the Plan in a manner so as to ensure consistency with other national policies, including privacy policies.

According to the report funding for CIP information systems protection has tripled since FY 1998. This development is driven by the growth in R&D that has reached over $606 million in FY2001 mostly performed by the national security community. [170]

Government Wide Spending on CIP

The report separated out two main sectors of CIP spending, funding for protection of federal infrastructure and funding for CIP assistance and outreach to the public sector. In FY2001 the latter made for 16 percent of the President's CIP budget, while funding for the protection of cyber and physical federal infrastructure makes up the lion's share. CIP assistance and public outreach includes funding for information and communications, banking and finance, transportation, energy, water supply, emergency services and interdependencies. Descriptions of sectors of particular interest are:

> *Government Services*
>
> As might be expected, most agency funding supports the protection of internal agency infrastructures. 84% of total CIP funding relates to government services. The Administration has significantly increased investment in this area (increasing 65% since FY1998)... [171]
>
> *Information and Communications*
>
> This sector is arguably the most critical in the CIP effort, because almost all other sectors depend to some extent on computers and other information networks. The Administration has had considerable success in reaching out to industry associations to establish public/private partnerships for input into our R&D agenda, but we have only begun to encourage the operational changes necessary for effective protection of this sector. The National Plan for Information Systems Protection is intended to provide strategic guidance for government protection of its own infrastructures as well as outreach to the private sector. The Administration is committed to implementing the Plan in a manner as to ensure consistency with other national policies, including privacy policies...
>
> *Banking and Finance*
>
> We have made significant progress in the Banking and Finance sector because the industry is sensitive to this issue from its experience with cybercrime. Treasury is the lead agency for outreach and assistance to this sector. In October 1999 the industry, with significant assistance from Treasure established an information sharing and analysis center (IASC) to facilitate exchange of warning and best practices information in this sector. Funding in this sector reflects Treasury Department activities for physical and cyber protection of currency production, and Secret Service, Justice and FBI cyber-crime investigations.
>
> *Emergency Services*
>
> The Department of Justice/FBI is the lead agency for outreach and assistance to the emergency law enforcement service sector and is responsible for about half the funding for emergency services CIP. Justice funds efforts to address global computer crime and works with other agencies, the private sector, academic institutions, and foreign representatives to prevent, investigate, and prosecute computer terrorists. Justice improves the domestic and

> international infrastructure by providing assistance and advice to investigative agencies. FBI activities include prevention of attacks, computer intrusion response and investigation, and prosecution of computer terrorist.

Most of the money goes to funding Government Services. This may call into question government's commitment to shared cooperation with the public sector when most CIP money is spent within government on government infrastructure.

Of the funding for Federal Infrastructure Protection $740 million of the almost 1.7 billion requested is slated for "system protection." To date the drafted **r**eport has not further defined what constitutes "system protection" in detail. Roughly half of the money requested for system protection has been for "multiple program areas" which are also not defined in the draft. Intrusion monitoring and response and threat, vulnerability and risk assessments have received the next greatest amount of requested funding as indicated by the $249.27 million and $229.15 million request in FY 2001.

The overall trends in CIP funding are shown in Tables 5.3 and 5.4, and Charts 5.1 and 5.2.

Table 5.3

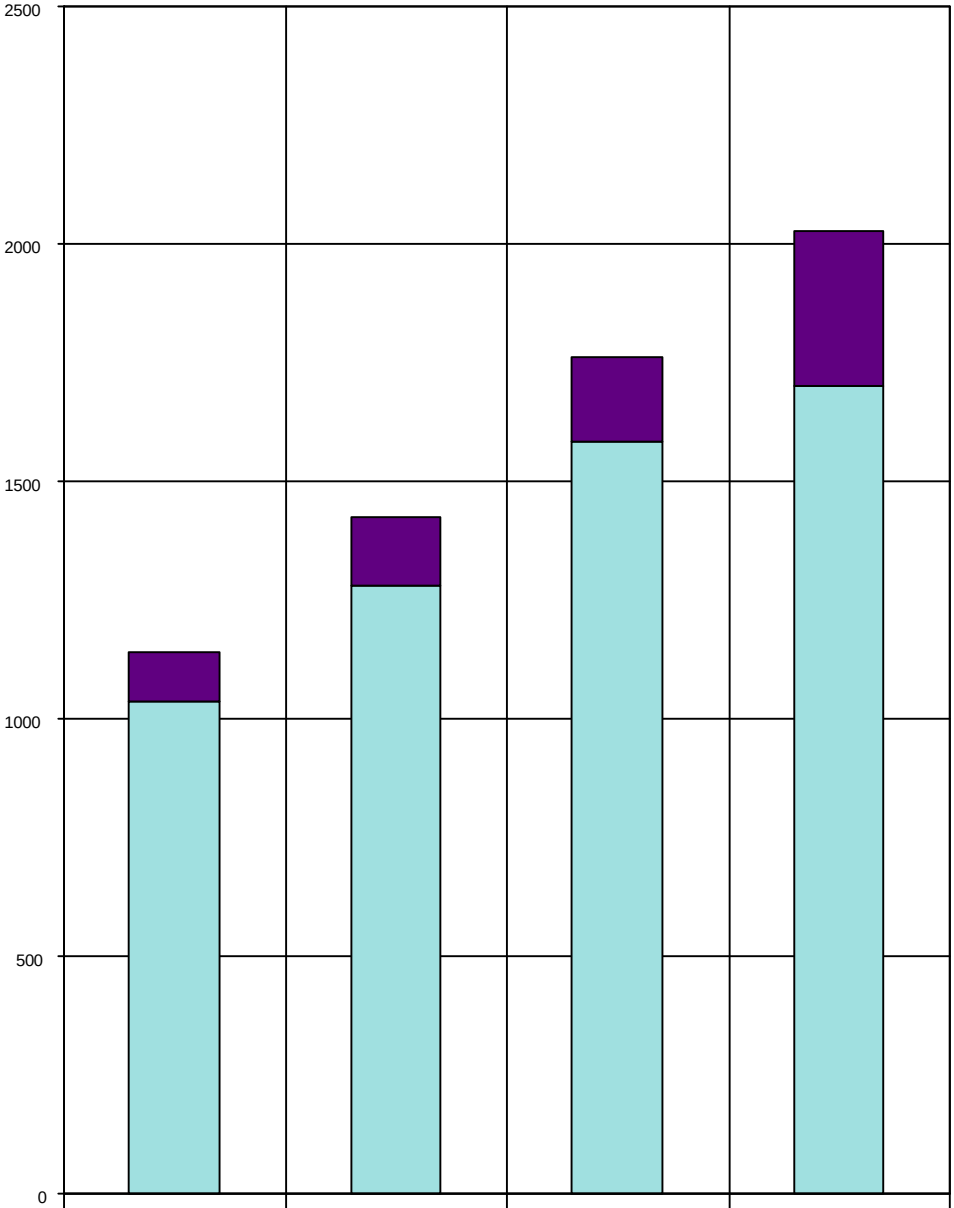
Government-wide Spending for Critical Infrastructure Protection

	FY1998	FY1999	FY2000	FY2001
Federal Government				
Critical Infrastructure Protection	1,142.00	1,428.57	1,759.42	2,027.25
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

Chart 5.1

Federal Spending on CIP by Activity: FY1998-FY20001

(Current $US Millions)



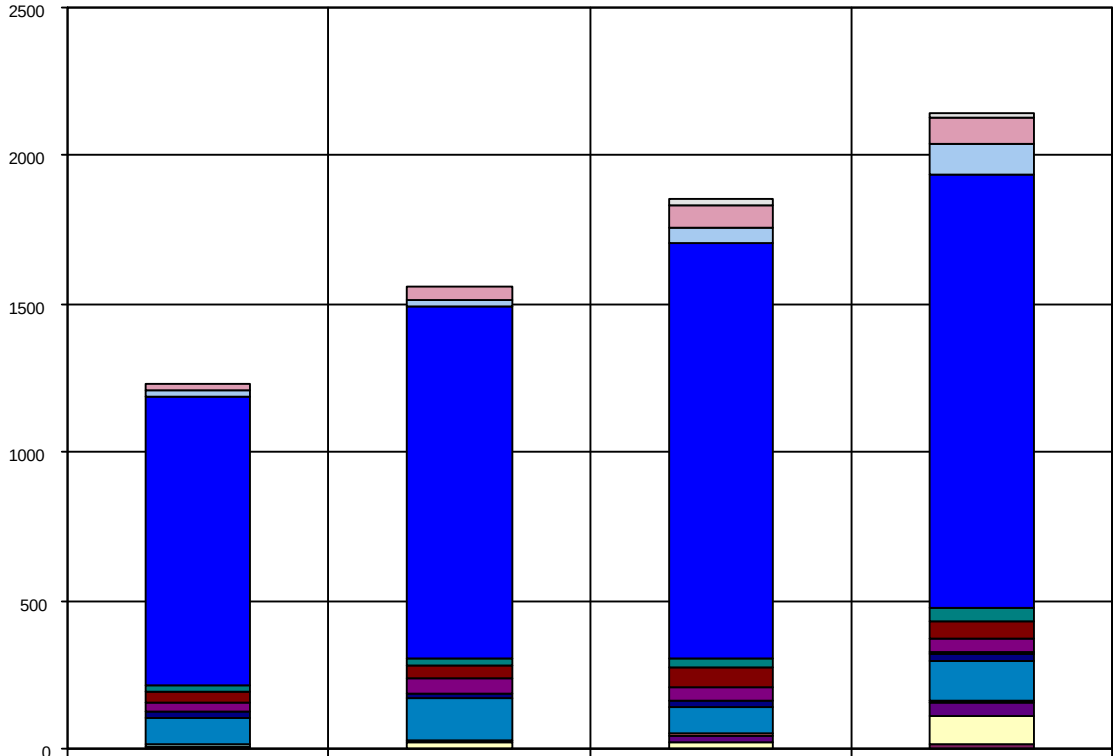
	FY1998	FY1999	FY2000	FY2001
Assist/Outreach to Private Sector	103.21	148.66	175.16	328.22
Federal Infrastructure Protection	1038.79	1278.91	1584.26	1699.03

Source: Adapted by Anthony H. Cordesman

Chart 5.2

Federal Spending on CIP by Agency: FY1998-FY2001 – Part One

(Current $US Millions)



	FY1998	FY1999	FY2000	FY2001
Veterans Affairs	0	0	17.33	17.39
Treasury	22.91	48.89	76.21	87.03
Transportation	20.33	24.88	50.68	99.34
OPM	0	0	2	7
NRC	0	0.2	0	0.25
National Secur	974.56	1185.22	1402.94	1458.91
NSF	19.15	21.42	26.65	43.85
NASA	41	43	66	61
Justice	25.61	54.09	44.02	45.51
Interior	1.29	1.6	2.65	1.83
HHS	21.85	14.39	22.11	27.6
GSA	89.6	136.5	92.8	132.36
FEMA	0	0	0.8	1.47
EPA	0.12	0.24	0.08	2.3
Energy	1.5	3.6	21.98	45.3
Education	3.59	4.45	5.23	2.51
Commerce	9.35	21.81	17.75	92.1
Agriculture	0.7	1.22	2.51	17.89

Source: Adapted by Anthony H. Cordesman

Table 5.4

Federal Spending on CIP by Agency: FY1998-FY2001 – Part Two
(Current $US Millions)

	FY1998	FY1999	FY2000	FY2001
Agriculture	0.70	1.22	2.51	17.89
Commerce	9.35	21.81	17.75	92.10
Education	3.59	4.45	5.23	2.51
Energy	1.50	3.60	21.98	45.30
EPA	0.12	0.24	0.08	2.30
FEMA	0.00	0.00	0.80	1.47
GSA	89.60	136.50	92.80	132.36
HHS	21.85	14.39	22.11	27.60
Interior	1.29	1.60	2.65	1.83
Justice	25.61	54.09	44.02	45.51
NASA	41.00	43.00	66.00	61.00
NSF	19.15	21.42	26.65	43.85
National Security	974.56	1185.22	1402.94	1458.91
NRC	0.00	0.20	0.00	0.25
OPM	0.00	0.00	2.00	7.00
Transportation	20.33	24.88	50.68	99.34
Treasury	22.91	48.89	76.21	87.03
Veterans Affairs	0.00	0.00	17.33	17.39

Source: Adapted by Anthony H. Cordesman

Efforts by Federal Agency

Table 5.5 shows an OMB analysis of the major CIP activities in each federal department and agency. In shaping these activities, the federal government has attempted to coordinate the response of each agencies' own infrastructure security and to educate and partner with private industry. The role of each agency is matched up with national infrastructure sectors to which its mission relates, and each agency is given a responsibility to work with the private sector of that particular infrastructure.

For example, the Department of Commerce is the lead agency in the communications sector. The Department of Transportation is the lead agency for transportation CIP. The Treasury Department is the lead agency for banking and finance. DOE partners with the energy community, EPA provides a limited partnership with the water suppliers (which now fall mostly within state jurisdiction). DOJ/FBI is the lead agency for assistance to the law enforcement and emergency management community.

Table 5.5

Agency Spending for Critical Infrastructure Protection

	FY1998	FY1999	FY2000	FY2001
Department of Agriculture				
Critical Infrastructure Protection	**0.70**	**1.22**	**2.51**	**17.89**
Federal Infrastructure Protection	0.00	0.22	1.11	16.89
Intrusion Monitoring and Response	0.00	0.22	1.11	6.44
System Protection	0.00	0.00	0.00	9.00
Threat/Vulnerability/Risk Assessments	0.00	0.00	0.00	1.46
CIP Assistance/Outreach to Private Sector	0.70	1.00	1.40	1.00
Threat/Vulnerability/Risk Assessments	0.70	1.00	1.40	1.00
Department of Commerce				
Critical Infrastructure Protection	**9.35**	**21.81**	**17.75**	**92.10**
Federal Infrastructure Protection	2.00	10.84	6.75	15.58
Multiple Program Areas	0.00	3.00	1.50	3.00
System Protection	2.00	7.84	5.25	6.33
Threat/Vulnerability/Risk Assessments	0.00	0.00	0.00	6.25
CIP Assistance/Outreach to Private Sector	7.35	10.97	11.00	76.52
Education and Training	0.00	0.00	0.00	0.50
Intrusion Monitoring and Response	0.50	0.62	0.65	0.62

Multiple Program Areas	0.00	3.00	1.50	56.50
Public Awareness/Outreach	0.00	0.00	0.00	0.50
System Protection	6.85	7.35	7.85	9.85
Threat/Vulnerability/Risk Assessments	0.00	0.00	1.00	8.55
Department of Education				
Critical Infrastructure Protection	**3.59**	**4.45**	**5.23**	**2.51**
Federal Infrastructure Protection	3.58	4.44	5.22	2.50
Education and Training	0.01	0.07	0.03	0.03
Intrusion Monitoring and Response	1.46	2.06	2.44	2.25
Reconstitution	0.39	0.51	0.52	0.00
System Protection	1.39	1.64	2.06	0.10
Threat/Vulnerability/Risk Assessments	0.33	0.16	0.17	0.13
CIP Assistance/Outreach to Private Sector	0.01	0.01	0.01	0.01
Multiple Program Areas	0.01	0.01	0.01	0.01
Department of Energy				
Critical Infrastructure Protection	**1.50**	**3.60**	**21.98**	**45.30**
Federal Infrastructure Protection	0.00	1.80	17.56	32.30
Education and Training	0.00	1.00	1.00	3.50
Intrusion Monitoring and Response	0.00	0.80	7.34	9.30
Multiple Program Areas	0.00	0.00	1.00	2.00
System Protection	0.00	0.00	6.18	15.50
Threat/Vulnerability/Risk Assessments	0.00	0.00	2.04	2.00
CIP Assistance/Outreach to Private Sector	1.50	1.80	4.42	13.00
Intrusion Monitoring and Response	0.00	0.10	0.16	0.60
Legislative Initiatives and Legal Issues	0.00	0.00	0.00	0.60
Multiple Program Areas	1.50	1.50	0.80	1.50
Public Awareness/Outreach	0.00	0.00	2.00	0.20
Reconstitution	0.00	0.00	0.00	2.00
System Protection	0.00	0.00	0.00	1.70
Threat/Vulnerability/Risk Assessments	0.00	0.20	1.46	6.40
Environmental Protection Agency				
Critical Infrastructure Protection	**0.12**	**0.24**	**0.08**	**2.30**
Federal Infrastructure Protection	0.11	0.23	0.00	0.00
Threat/Vulnerability/Risk Assessment	0.11	0.23	0.00	0.00
Federal Emergency Management Agency				
Critical Infrastructure Protection	**0.00**	**0.00**	**0.80**	**1.47**
Federal Infrastructure Protection	0.00	0.00	0.00	1.17
Threat/Vulnerability/Risk Assessments	0.00	0.00	0.00	1.17
CIP Assistance/Outreach to Private Sector	0.00	0.00	0.80	0.30
Multiple Program Areas	0.00	0.00	0.80	0.15
Public Awareness/Outreach	0.00	0.00	0.00	0.15
General Services Administration				
Critical Infrastructure Protection	**0.00**	**3.00**	**0.00**	**15.40**
Federal Infrastructure Protection	0.00	2.00	0.00	15.40
Intrusion Monitoring and Response	0.00	2.00	0.00	15.40
CIP Assistance/Outreach to Private Sector	0.00	1.00	0.00	0.00
Multiple Program Areas	0.00	1.00	0.00	0.00
Department of Health and Human Services				
Critical Infrastructure Protection	**21.85**	**14.39**	**22.11**	**27.60**
Federal Infrastructure Protection	21.85	14.39	22.11	25.60
Multiple Program Areas	18.40	8.17	8.70	9.70

System Protection	2.45	5.02	12.21	14.70
Threat/Vulnerability/Risk Assessments	1.00	1.20	1.20	1.20
CIP Assistance/Outreach to Private Sector	0.00	0.00	0.00	2.00
Multiple Program Areas	0.00	0.00	0.00	2.00
Department of the Interior				
Critical Infrastructure Protection	**1.29**	**1.60**	**2.65**	**1.83**
Federal Infrastructure Protection	0.64	0.80	1.33	0.91
Threat/Vulnerability/Risk Assessments	0.64	0.80	1.33	0.91
CIP Assistance/Outreach to Private Sector	0.64	0.80	1.33	0.91
Department of Justice				
Critical Infrastructure Protection	**25.61**	**54.09**	**44.02**	**45.51**
Federal Infrastructure Protection	0.84	1.73	1.43	1.50
Legislative Initiatives and Legal Issues	0.12	0.20	0.20	0.23
Multiple Program Areas	0.72	1.54	1.24	1.27
CIP Assistance/Outreach to Private Sector	24.77	52.36	42.59	44.01
Legislative Initiatives and Legal Issues	1.58	2.60	2.60	3.07
Multiple Program Areas	23.19	49.76	39.98	40.94
National Aeronautics and Space Administration				
Critical Infrastructure Protection	**41.00**	**43.00**	**66.00**	**61.00**
Federal Infrastructure Protection	41.00	43.00	66.00	61.00
Education and Training	1.00	1.00	2.00	2.00
Intrusion Monitoring and Response	16.00	17.00	25.00	24.00
Multiple Program Areas	5.00	5.00	5.00	5.00
System Protection	18.00	19.00	32.00	28.00
Threat/Vulnerability/Risk Assessment	1.00	1.00	2.00	2.00
National Science Foundation				
Critical Infrastructure Protection	**19.15**	**21.42**	**26.65**	**43.85**
Federal Infrastructure Protection	0.57	0.60	0.63	10.87
Education and Training	0.00	0.00	0.00	10.20
System Protection	0.57	0.60	0.63	0.67
CIP Assistance/Outreach to Private Sector	18.58	20.82	26.02	32.98
Intrusion Monitoring and Response	0.00	0.51	0.53	0.54
Multiple Program Areas	0.00	0.00	-	4.00
System Protection	17.21	18.34	23.11	25.81
Threat/Vulnerability/Risk Assessments	1.37	1.97	2.38	2.63
National Security				
Critical Infrastructure Protection	**974.56**	**1,185.22**	**1,402.94**	**1,458.91**
Federal Infrastructure Protection	956.27	1,160.80	1,379.56	1,420.05
Education and Training	36.53	46.42	73.61	81.46
Intrusion Monitoring and Response	108.66	158.70	172.79	187.18
Multiple Program Areas	218.33	265.01	379.77	348.08
Reconstitution	25.50	29.17	15.40	5.19
System Protection	503.58	584.28	630.23	638.12
Threat/Vulnerability/Risk Assessment	63.67	77.22	107.75	160.01
CIP Assistance/Outreach to Private Sector	18.29	24.42	23.38	38.86
Intrusion Monitoring and Response	0.00	0.80	0.24	0.24
Multiple Program Areas	13.29	15.52	18.04	18.82
System Protection	5.00	7.15	5.10	4.80
Threat/Vulnerability/Risk Assessment	0.00	0.95	0.00	15.00
Nuclear Regulatory Commission				

Critical Infrastructure Protection	**0.00**	**0.20**	**0.00**	**0.25**
Federal Infrastructure Protection	0.00	0.20	0.00	0.25
Reconstitution	0.00	0.20	0.00	0.00
Threat/Vulnerability/Risk Assessment	0.00	0.00	0.00	0.25
Office of Personnel Management	**0.00**	**0.00**	**2.00**	**7.00**
Critical Infrastructure Program	**0.00**	**0.00**	**2.00**	**7.00**
Federal Infrastructure Program	0.00	0.00	2.00	7.00
Education and Training	0.00	0.00	2.00	7.00
Department of Transportation				
Critical Infrastructure Protection	**20.33**	**24.88**	**50.68**	**99.34**
Federal Infrastructure Protection	0.94	1.42	1.49	2.32
Reconstitution	0.30	0.30	0.37	0.45
System Protection	0.64	1.12	1.12	1.12
Threat/Vulnerability/Risk Assessments	0.00	0.00	0.00	0.75
CIP Assistance/Outreach to Private Sector	19.39	23.46	49.19	97.03
Intrusion Monitoring and Response	0.00	0.00	0.00	1.50
Multiple Program Areas	0.00	0.00	0.00	4.00
Public Awareness/Outreach	0.00	0.00	0.10	2.05
Reconstitution	0.00	0.00	0.00	0.13
System Protection	7.47	8.95	19.76	28.90
Threat/Vulnerability/Risk Assessments	11.92	14.51	29.33	60.45
Department of Treasury				
Critical Infrastructure Protection	**22.91**	**48.89**	**76.21**	**87.03**
Federal Infrastructure Protection	10.94	35.86	61.27	67.73
Intrusion Monitoring and Response	1.50	5.50	4.70	4.70
System Protection	4.64	11.06	4.47	10.93
Threat/Vulnerability/Risk Assessments	4.80	19.30	52.10	52.10
CIP Assistance/Outreach to Private Sector	11.96	13.03	14.96	19.30
Education and Training	1.14	1.60	1.60	2.00
Intrusion Monitoring and Response	3.25	3.17	3.12	3.12
Multiple Program Areas	0.00	0.00	0.00	4.00
Public Awareness/Outreach	0.00	0.00	0.20	0.20
System Protection	0.78	1.36	1.24	1.08
Threat/Vulnerability/Risk Assessments	6.80	6.90	8.80	8.90
Department of Veterans Affairs				
Critical Infrastructure Protection	**0.00**	**0.00**	**17.33**	**17.39**
Federal Infrastructure Protection	0.00	0.00	17.33	17.39
Education and Training	0.00	0.00	0.82	0.81
System Protection	0.00	0.00	15.60	15.65
Threats/Vulnerability/Risk Assessments	0.00	0.00	0.91	0.93

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," Figures part of 2001 budget

Department of Agriculture

Money slated for DOA federal infrastructure protection has grown from zero funding, across the board for any CIP related programs in FY 1998.[172] In FY2001 DOA requested roughly $17.89 million for protection of federal infrastructure and assistance/outreach to private

sector a request raise of over $15 million from FY2000 and over a $16 million raise from FY 1999.[173]

Of the nearly $18 million dollar request, $16.89 million is to fund the protection of federal infrastructure side of CIP with the majority of the money going to system protection and intrusion monitoring and response. The rest of the money is earmarked for threat and vulnerability assessment. For public-private partnership the Administration has requested $1 million, for threat vulnerability and assessments, funding has stayed between the $700,000 dollar range in FY 1998 up to $1.4 million in FY2000.

Table 5.6

Agency Spending for Critical Infrastructure Protection

	FY1998	FY1999	FY2000	FY2001
Department of Agriculture				
Critical Infrastructure Protection	**0.70**	**1.22**	**2.51**	**17.89**
Federal Infrastructure Protection	0.00	0.22	1.11	16.89
Intrusion Monitoring and Response	0.00	0.22	1.11	6.44
System Protection	0.00	0.00	0.00	9.00
Threat/Vulnerability/Risk Assessments	0.00	0.00	0.00	1.46
CIP Assistance/Outreach to Private Sector	0.70	1.00	1.40	1.00
Threat/Vulnerability/Risk Assessments	0.70	1.00	1.40	1.00

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," Figures part of 2001 budget

Department of Commerce

The Department of Commerce (DOC) plays a lead role "in establishing and enhancing the partnership between the Federal government and the private sector to protect the Nation's infrastructure." As a result of PDD-63, the DOC was assigned three major functions: "the Critical Infrastructure Assurance Office (CIAO), lead agency responsibilities for the information and communications sector, and CIP research and development responsibilities."[174]

The bureaus within the department that support these activities are: the Bureau of Export

Administration that houses CIAO. The National Telecommunications and Information Agency (NTIA) which leads outreach and assistance to the information and communications sector. The National Institute of Standards and Technology (NIST), along with the National Oceanic and Atmospheric Administration and NTIA conduct research to develop CIP technology, standards and best practices. The following is a breakdown of the key DOC initiatives with FY 2001 budget request, as reported by the "Annual Report to Congress on Combating Terrorism" 2000

- ***Lead Agency for Information and Communications Sector ($3.5million):*** NTIA's responsibility as lead agency is to develop an effective partnership relationship with the private sector to identify and resolve infrastructure protection problems and technology needs. NTIA will raise industry awareness of the nature of threats and vulnerabilities within this sector and facilitate industry efforts in sharing information to improve preparedness against threats.

- ***Critical Infrastructure Assurance Office ($6 million):*** The CIAO functions as the Federal Government's interagency coordination mechanism for implementation of PDD-63. It supports the National Coordinator's work with government agencies in the private sector in developing a plan to reduce the exposure to attack of the Nation's critical infrastructures. It coordinates the Administration's Partnership for Critical Infrastructure Security, a public-private initiative designed to promote cross-industry dialogue and participation in developing the next version of the National Infrastructure Assurance Plan. Analytical support for the CICG and lead agencies includes assisting agencies in identifying their dependencies on critical infrastructures; summarizing key infrastructure laws; identifying and compiling cyber and physical security standards; cataloging training programs; and analyzing model mutual aid agreements to assist state and local governments and the private sector in protection and restoring critical facilities.

- ***Institute for Information Infrastructure Protection (I3P) ($50 million):*** The budget proposes the establishment of an Institute housed at NIST to work collaboratively with industry and academia on key information infrastructure protection technologies, filling research and other key technology gaps that neither the private sector nor the government's national security community would otherwise address. Research work will be performed at existing institutions including private corporations, universities, and non-profit research institutes, seeking to engage the nation's finest technical experts to address priority research areas.

- ***Expert Review Team ($5 million):*** The budget proposes the establishment of a technical assistance team housed at NIST to assist agencies in adhering to Federal computer security requirements. The team would be responsible for helping Agencies identify vulnerabilities, plan secure systems, and implement Critical Infrastructure Protection plans. The team would also assist agencies with specific computer security projects, including computer intrusion drills and security fixes for systems identified to have unacceptable security risks.

- ***CIP Research and Development (13.3 million):*** DOC's extensive research addresses deficiencies in current software development and assurance methods, including technology development for system survivability, secure Internet protocols, and encryption.[175]

Despite its seeming importance to CIP, DOC suffered a cut of $4 million from $21.8 million in FY99 enacted to $17.8 million in FY00 enacted.[176] Yet the Administration in FY01 is

requesting a significant increase to $92.1 million giving the DOC the highest requested budget for CIP behind National Security if enacted.

DOC status as a lead agency for CIP has not kept it from suffering budget cuts. Agency funding for federal infrastructure protection and assistance/outreach efforts was cut from $21.81 million in FY 1999 to $17.75 million in FY 2000. According to the report Congress rejected all of Commerce's request for lead agency activities which accounted for $3.5 million.[177]

In FY 2001, however, the Administration has requested a considerable increase in funding to $92.10 million in the 01 budget. The cause for the significant rise in request lies in the DOC's fulfilling of its assigned PDD-63 functions. Of the $92.10 million, $3.5 million is to be allocated in the budget to allow DOC to serve as the lead agency for the information and communications sector. $6 million is to be assigned to CIAO. A great portion of the newly requested funds, $50 million, if enacted would go to the establishment of the Institute for Information Infrastructure Protection (I3P).

This new entity would be housed at NIST and tasked with the work of collaborating with industry and academia "on key information infrastructure protection technologies, filing research and other key technology gaps that neither the private sector nor the government's national security community would otherwise address. Research work will be performed at existing institutions including private corporations, universities, and non-profit research institutes, engaging our nation's finest technical experts to address priority research areas."[178]

Another $5 million would be used to establish of an Expert Review Team housed in NIST that would assist agencies in becoming compliant with Federal computer security requirements. This team would help Agencies identify vulnerabilities, plan secure systems, implement CIP plans and assist with computer security projects such as computer intrusion drills and security fixes for at risk systems.[179]

A total of $13.3 million of the President's budget is to be marked for CIP R&D which according to the report includes "DOC's extensive research address deficiencies in current

software development and assurance methods, including technology development for system survivability, secure Internet protocols, and encryption."[180] This prose raises some basic questions: Can $13 of government funds really make a difference when private industry can kick in more in R&D.

Table 5.7

Department of Commerce Spending for Critical Infrastructure Protection

	FY1998	FY1999	FY2000	FY2001
Department of Commerce				
Critical Infrastructure Protection	9.35	21.81	17.75	92.10
Federal Infrastructure Protection	2.00	10.84	6.75	15.58
Multiple Program Areas	0.00	3.00	1.50	3.00
System Protection	2.00	7.84	5.25	6.33
Threat/Vulnerability/Risk Assessments	0.00	0.00	0.00	6.25
CIP Assistance/Outreach to Private Sector	7.35	10.97	11.00	76.52
Education and Training	0.00	0.00	0.00	0.50
Intrusion Monitoring and Response	0.50	0.62	0.65	0.62
Multiple Program Areas	0.00	3.00	1.50	56.50
Public Awareness/Outreach	0.00	0.00	0.00	0.50
System Protection	6.85	7.35	7.85	9.85
Threat/Vulnerability/Risk Assessments	0.00	0.00	1.00	8.55

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," Figures part of 2001 budget

Critical Infrastructure Assurance Office

Originally called the National Plan Coordination Staff in PDD-63, the Critical Infrastructure Assurance Office (CIAO) serves to coordinate several elements of the Administration's CIP mechanisms.

Department of Energy

Being the lead agency for energy infrastructures, DOE's CIP responsibilities include collaborating with private sector energy infrastructure elements for critical infrastructure assurance.

Funding for CIP within DOE has grown from virtually nothing in FY 1998, with an enacted budget of $1.5 million to a much larger requested budget of $45.3 million in FY 2001.

The greatest expansion of funds has been seen in the past two years. For FY 1998 and FY 1999 the department delegated little, if any funds to CIP. For protection of federal infrastructure, DOE received no funds in FY 1998 and $1.8 million in FY 1999. In the past two fiscal years DOE has seen an increase in funding for federal infrastructure protection to $17.56 million in FY2000 and a requested $32.3 million in FY2001. The bulk of the money requested in FY2001 is set to go to system protection efforts with $15.5 million devoted to that effort in the report.

CIP outreach funding has increased from $1.5 million in FY1998 to $13 million requested in the FY2001 budget. Most of the funding requested in FY2001 is to go to threat, vulnerability, and risk assessments.

The programs highlighted by OMB in the report were the DOE CIP program and the Cyber Security Program. The DOE CIP program is for the focus on "thrust areas of Analysis and Risk Management and Protection and Mitigation Technologies." The report states that this will provide real-time control mechanisms, integrated multi-sensor and warning systems, and risk management and consequence analysis tools that will help the national energy sector address the physical and cyber threats to, and vulnerabilities of the energy infrastructures. DOE will develop infrastructure interdependence tools to improve the capability to assess the technical, economic and national security implications of cascading energy infrastructure disruptions and to improve the reliability and security of the Nation's interdependent energy grid. This program will involve collaboration between DOE and the major stakeholders, including private sector owners of energy elements, other federal agencies involved in critical infrastructure protection, and state and local governments. The national laboratories, academia, and private research organizations will participate in developing and implementing the research program.[181]

A total of $30 million is requested for the Cyber Security Program to allow DOE to fulfill its responsibilities in protecting its cyber systems. This program supports development of high level, consistent, risk management-based policies and implementation guidance for the protection of cyber assets; training to provide consistent core training requirements for cyber security professionals, system administrators, senior management, and general users; operations

to provide departmental capabilities for cyber incident response, core cyber security architecture, cyber intrusion detection and reporting, and Public Key Infrastructure architecture; and technical development to provide tools to eliminate cyber security vulnerabilities where commercial or Government products are not available. [182]

As indicated by the recent rise in funding for CIP within the DOE, however, DOE is just beginning to get the kind of funding need for CIP preparedness. DOE only devoted limited funding to protection of its infrastructure in 1998 and only $1.8 million in 1999.

Table 5.8

Department of Energy Spending for Critical Infrastructure Protection

	FY1998	FY1999	FY2000	FY2001
Department of Energy				
Critical Infrastructure Protection	1.50	3.60	21.98	45.30
Federal Infrastructure Protection	0.00	1.80	17.56	32.30
Education and Training	0.00	1.00	1.00	3.50
Intrusion Monitoring and Response	0.00	0.80	7.34	9.30
Multiple Program Areas	0.00	0.00	1.00	2.00
System Protection	0.00	0.00	6.18	15.50
Threat/Vulnerability/Risk Assessments	0.00	0.00	2.04	2.00
CIP Assistance/Outreach to Private Sector	1.50	1.80	4.42	13.00
Intrusion Monitoring and Response	0.00	0.10	0.16	0.60
Legislative Initiatives and Legal Issues	0.00	0.00	0.00	0.60
Multiple Program Areas	1.50	1.50	0.80	1.50
Public Awareness/Outreach	0.00	0.00	2.00	0.20
Reconstitution	0.00	0.00	0.00	2.00
System Protection	0.00	0.00	0.00	1.70
Threat/Vulnerability/Risk Assessments	0.00	0.20	1.46	6.40

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," Figures part of 2001 budget

Environmental Protection Agency and GAO Audits

The balance of EPA spending for CIP is requested for protection of the water sector from the threat of terrorist attack.[183] An October 1999 agency review showed that the EPA had several security weaknesses in its computer operating systems and agency-wide network. These

systems and network support most of the EPA's mission-related and financial operations. GAO also noted that EPA's own records cited several serious computer incidents in the last two years.[184]

Table 5.9

Environment Protection Agency Spending for Critical Infrastructure Protection

Environmental Protection Agency				
Critical Infrastructure Protection	**0.12**	**0.24**	**0.08**	**2.30**
Federal Infrastructure Protection	0.11	0.23	0.00	0.00
Threat/Vulnerability/Risk Assessment	0.11	0.23	0.00	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," Figures part of 2001 budget

Health and Human Services

Unlike DOE, HHS received significant funding in FY1998 of $21.85 million. HHS has seen these funds drop in FY1999 to $14.39 million, rise back up to $22.11 million in FY2000 and see a request of $27.60 million in FY 2001.[185] The OMB report is not clear on what this funding is used for, only that the vast majority of funds are aimed at the protection of federal infrastructure (the total balance of the funds were devoted to this area in FY98, FY99 and FY00). Most of the funds within this total were spent on multiple program areas in FY98 and FY99 and then on systems protection in the following two fiscal years.[186] OMB highlighted no special programs for HHS.

Table 5.10

Agency Spending for Critical Infrastructure Protection

	FY1998	FY1999	FY2000	FY2001
Department of Health and Human Services				
Critical Infrastructure Protection	**21.85**	**14.39**	**22.11**	**27.60**
Federal Infrastructure Protection	21.85	14.39	22.11	25.60
Multiple Program Areas	18.40	8.17	8.70	9.70
System Protection	2.45	5.02	12.21	14.70
Threat/Vulnerability/Risk Assessments	1.00	1.20	1.20	1.20
CIP Assistance/Outreach to Private Sector	0.00	0.00	0.00	2.00
Multiple Program Areas	0.00	0.00	0.00	2.00

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," Figures part of 2001 budget

Department of Interior

Neither the OMD nor DOE provide a detailed analysis of the Department's spending on critical infrastructure protection.

Table 5.11

Department of Interior Spending for Critical Infrastructure Protection

	FY1998	FY1999	FY2000	FY2001
Department of the Interior				
Critical Infrastructure Protection	**1.29**	**1.60**	**2.65**	**1.83**
Federal Infrastructure Protection	0.64	0.80	1.33	0.91
Threat/Vulnerability/Risk Assessments	0.64	0.80	1.33	0.91
CIP Assistance/Outreach to Private Sector	0.64	0.80	1.33	0.91

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," Figures part of 2001 budget

Department of Justice

With the FBI being the lead federal agency for coordinating emergency law enforcement services in responding to critical infrastructure attacks, DOJ requested in the President's budget $45.51 million for CIP.[187] Very little of the funding for the past four fiscal years has gone to protection of federal infrastructures. Only $1.5 million in FY2001.[188]

The majority of the funds are allocated for public assistance. OMB reporting places this spending in the somewhat nebulous category of multiple programs. However, when looking at the highlighted program list it is apparent that the majority of the money will be placed in the National Infrastructure Protection Center ($20 million) and Computer Intrusion Squads ($22 million).[189]

Table 5.12

Department of Justice Spending for Critical Infrastructure Protection

	FY1998	FY1999	FY2000	FY2001
Department of Justice				
Critical Infrastructure Protection	25.61	54.09	44.02	45.51
Federal Infrastructure Protection	0.84	1.73	1.43	1.50
Legislative Initiatives and Legal Issues	0.12	0.20	0.20	0.23
Multiple Program Areas	0.72	1.54	1.24	1.27
CIP Assistance/Outreach to Private Sector	24.77	52.36	42.59	44.01
Legislative Initiatives and Legal Issues	1.58	2.60	2.60	3.07
Multiple Program Areas	23.19	49.76	39.98	40.94

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," Figures part of 2001 budget

NASA

NASA has consistently received funding for protection of its infrastructure. This funding has consistently been spent within the department on intrusion monitoring and response ($16 million in FY98, $17 million in FY99, $25 million in FY00 and $24 million in FY2001) and system protection ($18 million in FY98, 19 million in FY99 and 32 and 28 million in FY00 and FY01 requested).[190]

Table 5.13

National Aeronautics and Space Administration Spending for Critical Infrastructure Protection

	FY1998	FY1999	FY2000	FY2001
National Aeronautics and Space Administration				
Critical Infrastructure Protection	**41.00**	**43.00**	**66.00**	**61.00**
Federal Infrastructure Protection	41.00	43.00	66.00	61.00
Education and Training	1.00	1.00	2.00	2.00
Intrusion Monitoring and Response	16.00	17.00	25.00	24.00
Multiple Program Areas	5.00	5.00	5.00	5.00
System Protection	18.00	19.00	32.00	28.00
Threat/Vulnerability/Risk Assessment	1.00	1.00	2.00	2.00

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," Figures part of 2001 budget

GAO Assessments of NASA Information Security

In a May 1999 report, GAO declared that tests done on 10 field sites had found that some of NASA's mission critical systems where vulnerable to penetration. While all systems GAO testers gained accessed had effective security measures to deny further access, some systems could be compromised to the point that an intruder could have "disrupted NASA's ongoing command and control operations and stolen, modified, or destroyed system software and data."[191] GAO linked these weaknesses to what GAO deduced as NASA's inability to effectively and consistently manage IT security throughout the agency. GAO reported that NASA:[192]

- did not effectively assess risks or evaluate needs. One hundred thirty-five of the 155 mission-critical systems that we reviewed did not meet all of NASA's requirements for risk assessments.
- did not effectively implement policies and controls. NASA's guidance did not specify what information can be posted on public World Wide Web sites or how mission-critical systems should be protected from well-known Internet threats.
- was not monitoring policy compliance or the effectiveness of controls. NASA had not conducted an agency-wide review of IT security at its 10 field centers since 1991. Furthermore, the security of 60 percent of the systems that we reviewed had not been independently audited.
- was not providing required computer security training. NASA had no structured security training

curriculum.

- did not centrally coordinate responses to security incidents. NASA field centers were not reporting incidents to the NASA Automated Systems Incident Response Capability (NASIRC).

GAO recommended a five category approach to dealing with NASA's information security weaknesses. [193]

We are recommending that the NASA Administrator implement an effective agency-wide security program that includes improvements in five categories: assessing risks and evaluating needs, implementing policies and controls, monitoring compliance with policy and effectiveness of controls, providing computer security training, and coordinating responses to security incidents. NASA concurs in all of our recommendations.

In detail GAO recommended that[194]

- Assessing risks and evaluating needs, which includes the following:
    - Developing and instituting a review process to ensure that managers conduct complete risk assessments for all major systems prior to the systems becoming operational, upon significant change, or at least every 3 years.
    - Formally authorizing all systems before they become operational and at least every three years
- Implementing policies and controls, which includes the following
    - Streamlining the policy-making and standards-setting process for IT security so that guidance can be issued and modified promptly to address changes in threats and vulnerabilities introduced by rapidly evolving computer and telecommunication technologies.
    - Developing and issuing guidance that specifies information that is appropriate for posting on World Wide Web sites and distinguishes this from information that is sensitive and should be more closely controlled.
- Developing and issuing guidance that identifies systems, including those involved in the command and control of orbiting spacecraft that require strong user authentication.
- Monitoring compliance with policy and effectiveness of controls, which includes the following:
    - Developing and implementing a management oversight process to periodically monitor and enforce field centers' compliance with agency-wide policy.
    - Ensuring that independent audits or reviews of systems' security controls are performed at least every 3 years and that identified weaknesses are expeditiously corrected.
- Providing required computer security training, which includes the following:
    - Developing and implementing a structured program for ensuring that NASA employees receive periodic training in computer security to provide them with awareness, knowledge, and skills

necessary to protect sensitive information and mission critical systems.

- Modifying relevant contracts to include provisions for ensuring that NASA contract personnel are similarly trained.

- Developing and implementing a program for certifying that NASA civil servants and contract employees are competent to discharge their IT security-related responsibilities

- Coordinating responses to security incidents, which includes the following:

  - Clarifying policy and procedures for mandatory reporting of security incidents to NASIRC.

  - Strengthening the role of NASIRC in disseminating vulnerability information within NASA, analyzing threats in real time and developing effective countermeasures for ongoing attacks.

We also recommend that the NASA CIO review the specific vulnerabilities and suggested actions provided to field center officials at the conclusion of our penetration testing, determine and implement appropriate security countermeasures, and track the implementation and/or disposition of these actions.

National Science Foundation

NSF plays a role in protecting federal infrastructure through education and training ($10.2 million for FY2001) and assistance to the public sector through system protection ($32.98 million).[195] Most of the $32 million for public sector assistance is most likely going to Research and Development, as indicated by the OMB report.

OMB also reports that NSF will provide support for research in FY2001, in areas including networking, high performance computing and software that will enable computer and communications systems to be safer, more reliable, and free from intrusions. NSF will also provide support for research in critical infrastructure protection by sponsoring work on software development methods to improve the predictability and security of critical software systems, innovative approaches to fault tolerance, and modeling, simulation and optimization of control of electric power systems.[196]

Table 5.14

National Science Foundation Spending for Critical Infrastructure Protection

	FY1998	FY1999	FY2000	FY2001
National Science Foundation				
Critical Infrastructure Protection	**19.15**	**21.42**	**26.65**	**43.85**
Federal Infrastructure Protection	0.57	0.60	0.63	10.87
Education and Training	0.00	0.00	0.00	10.20
System Protection	0.57	0.60	0.63	0.67
CIP Assistance/Outreach to Private Sector	18.58	20.82	26.02	32.98
Intrusion Monitoring and Response	0.00	0.51	0.53	0.54
Multiple Program Areas	0.00	0.00	-	4.00
System Protection	17.21	18.34	23.11	25.81
Threat/Vulnerability/Risk Assessments	1.37	1.97	2.38	2.63

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," Figures part of 2001 budget

National Security Community

The National Security Community dominates the budget regarding CIP. In the community DOD is considered the lead agency for protecting critical defense infrastructures against attack and ensuring the integrity and security of DOD information systems.[197]

The OMB report omits any data on US offensive and retaliatory cyver and information warfare capability and provides few details on the allocation of over $1.458 billion requested in FY2001, which is more than half of the entire CIP budget. What can be understood from the OMB report is that nearly all of that money is spent on the protection of federal infrastructure ($1.42 billion). Of that $1.42 billion, almost half goes to system protection ($638.12 million) and over $300 million is requested for multiple programs. Over $100 million is spent in both intrusion monitoring and response, and threat, vulnerability, and risk assessments with $187.18 million and $160 million respectively.

A total of $460 million of the highlighted programs is delegated for R&D purposes. A total of $177 million is to be spent on Public Key Infrastructures. $14 million will be used for

developing Computer Network Defense capability. OMB mentions funding for Operation and Maintenance which will pay over 2,800 civilians involved in information assurance and support activities. OMB does not mention a cost for that particular program.

It should be noted, however, that all of these figures fail to address the scale of offensive information warfare and cyberattack capabilities within the national security community. They focus almost solely on defense efforts, and this approach to programming and budgeting reinforces the massive disconnect between cyberoffense and cyberdefense that characterizes all of the public literature on critical infrastructure protection.

This highlights the problem of focusing largely on defense in most federal critical infrastructure protection planning, rather than deterrence and active offensive response. It can be argued that such a focus is proper in dealing with low to moderate level attacks and threats because of the difficulty of attribution and the limits to the technology available for retaliation and counterattack. However, it is striking that no public federal assessment of these trade-offs seems to be available, and that the national security community has failed to address them in ways which can guidance other elements of government and the private sector.

These problems are reinforced by the lack of any apparent net technical assessment effort to assess the balance between offense and defense, and vulnerability. There does not seem to be anything approaching an adequate and integrated analytic underpinning for programming the critical infrastructure protection efforts of the national security community, and this inevitably means that other federal agencies, state and local governments, businesses, NGOs, and utilities also lack proper priorities and guidance.

The Role of the Department of Defense

The Department of Defense is a critical player in the nation's effort to conduct offensive information and cyberwarfare, and its ability to deter or respond to foreign attacks. Virtually no data are public on this aspect of its capabilities, although – as has been discussed earlier – the Department does have operational plans to carry out such attacks and is known to have

developed detailed contingency plans for Desert Storm, Desert Fox, and NATO's intervention in Kosovo.

At the same time, few federal agencies are as dependent on secure information systems as the Department of Defense. The Defense Department has roughly 10,000 computer systems and 1.5 million individual computers. Arthur Money, the assistant secretary of defense for command, control, communications and intelligence, told a House Armed Services subcommittee in March, 2000 that about 2,000 of these systems are "mission-critical," and "must work for [the DoD] to successfully execute its myriad missions."

Over 95% of all DOD communications utilize the public switched network. This includes supporting such critical defense missions as the movement of troops and operational plans, procurement, and weapons systems maintenance. Secretary of Defense William Cohen's Annual Report to the President and the Congress for the year 2000 states,

> DoD is committed to taking full advantage of opportunities provided by the information age's concepts and technologies in the 21st century. Creating and leveraging information superiority and exploiting the potential of Space are on DoD's critical path to the future. The synergy resulting from the consolidation of Information Superiority and Chief Information Officer (CIO) functions under the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) continues to yield significant technical, operational, and financial benefits. The consolidation of space policy development and oversight and closer coordination with the Intelligence Community resulted in space concepts being better integrated into defense strategy and processes. These actions create and leverage information superiority.
>
> The information age provides an opportunity to move from an approach to war preoccupied with uncertainty and damage control to one that leverages information to create competitive advantage. The United States currently enjoys a superior information position over potential adversaries by virtue of its ability to collect, process, protect, and distribute relevant and accurate information in a timely manner while denying this capability to adversaries.
>
> This information edge is translated directly into increased effectiveness by enabling emerging network–centric concepts designed to leverage improved situation awareness. Thus, information superiority is reflected in the twin revolutions, the Revolutions in Military Affairs and Business Affairs. These twin revolutions are mutually supportive as improved business processes result in additional resources for combat capabilities increasing the tooth to tail ratio.
>
> Information superiority is the critical enabler of the transformation of the Department currently in progress. The results of research, analyses, and experiments designed to create and leverage information superiority, reinforced by recent experiences in Kosovo, are very encouraging. They demonstrate that the availability of information and the ability to share it results in enhanced mission effectiveness and improved efficiencies. This evidence points to increased speed of command, a higher tempo of operations, greater lethality, less

> fratricide and collateral damage, increased survivability, streamlined combat support, and more effective force synchronization.
>
> The ability to move information quickly where it is needed and to create shared awareness provides an opportunity to develop new concepts of operation and approaches to command and control (C2) that are more responsive and provide greater flexibility. To achieve their full potential, these new concepts may require changes in organization, doctrine, material, and the like—changes that need to be co–evolved along with the development of new operational concepts and approaches to command and control. New approaches to command and control include integrating the now separate and sequential planning and execution processes to achieve greater agility and flexibility and the capability for self–synchronizing forces. Based upon a common understanding of the situation and the commander's intent, these forces are able to quickly respond in a coordinated fashion. Information superiority provides enhanced flexibility and agility, allowing U.S. forces to be more proactive and shape the battlefield.

Patterns of Attack and Response

The Department of Defense is a nearly constant target for attacks that range from random hacking to actions by states. Arthur Money, told a House Armed Services subcommittee in March 2000 that, "We are probed on a daily basis by those who are trying, or planning, to disrupt our nation's military capabilities…a few nation state operatives do major downloadings of unclassified materials."[198]

Money testified that one "seminal event" that led the Department to improve its computer security problems occurred in February 1998. Some youths in California, acting under the direction of an Israeli, took advantage of a "well-known vulnerability in Sun software" to break into the Solaris operating system used by Defense agencies. The attacks came as preparations were underway for a possible military operation against Iraq. John J. Hamre, then Deputy Secretary of Defense, testified in 1999 that these attacks "were widespread, systematic and showed a pattern that indicated they might be the preparation for a coordinated attack on the defense information infrastructure." Military computer administrators had been warned about the weaknesses that the California hackers exploited, but many had failed to heed the warning and patch their systems,[199]

One important result, was that the Department placed important limits on its ties to the Internet.[200] The Deputy Secretary of Defense a memo issued on September 24, 1998 that called for a Department-wide effort to limit the information available on the web, and to establish

comprehensive risk management procedures to determine the value of placing data on the web versus the security risk to the Department and those serving in it. It called on the Department to eliminate access to any data that might be used to gather information on operations, plans, troop movements, critical personnel information, and unit locations affecting operations. It also called for a C^4I architecture to protect sensitive, but unclassified information, plans to use reserve assets to strengthen the Department's cyberdefenses, comprehensive training in cybersecurity, and new procedures to ensure the review of software, data bases, and systems.

According to a Department report issued in December 2000, the Defense Department suffered more than 22,000 electronic attacks on its computer systems in 1999 and about 14,000 in the first seven months of 2000. In 1999, the Department detected 22,144 attempts to probe, scan, hack into, infect with viruses or disable its computers. Roughly three percent (or more than 600) of those incidents caused temporary shutdowns or other damage. About one percent (or roughly 200) were intrusions by hackers who managed to break into unclassified computer systems. The number of attacks rose approximately 10 percent in the first seven months of 2000, and the percentage that have caused damage or resulted in intrusions is about the same.[201]

The Department reported that the "vast majority of those attacks were either harmless or caused only petty harassment." It also indicated, however, that hackers believed to be working for foreign countries had broken into unclassified computer systems in a few cases, and downloaded large amounts of information. The Department reported that no incidents were detected that were able to enter the Department of Defense's classified computer systems. These figures reported the Departments first effort to make a really accurate count of the number of attacks because it only installed devices to monitor attempts by hackers to penetrate its computers at the end of 1998. [202]

Money predicted that the number of attacks was "going to increase" in the future." He also indicated why designing less vulnerable systems may be at least as critical as improving defenses. He reported that a majority of the attacks that caused damage "come through vulnerabilities in existing software, most of it from commercial companies," such as Microsoft,

Netscape and Lotus. He stated that the Department was "putting more and more effort into testing" off-the-shelf software and was working with major software companies in the design stages, Money stated, however, that "there is hardly any way to prevent" vulnerabilities from creeping into the millions of lines of commercial computer code. He noted that code is also written in India, Ireland, Israel and other countries. "On a lot of these [programs], we don't know where the code is written." Other officials stated that most vulnerabilities were unintentional, but some seemed to be "trapdoors" deliberately left by the authors of the software to allow intrusions, while others were "backdoors" that were designed to help systems administrators that had been "discovered by kids and hackers and used to harass the systems." A Pentagon official added, "we are not buying such off-the-shelf products in our most sensitive systems."

These attack patterns led Congress to allocate an additional $163 million for computer security into the fiscal 2001 defense appropriations bill. At the same time, the House-Senate conferees' report on the bill warned that the new funds "will be of limited value if the software used by the department has been designed with intentional weaknesses to permit future unauthorized access." The conference report directed the Pentagon "to carefully consider the origin of all software used in developing or upgrading information technology or national security systems." [203]

It is also clear that these effort present problems in terms of skilled manpower. The Department announced in December 2000 that it planne to recruit hundreds of reserve component information technology specialists in coming years to fill positions in several new military "cyber-security" organizations to ensure that American war fighters could dominate military computer information warfare in future conflicts. Rudy de Leon, the Deputy Secretary of Defense stated that "Information operations has emerged as an area that is extremely well-suited to integration of reserve capabilities. Members of the reserve and National Guard are often way ahead by the very nature of their civilian employment, trained in their workplaces to exploit technology."

The Department reported that it needed 182 reserve component officers and enlisted members to

man the five organizations for fiscal 2001 and 2002, officials said. Numbers of people in each organization will vary. The total number of people in the units is expected to grow to more than 600 through fiscal 2007. The reserve component technicians and their units were assigned to support the Defense Information Security Agency, Arlington, Va.; the Joint Task Force-Computer Network Defense, Arlington; the National Security Agency, Fort Meade, Md.; the Joint Information Operations Center, Kelly Air Force Base, Texas; and the Information Operations Technical Center, Fort Meade.[204]

The Department reported that the need for DoD to safeguard its computerized information systems was highlighted by recent "cyber warfare" between Israeli and Palestinian computer technicians featuring the defacing of opponents' websites and massive "jamming" of digital information conduits by email saturation and virus "mail." It also that that the decision to upgrade DoD's information security infrastructure originated from a recommendation from the Reserve Component Employment 2005 study, which suggested new ways to employ reserve forces as part of fostering improved integration in the Total Force. Reserve component members who work for info-tech industry firms like Microsoft and IBM were found to make good fits for the new organizations.

Major DoD Cyberdefense Programs

The Department of Defense has major programs designed to protect its information systems that are reinforced by the physical protection measures it has taken in response to the threat posed by other forms of terrorism:

> The Department of Defense, being the largest organization in the nation, faces significant information technology challenges in its efforts to ensure the continuity of critical missions and systems in the face of Y2K–related problems. Over one–third of all mission critical computer systems in the federal government are within DoD. DoD treated the Year 2000 problem as if it were a cyber attack directed at the very core of its military capability—at the ability to obtain, process, and control information. Securing systems for 2000 provided numerous lessons that will translate well to efforts in securing the critical information infrastructure in the future.
>
> Y2K efforts have led to the best ever accounting of DoD systems and status. The information management structure now in place meets the requirements of the Clinger–Cohen Act. The enormous effort and awareness of IT generated by the Year 2000 problem has resulted in significant progress across the board in

information superiority.

Information Assurance

Information Assurance, a critical component of DoD's operational readiness, ensures that the DII is capable of providing continuous and dependable service. IA depends on the continuous integration of personnel, operational, and technical capabilities to guarantee the availability, integrity, authenticity, confidentiality, and non-repudiation of information services, while providing the means to efficiently reconstitute these vital services following an attack.

In August 1998, DoD created the Joint Task Force–Computer Network Defense (JTF–CND), with a mission of coordinating and directing the defense of DoD computer systems and computer networks including the coordination of DoD defensive actions with non–DoD government agencies and appropriate private organizations. In June 1999, the JTF–CND reached its full operational capability. Effective October 1, 1999, the Commander in Chief, United States Space Command, was assigned the responsibility for Computer Network Defense (CND). Detailed studies are underway to identify core functions and develop an integrated, defense–wide, enterprise CND policy and assignment of responsibilities.

In May 1999, the Deputy Secretary of Defense issued the defense–wide PKI policy that requires the use of a common, integrated DoD PKI to enable security services at multiple levels of assurance, provides a solid foundation for IA capabilities across the Department, and mandates an aggressive approach in acquiring and using a PKI that meets DoD requirements for all information assurance services.

Critical Infrastructure Protection

CIP addresses the protection of the critical assets and infrastructures DoD relies upon to accomplish its mission. A CIP Plan went into effect in January 1999 to ensure an integrated approach to CIP. The ASD(C3I) was designated the Department's Chief Infrastructure Assurance Officer (CIAO), and senior DoD executives have been designated as CIAOs for each infrastructure. The Department began development of an analytic and assessment capability for the Defense infrastructures, leveraging existing capabilities which had been focused on commercial infrastructures. The ASD (C3I) has also been designated at the Functional Coordinator for National Defense, responsible (under Presidential Decision Directive 63) for coordinating all the CIP–related national defense activities of the U.S. government, ensuring that the comprehensive approach DoD is applying to its internal infrastructures is supported nationally and internationally by the other federal departments and agencies as well as allies and coalition partners.

Security

DoD needs security policies and programs that pace the revolutionary changes in technology and combat on the modern battlefield. Policies must focus on providing protection based on assessments of threats and the danger and consequences of compromise for the most critical and vulnerable information, systems, capabilities, people, and facilities. The Department requires an active security paradigm that includes the following steps:

- Establish Criticality. Identify what must be protected and determine the protection requirements, analyze what is required to accomplish the mission, assess protective and deterrence systems, determine vulnerabilities to the threat environment, establish a degree of assurance to determine acceptable risk.

- Prepare. Reduce the threat by establishing a high level of assurance in the trustworthiness and reliability of people, practices, systems, and programs.

- Protect Assets. Control asset sharing, isolating information and capabilities based on need–to–know; mitigate known operational deficiencies and vulnerabilities; employ a defense in–depth strategy; and employ new technology to enforce or support security policy.

- Detect. Actively seek potential isolated and correlated threats or problems, particularly that may result in future malicious or anomalous activity.

- Respond. React to isolated or correlated anomalous or malicious activity, fix technology–based problems and correct suspected and actual unacceptable behavior using sound personnel and security management practices, seek legal or other management remedies as appropriate and when necessary.

- Strengthen Foundation. Refine security policy constructs, programs, and practices to anticipate the changing threat environment; deconflict security requirements to foster information sharing while maintaining need–to–know; strengthen personnel management practices to provide a motivated, skilled, and security–responsive workforce; establish and maintain mission–related performance measures; develop standards of professional competence for security practitioners and enhance awareness and training to ensure information is tailored for the designated audience.

    Developing and implementing a new vision of security in the information age requires recognition of the globalization of the defense industrial base and the closer integration of foreign countries in defense production. These trends will require changes in the existing security paradigm.

    The Department established a single office within the Office of the Secretary of Defense responsible for CI, Security, IA, CIP, and IO to ensure a coherent approach to these issues; established the Defense Information Assurance Program to better integrate the information assurance requirements and budgets of the DoD components, implemented a new certification process for systems administrators; and contributed personnel to the National Infrastructure Protection Center.

    The Department implemented the Information Assurance Vulnerability Alert process that disseminates information threat warning and remediation messages throughout DoD and monitors implementation of countermeasures, issued new guidance for Web pages to prevent inadvertent disclosure of sensitive information, and established a Joint Web Risk Assessment Cell to monitor compliance.

The Department of Defense is also developing offensive capabilities that can be used for deterrent and retaliatory purposes, although little unclassified data are available on these programs:

> Information operations support the objectives of the National Security Strategy by enhancing information superiority and influencing foreign perceptions. The Department's emerging concept for IO will be the basis for aligning strategy and policy across DoD. When approved, the strategic concept will guide and integrate IO policy, organization, and implementation and the research, development, and acquisition of IO capabilities.
>
> To protect information, maintain information superiority, and improve preparedness, DoD is employing Red Teams, which are interdisciplinary, threat–based opposing forces to expose and exploit IO vulnerabilities of friendly forces. The Department is preparing policy to standardize the methodology for conducting DoD Red Team operations.
>
> The Department is developing an IO resource baseline to identify DoD component IO–related efforts. This

will provide the Department's leadership with great insight into DoD component IO resource, R&D efforts, and organizational focus, allowing greater resource efficiencies and DoD IO program integration.

Based on IO experience in support of Kosovo operations, DoD now has the makings of an IO framework from which to deal with future coalition/allied warfare issues to achieve/maintain information superiority. DoD education programs continue to be offered and are available to federal and military personnel. IO continues to be integrated into military exercises and wargames

GAO Critiques of DoD Efforts: The 1996 Study

In a September 1996 GAO issued a report to the Secretary of Defense, the DISA Director, and the CIOs of the military departments and other Defense agencies aimed at,[205]

- Empowering the DoD CIO to establish a comprehensive, department-wide information security program;
- Ensuring that security programs of the military departments and Defense agencies are consistent with the department program; and
- Periodically reporting on progress in improving controls over information security

The 1996 report listed 10 recommendations, each of which DoD has reported to have taken corrective actions on. The recommendations for the 1996 report are as follows:[206]

I. We recommend that the Secretary of Defense assign clear responsibility and accountability within the Office of the Secretary of Defense, the military services, and the Defense agencies for ensuring the successful implementation of an information security program that includes, for example, department-wide policies for preventing, detecting, and responding to hacker attacks on Defense information systems.

II. We further recommend that you direct the DOD CIO to develop and implement a comprehensive DOD-wide computer security management program that includes the hacker prevention policies we previously recommended as well as

• establishing a risk-based control program to assess computer security in DOD computer systems,

• developing and implementing effective security policies and related control techniques, and

• reporting to DOD managers on security issues impacting their information processing systems.

III. We also recommend that you direct the Deputy Secretary of Defense to ensure that the duties established for the military departments' and Defense agencies' CIOs include reporting on ongoing computer security efforts and activities to the DOD CIO for review, assessment, and appropriate action to ensure proper coordination and an integrated information technology structure within the Department.

IV. Further, you should direct the DOD CIO to review and assess the specific

deficiencies noted and establish a process to address them.

V. In addition, we recommend that the DISA Director, the CIOs of the military departments, and the CIOs of the other Defense agencies submit their policies and procedures to improve general computer controls to the DOD CIO for review, assessment, and appropriate action to ensure a comprehensive security approach is operational throughout the Department. Such policies and procedures should

• limit computer system access authorizations to only those who need access to perform their work responsibilities, and are periodically reviewed to ensure their continued need;

• require sensitive data files and critical production programs to be identified and successful and unsuccessful access to them to be monitored;

• strengthen security software standards in critical areas, such as by preventing the reuse of passwords and ensuring that security software is implemented and maintained in accordance with the standards;

• control physical security at computer facilities; and

• provide for completing and testing disaster recovery plans.

VI. To ensure that general computer controls are improved at the DMCs, we recommend that the DOD CIO direct the DISA Director to develop and implement a comprehensive computer security program at the DMCs, consistent with the DOD-wide program, that includes the elements outlined in this report. These elements encompass

• policies and procedures to ensure that access to DMC computer facilities is appropriately granted and periodically reviewed,

• clearly defined roles and responsibilities of DMC employees, information system security officers, and security managers, and

• security oversight at each DMC to monitor, measure, test, and report on the ongoing effectiveness of computer system, network, and process controls.

VII. In addition, we recommend that the CIOs of the military departments and the Defense agencies submit plans for coordinating with DISA to improve computer controls affecting DMC operations to the DOD CIO for review, assessment, and appropriate actions. Greater cooperation is necessary, for example, to

• determine who is given access to computer systems applications,

• identify critical computer systems applications to be covered by disaster recovery plans, and

• ensure that locally designed software application program changes are in accordance with prescribed policies and procedures.

VIII. Also, the DISA Director and the CIOs of the military departments and Defense agencies should provide their plans to the DOD CIO, for review, assessment, and appropriate action to ensure that computer system security reviews are performed as part of future transfers of computer systems to

the DMCs.

IX. Further, the DOD CIO should monitor implementation of those plans.

X. Finally, to strengthen DOD's computer security program in a coordinated and timely manner, we recommend that you

• direct the DOD CIO to monitor and to periodically report on the status of the actions taken to improve computer security throughout DOD and

• ensure that the DOD CIO has the necessary authority to ensure that there are adequate computer security controls throughout DOD, including the military departments and Defense agencies.

The GAO's 1999 Recommendations

In the August 1999 report the GAO reaffirmed the recommendations of September 1996 and added additional recommendations to "realize the full potential and maximize the effectiveness of DISA's security oversight program, the DIAP, and other DoD IA initiatives…" GAO recommended that the Secretary of Defense[207]

- Direct the DISA Director to expand the Security Readiness Review process to include timely and independent verification of the corrective actions reported by DMCs or other responsible parties
- Direct the DoD CIO to ensure that the Defense-wide Information Assurance Program defines how its efforts will be coordinated with the Joint Task Force and other related initiatives.

The GAO noted an improvement in DISA's processes to identify information security weaknesses.[208]

Our reports identified pervasive information security weaknesses in DoD and made recommendations for correcting them. While some corrective actions had been initiated to address our recommendations, our current review found that weaknesses persisted in every area of general controls.

Among the DoD components evaluated, only DISA had begun to establish a comprehensive process to identify and resolve information security weaknesses. DISA was issuing technical guidance to establish minimum standards for configuring system software and was implementing systematic entity-wide inspections to monitor effectiveness of computer controls. As a result, DISA had identified and resolved thousands of control weaknesses.

The GAO report on DoD Information Security also found, however, that serious weaknesses created a continued risk to defense operations. The report cited that these weaknesses impaired DoD's: [209]

ability to (1) control physical and electronic access to its systems and data, (2) ensure that software running on its

systems is properly authorized, tested, and functioning as intended, (3) limit employees' ability to perform incompatible functions, and (4) resume operations in the event of a disaster. As a result, numerous Defense functions, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll, have already been adversely affected by system attacks of fraud.

The GAO found that the DoD's massive information processing systems included over 2.1 million computers, over 10,000 local area networks, and over 100 long distance networks.[210] It listed the following weaknesses and recommendations for correcting them in its August 1999 report:[211]

> In our current review we found that significant DOD information security weaknesses in general computer controls persisted for all the components evaluated, including DISA. The following sections give examples illustrating the types of weaknesses we found in access controls, application software development and change controls, and segregation of duties, system software controls, and service continuity controls.
>
> Access controls limit or detect inappropriate access to computer data, programs, facilities, and equipment to protect these resources against unauthorized modification, disclosure, loss, or impairment. Access controls include physical protections, such as gates and guards, and logical controls, which are built into software to authenticate users (through passwords or other means) and to restrict their access to certain data, programs, transactions, or commands. DOD policy states that access to automated information systems should be restricted based on one's need-to-know.
>
> We found, however, that users were granted access to computer resources that exceeded what they required to carry out their job responsibilities, including sensitive system privileges for which they had no need. On one system, systems support personnel had the ability to change data in the system audit log. On three systems, we tested the accounts of 12 users having access to a command that would allow them to substitute an unauthorized data file for a legitimate file. Seven out of 12 did not have a need to use this command. We also found user accounts that had certain privileges—including sensitive security administration privileges—for which no evidence of authorization was available. Access authorization was poorly documented or undocumented for users at every site; management estimated that on one system more than 20,000 users were not authorized in writing.
>
> Periodic review of user access privileges and monitoring of security violations and the use of powerful commands, utilities, and changes to sensitive files and records (such as user access profiles) are essential to preventing and detecting unauthorized activity. However, we found at every location we visited that there was inadequate periodic review of user access privileges to ensure that those privileges continued to be appropriate. Also, while the logging of security violations and access to sensitive resources had improved, these audit logs were not being consistently reviewed. Similarly, we found that data processing customers were not updating users' access levels to reflect changes in their access requirements or to cancel the access of terminated employees.
>
> Password management, though improved, was still weak in some areas. Users were not required to change their passwords often enough and in some cases were never required to change their passwords. Users were not prevented from using easily guessed passwords. These practices increase the risk that passwords will be guessed and systems will be compromised.
>
> User accountability was also weakened by the use of generic (group) user accounts, wherein a single account is used by two or more users, contrary to DISA standards. In the case of one generic user account

having system privileges, not only was the password known to multiple users, but it was neither encrypted in the system nor required to be changed periodically.

Application software development and change controls prevent unauthorized programs or modifications to programs from being implemented to ensure that the software functions as intended. Program change control policies and procedures include review and approval of application change requests, independent review and testing of program changes, documentation of program changes, and formal authorization to implement those changes, along with the access controls necessary to ensure that these objectives are met.

We found that structured methodologies for designing, developing, and maintaining applications were inadequate or nonexistent. There was no requirement for users to document the planning and review of application changes and to test them to ensure that the system functioned as intended. Also, application programs were not adequately documented with a full description of the purpose and function of each module, which increases the risk that a developer making program changes will unknowingly subvert new or existing application controls.

One fundamental technique of program change control is the use of two or more computer processing environments to segregate the test and development versions of application programs and data from the production resources (those versions approved and currently being used by the data processing customer). We found that application programmers, users, and computer operators had direct access to production resources, increasing the risk that unauthorized changes to production programs and data could be made and not detected. On one system, 74 user accounts had privileges enabling them to change program code without supervisory review and approval. This number had increased from the 37 users that we had documented in our earlier review. According to management, only four people should have this authority. On another system, nearly 300 programmers could alter production programs and data.

Segregation of duties refers to the policies, procedures, and organizational structure that help to ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions without detection. As an example, a computer programmer should not be allowed to independently write, test, and approve program changes. In the information processing environment, the duties and access capabilities of systems programmers, application programmers, security administrators, and end-users, for example, should generally be segregated from one another.

Duties in the DOD computing environment were not adequately segregated. We found that personnel were still assigned both systems programming and security administration duties. These individuals could make unauthorized changes to programs and data while using their security privileges to disable the system's capability to create an audit trail of those changes. Thus they could, for example, modify payroll records or shipping records to generate unauthorized payments or to misdirect inventory shipments and suppress the related system audit data to avoid detection.

System software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation. System software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on the system. Some system software can change data and program code without creating an audit trail or can be used to modify or delete audit trails.

Improperly configured or poorly maintained system software can be exploited to circumvent security controls to read, modify, or delete critical or sensitive data or programs. It can also be used to gain privileges to conduct unauthorized transactions or to circumvent edits or other controls built into application programs. For these reasons, system software vulnerabilities are a common target of hackers, both internal and external to the entity. As a result, most entities have a separate set of procedures for

controlling system software.

We found end-users had been given unnecessary (and in some cases unauthorized) access to system functions, tools, and data. For example, users could read system data files containing information useful to hackers. On four systems, users could view other users' output, which could include sensitive or confidential information. On one system, end-users had the capability to issue commands that would allow them to disrupt all processing on that system. As with other groups of users, the activities and access privileges of users with sensitive system privileges were not adequately monitored.

We also found system software maintenance issues that create security exposures. For example, we found system libraries for privileged programs (i.e., programs that are allowed to perform powerful system functions) that contained the names of nonexistent programs. By creating a new program with the same name as one of these nonexistent members, a user could install malicious code with the authority to make changes to the operating system, the security software, and user programs or data and to delete audit logs. We found that one site was running a proprietary mainframe operating system and other system software products that were no longer supported by the vendor. Management informed us that such software was needed to support application programs that had not yet been upgraded to run on a current version of the operating system. This site was also running programs that were undocumented. These practices increase the risk that security vulnerabilities or other problems will not be detected or corrected.

Service continuity controls ensure that when unexpected events occur, critical operations continue without undue interruption and critical and sensitive data are protected. A well-documented plan for disaster recovery and continuity of operations, based upon an up-to-date risk analysis and periodic testing, is critical to ensure that an organization can continue to fulfill its mission while responding to natural disasters, accidents, or other major and minor interruptions in data processing.

We found mission-related applications and the activities they support that are at risk because of inadequate planning for service continuity. Although DISA recommends nightly back-up of high-activity application data files, some information processing customers did not require that their application data be backed up frequently enough to ensure effective mission support after a service disruption. This increases the risk that some data cannot be restored, particularly as temporary data files may not exist at the time the full system back-up is done, which is typically once a week. Also, although DISA requires that back-up tapes be stored at least 25 miles, and preferably 100 miles, from the processing site, we noted that one DMC was storing back-up tapes only 14 miles from the data center without having obtained a waiver from DISA. This increases the risk that both the back-up tapes and the data center could be affected by the same emergency.

We found that disaster recovery plans were incomplete and did not specify the order in which the customer's applications (or the programs within a particular application) should be restored. This increases the risk that relatively trivial functions may be restored before those that are most critical to the user's mission. One plan assumed the availability of hardware that was not on-site and was still in the procurement process.

Many DISA customers had not tested their recovery procedures or had not tested them under the conditions likely to prevail in the event of a disaster. These weaknesses increase the risk that the organization may fail in its mission or incur unnecessary expense as the result of a prolonged service interruption.

DoD Progress in Addressing Security Weaknesses

GAO has cited DISA’s progress in identifying thousands of specific control weaknesses

as a major source of progress in DoD organizations. Since DISA created a task force to assess security Defense Megacenters (DMCs) in 1994 it has completed 542 Security Readiness Reviews (SRR), generated a total of 14,860 findings and reported that 11,418 of these findings had been corrected.[212] DISA also began drafting detailed technical guidance for individual systems called Security Technical Implementation Guides (STIG), which give minimum security standards for managing system software security. More specifically, STIGs[213]

> cover topics such as organizational relationships and responsibilities and the management processes and technical requirements needed to ensure hardware integrity, system software integrity, and data-level integrity. They define the requirements for interfacing the various components of system software and include such details as specific configuration options to be used, password management, testing requirements, and permissible levels of access to system resources. Most importantly, all DMC systems are subject to SRRs and DMC management is accountable for the findings generated. DISA officials and staff report that correcting SRR deficiencies is given a high priority because the status of SRR findings is a part of each DMC director's or commander readiness report.

At the same time, GAO noted that DISA's publishing of STIGs, while a good first step, is still deficient. Lag time in verification of when corrective actions are reported as completed and actually are completed is a serious oversight problem. Corrective actions are reported as being completed in the SRR database when in fact they may not be verified for several months.[214]

> DISA has published STIG's for most of its systems and expects to have performed SRRs of all its systems before the end of 1999. Additional action, however, is needed to improve DISA's oversight of information security. For example, while the DISA's inspector will generally verify any corrective actions taken while he or she is still on site, subsequent corrective actions are reported in the SRR database as having adequately addressed deficiencies even though the actions may not be verified until the next regularly scheduled inspection, which may be 15 to 36 months later. We found this practice has resulted in some inaccuracies. We tested 55 deficiencies that were "accepted-as-fixed" in the SRR database and determined that about one-fourth had not been corrected. For example, several DMCs had reported that their system software configuration options had been changed to conform to DISA requirements, and the SRR database had been updated accordingly. However, our testing showed that the options in question were not in compliance with DISA standards. We did not attempt to determine whether these inconsistencies were the result of oversights, misrepresentations, or other factors. DISA officials agreed more timely, independent verification of corrective actions is desirable and reported that they were exploring ways to address the issue.
>
> Other DoD components had not made similar progress in instituting an effective oversight process. The modest improvements that these components had made were a result of individual and isolated command or unit actions rather than comprehensive service, agency, or department actions.

GAO reported that overall the DoD has developed but not yet implemented a department-wide information security program. In 1996, GAO made several recommendations to DoD after

it found that the department "lacked a department-wide security program to comprehensively address the general control weaknesses we had identified." DoD concurred with these recommendations and issued plans for a Defense-wide Information Assurance Program (DIAP) which would "provide the framework for a comprehensive information security program. As of the 1999 report GAO found that it was too early to assess how effective DIAP management and implementation plans have been implemented and whether or not DIAP's efforts would ensure adequate information security.[215]

Cyber and Information Warfare and the Role of the Intelligence Community

Most intelligence community offensive cyber activity is highly classified, and should be. There are no public break outs of federal spending on intelligence activity related to the defense of critical infrastructure, no unclassified assessments, and few useful leaks. At the same time, there are enough anecdotal reports to raise important questions.

- *Who is in charge of intelligence collection on foreign threats to the nation's critical infrastructure and information systems?* The issue here is not the designation of responsibility per se, but function capability. It simply is not clear that there is functional capability to carry out the necessary tasks, suitable coordination and information flow, and close communication with users.

- *Is there sufficient coordination within the intelligence community and flow to users?* Virtually all intelligence agency personnel privately complain about a lack of adequate coordination within the intelligence community, particularly about the flow of information from NSA. Many such complaints, however, seem to be parochial, and many user complaints seem to stem from poor user tasking and prioritization. The Gulf War, Kosovo, and areas like missile threat analysis have revealed serious problems in these areas, but it is not clear what problems specifically affect the problem of critical infrastructure protection.

- *Does the community have the necessary resources?* The numbers and quality of technical personnel seem to be inadequate, adequate funding often does not go to technical expertise and capability, and there is heavy dependence on contractors under conditions where contract awards and management often seem to be poorly handled and involve long delays and misuse of the resulting work effort.

- *What is the responsibility of the intelligence community to wage offensive warfare?* The war in Kosovo showed that the intelligence community still had many of the coordination problems exposed during the Cold War. More than that, it indicated that the natural collection and analysis bias of the intelligence community meant that it was not ready to wage offensive information warfare even against a local and relatively weak opponent. The intelligence community often proposes the use of aggressive information warfare at games and exercises, but many proposals reveal a theoretical or conceptual understanding of the role such warfare might play that is not supported by technical expertise. There are indications that the community is better prepared to "talk the talk" than "digitize the digits." It is also often far from clear that the community and US military are effectively organized to coordinate in such actions.

- *What are the special responsibilities of the CIA and NSA?* It is unclear from the open literature that the federal government has yet conducted a zero-based review of the role the nation's key intelligence agencies must play in dealing with cyberthreats, although there are indications that such a review may be underway at NSA. Once again, the issue is not assigning responsibility or creating organizational structures, but one of determining exactly what capabilities are needed and ensuring that they are properly staffed and funded.

    - *The risk of deep management and conceptual failures within the intelligence community.* It is dangerous to try to assess the adequacy of the efforts of agencies like NSA, and the many other intelligence efforts dealing with information warfare, from the outside and without fully access to classified information. At the same time, it is far from clear that NSA and other members of the intelligence community have the personnel, technology, and resources to carry out their information warfare and cyberattack/defense missions. It is also far from clear that there has been sufficient net assessment of the trends in technology, the growth of private sector use of advanced information systems, and intelligence collection and analysis resources to determine how NSA and other relevant intelligence agency efforts will cope in the future. It is at least possible that the capability of national technical means will slowly erode over time or require major unprogrammed investment.

- *Has a proper net technology assessment been conducted to support intelligence planning and programming?* Much of the community activity seems to be centered around concepts that are not supported by a coherent view of the present and probable technical capabilities of our allies and opponents, and the balance of offensive and defensive technology. It is unclear that programs and activities must be evaluated in these terms, or that program goals and milestones are based on such an evaluation.

- *Do adequate laws and regulations exist to allow the proper coordination between intelligence and law enforcement?* There seem to be serious problems in ensuring the kind of near real-time exchange of data needed between the intelligence community, law enforcement, and those under attack. Legal problems exist at one level because of the risk of spying on US citizens, and at another level because law enforcement agencies often cannot or will not report on ongoing investigations or cases before a grand jury or trial.

Total Spending on National Security Activity

The OMB estimate of total national security agency spending on critical infrastructure protection is shown in Table 5.15 below: There is no indication of the extent to which this activity relates to offensive and retaliatory capabilities in cyberwarfare, and the level of preparation for asymmetric attacks by states, their proxies, and major terrorist groups versus lower levels of attack. Similarly, no data are available on NSA plans to maintain and improve national collection capabilities in this area, and as the whether net technical assessments have been performed to estimate future NSA capability (or that of any other element of the national security community.)

Table 5.15

National Security Community Spending for Critical Infrastructure Protection

	FY1998	FY1999	FY2000	FY2001
National Security				
Critical Infrastructure Protection	974.56	1,185.22	1,402.94	1,458.91
Federal Infrastructure Protection	956.27	1,160.80	1,379.56	1,420.05
Education and Training	36.53	46.42	73.61	81.46
Intrusion Monitoring and Response	108.66	158.70	172.79	187.18
Multiple Program Areas	218.33	265.01	379.77	348.08
Reconstitution	25.50	29.17	15.40	5.19
System Protection	503.58	584.28	630.23	638.12
Threat/Vulnerability/Risk Assessment	63.67	77.22	107.75	160.01
CIP Assistance/Outreach to Private Sector	18.29	24.42	23.38	38.86
Intrusion Monitoring and Response	0.00	0.80	0.24	0.24
Multiple Program Areas	13.29	15.52	18.04	18.82
System Protection	5.00	7.15	5.10	4.80
Threat/Vulnerability/Risk Assessment	0.00	0.95	0.00	15.00

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," Figures part of 2001 budget

Department of State

The OMB reporting on the State Department's role in critical infrastructure protection does not provide a detailed description. The GAO reported in May 1998, however, that its tests on State computer systems were "very susceptible to hackers, terrorists, or other unauthorized individuals seeking to damage State operations or reap financial gain by exploiting the department's information security weaknesses."[216]

An independent accounting firm reported in August of 1999 that the Department of State's mainframe computers for domestic operations were vulnerable to unauthorized access. "Consequently, other systems, which process data using these computers, could also be vulnerable

Department of Transportation

The DOT is lead federal agency for protecting the transportation sector from both

physical and cyber threats and has had significant funding, especially in FY2001 where $99.34 million has been requested for CIP protection. A total of $97 million of the requested FY2001 budget is slated for public CIP assistance. Another $60.45 million is allocated in the budget for threat, vulnerability and assessments an increase from the $29.33 enacted in FY2000.

Table 5.16

Department of Transportation Spending for Critical Infrastructure Protection

	FY1998	FY1999	FY2000	FY2001
Department of Transportation				
Critical Infrastructure Protection	20.33	24.88	50.68	99.34
Federal Infrastructure Protection	0.94	1.42	1.49	2.32
Reconstitution	0.30	0.30	0.37	0.45
System Protection	0.64	1.12	1.12	1.12
Threat/Vulnerability/Risk Assessments	0.00	0.00	0.00	0.75
CIP Assistance/Outreach to Private Sector	19.39	23.46	49.19	97.03
Intrusion Monitoring and Response	0.00	0.00	0.00	1.50
Multiple Program Areas	0.00	0.00	0.00	4.00
Public Awareness/Outreach	0.00	0.00	0.10	2.05
Reconstitution	0.00	0.00	0.00	0.13
System Protection	7.47	8.95	19.76	28.90
Threat/Vulnerability/Risk Assessments	11.92	14.51	29.33	60.45

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," Figures part of 2001 budget

Department of Treasury

The Treasury is the lead federal agency in banking and finance. Treasury is scheduled to receive $87.03 million for CIP efforts in the FY2001 budget. Of this money, $4 million is to go to research and development into "authentication technologies; physical and electronic protection technologies; test facilities; simulation model development information security analysis; intrusion indications and warning tools system reliability enhancement; information system standardization; electronic commerce security enhancement."[217] Another $7 million is to go to protecting Public Key Infrastructures (PKI)

Table 5.17

Department of Treasury Spending for Critical Infrastructure Protection

	FY1998	FY1999	FY2000	FY2001
Department of Treasury				
Critical Infrastructure Protection	**22.91**	**48.89**	**76.21**	**87.03**
Federal Infrastructure Protection	10.94	35.86	61.27	67.73
Intrusion Monitoring and Response	1.50	5.50	4.70	4.70
System Protection	4.64	11.06	4.47	10.93
Threat/Vulnerability/Risk Assessments	4.80	19.30	52.10	52.10
CIP Assistance/Outreach to Private Sector	11.96	13.03	14.96	19.30
Education and Training	1.14	1.60	1.60	2.00
Intrusion Monitoring and Response	3.25	3.17	3.12	3.12
Multiple Program Areas	0.00	0.00	0.00	4.00
Public Awareness/Outreach	0.00	0.00	0.20	0.20
System Protection	0.78	1.36	1.24	1.08
Threat/Vulnerability/Risk Assessments	6.80	6.90	8.80	8.90

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," Figures part of 2001 budget

Department of Veterans Affairs

The Department of Veterans spends the majority of the $17.33 million in FY 2000 and $17.39 million requested in FY2001 on systems protection. ($15.6 in FY2000 and $15.65 in FY2001).[218] The rest is spent on education and training and threat assessments.

According to an October 1999 GAO report, "serious weaknesses placed sensitive information belonging to the Department of Veterans Affairs at risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possible occurring without detection." GAO writes that such findings were disturbing because "VA collects and maintains sensitive medical record and benefit payment information for veterans and family members and is responsible for tens of billions of dollars of benefit payments annually."[219]

Table 5.18

Department of Veterans Affairs Spending for Critical Infrastructure Protection

Department of Veterans Affairs	FY1998	FY1999	FY2000	FY2001
Critical Infrastructure Protection	**0.00**	**0.00**	**17.33**	**17.39**
Federal Infrastructure Protection	0.00	0.00	17.33	17.39
Education and Training	0.00	0.00	0.82	0.81
System Protection	0.00	0.00	15.60	15.65
Threats/Vulnerability/Risk Assessments	0.00	0.00	0.91	0.93

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," Figures part of 2001 budget

VI. Conclusions and Recommendations

The US faces real and growing potential threats from state actors, their proxies, or independent extremists and terrorists. While various analysts have tended to exaggerate the immediate threat, or the current threat posted by given actors, this does not mean that the threat is not real or that the nation does not need to improve its defense and response capabilities.

The US cannot bet the lives and well being of its citizens on today's threats and probabilities. 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. US involvement in the world, the strength of US conventional and nuclear forces, and vulnerability at home are a dangerous combination, and unless the US acts to improve both deterrence and defense, the risk of major asymmetric and terrorist attacks involving CBRN weapons is likely to grow.

Finding the right mix of defense and response will be extremely difficult and it is far easier to call for dramatic action than to determine what actions will really succeed and be cost-effective, and then execute them. It is clear from the preceding analysis that the federal government is making 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 is much to be done. There are many areas where basic research and planning activity is needed to resolve grave uncertainties, and others where special interest pleading threatens to waste vast amounts of public money on the wrong priorities or measures which may either be ineffective or easy to counter. There have been far more attempts to define broad strategies or issue broad directives than come to grips with the need for detailed planning, adequate programs, and program budgets, and meaningful ways to review and coordinate annual budgets and programs.

Many proposed and ongoing programs probably cannot meet the most basic tests of intellectual validity and federal responsibility. There is no long term plan, program, or program budget. There is no supporting analysis of the balance of offense and defense, the countermeasures that could defeat a given program and the cost to defeat it. There is nothing approaching an adequate ongoing national threat analysis of domestic and foreign threats, no net assessment of the overall balance of defense and offense, and no net technical assessment of the trends in offensive and defensive capability.

Effective planning and action cannot be based itself on vague calls for improved strategy, exercising and training based on today's threat analyses and techniques, or altering organization charts at the top. It will take years of effort to create a coordinated and effective plan for federal, state, and local action. In most cases, it is the willingness and ability to address detailed issues and to make hands on efforts to create and implement a wide range of cost-effective programs that will determine the success of the US effort in Homeland Defense and not the effort to find a few major recommendations. The devil really does lie the details, and "bumper sticker" or one-issue approaches to policy, are a recommendation for disaster.

Improved management, planning, programming, and analysis is only one of many steps that need to be taken, Nevertheless, there many such areas where the federal government probably needs to take action.

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. The US budget, and agency program and budget descriptions 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, however, is threat-driven. It does not describe and justify the program, it simply 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 measure. 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 transparency and 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.*

- *Regions, state, local governments, and private entities cannot prepare in a closed environment, and there is little opportunity for feedback from outside the federal government. Equally, there is little practical way to determine the best trade-offs between federal, regional, state, and local efforts.* There cannot be an effective national partnership in dealing with Homeland defense, or basis for popular support, without a high degree of transparency as to federal efforts and ongoing discussion and debate over what needs to be done. The federal government lacks every conceivable element of the capability to plan and impose effective Homeland defense on state and local governments and the private sector. It needs constant feedback and commentary, and federal officials need to be exposed to constant challenge from state and local officials and experts, as well as analysts outside the federal government.

- *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.

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 importantly, 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 might 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 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.

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

The US would face serious resource allocation problems even if the threats were less uncertain and ambiguous. 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.

Unfortunately, however, the sudden popularity of Homeland defense 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 threats that different methods of attack can

pose.. 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.” 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 and immigration. 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 largely threat driven and the cost of new activities is relatively limited. As long as current outlays are limited, it is all too easy to 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 starting far more activities than can be finished, failing to consider the future trade-offs that must be made to deploy effective capabilities, duplicating other efforts, or refashioning 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 to develop clear priorities, ensure that cost estimates are provided of bringing 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.

- *The US must develop future year plans and coordinated program budgets.* It must develop five-year plans for on going programs, and long term RDT&E plans that include deployment plans and cost and supporting net threat assessments, for each federal department and agency. It must coordinate them at the White House level, where it will also be necessary to carry out review of relevant annual budget submissions to ensure the continued execution of federal efforts.

- *Carry out net technical assessments of the changing CBRN threat and of the technological options to improve defense and response capabilities.* Examine both the threat and federal RCT&E efforts in ways that support coordinated efforts to use technology to improve Homeland defense and response, which ensure the uncertainties in threat effects are reduced, that RDT&E efforts are tied to practical deployment plans, and risk assessments examine the cost to defeat new programs and RDT&E efforts.

- *Immediately undertake efforts that are not-resource-intensive, such as contingency planning on legal, psychosocial, and even military issues.* This planing should extend to worst case scenarios involving asymmetric state attacks, nuclear attacks, and major biological attacks, and involving the use of mixes of agents, multiple attacks, attacks against multiple cities or targets, and sequential and copy-cat attacks.

Unless this level of transparency and improve planning and programming 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 encourage 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.

---

[1] This history is based on material provided by BMDO.

[2] Based primarily on "Ballistic Missile Defense Organization Budgetary History," Ballistic Missile Defense Office, BMDO Fact Sheet PO-99-02, April 1999.

[3] Based primarily on "Ballistic Missile Defense Organization Budgetary History," Ballistic Missile Defense Office, BMDO Fact Sheet PO-99-02, April 1999.

[4] General Accounting Office, "National Missile Defense: Even With Increased Funding Technical and Schedule Risks are High," GAO/NSIAD-98-153, June 1998. Also see National Missile Defense: Schedule and Technical Risks Represent Significant Development Challenges (GAO/NSIAD-98-28, Dec. 12, 1997.

[5] General Accounting Office, "National Missile Defense: Even With Increased Funding Technical and Schedule Risks are High," GAO/NSIAD-98-153, June 1998. Also see National Missile Defense: Schedule and Technical Risks Represent Significant Development Challenges (GAO/NSIAD-98-28, Dec. 12, 1997.

[6] GAO, "National Missile Defense: Even With Increased Funding Technical and Schedule Risks Are High" (Letter Report, 06/23/98, GAO/NSIAD-98-153).

[7] The following history is adapted from General Accounting Office, "National Missile Defense: Even With Increased Funding Technical and Schedule Risks are High," GAO/NSIAD-98-153, June 1998. Also see National Missile Defense: Schedule and Technical Risks Represent Significant Development Challenges (GAO/NSIAD-98-28, Dec. 12, 1997.

[8] Jane's Missiles and Rockets, Vol. 3, No. 9, September 1, 1999.

[9] Jane's Missiles and Rockets, Vol. 3, No. 9, September 1, 1999.

[10] Announcement by Jaime Rubin, US State Department, September 9, 1999; The Vancouver Sun, September 10, 1999.

[11] `National Defense Authorization Act for Fiscal Year 2000', Sections 231-236.

[12] Phillp E. Coyle III, Director of Operational Test and Evaluation, Department of Defense, Annual Report for FY1999, Section VI, February 2000.

[13] Phillp E. Coyle III, Director of Operational Test and Evaluation, Department of Defense, Annual Report for FY1999, Section VI, February 2000.

[14] Statement of Lieutenant General Ronald T. Kadish, USAF, Director, Ballistic Missile Defense Organization, to the Senate Appropriations Committee, Defense Subcommittee,, April 12, 2000

[15] Washington Times, July 14, 2000, p. A-1.

[16] Lt. General Lyles, House Armed Services Committee Subcommittee on Military Research & Development, Hearing on ballistic missile defense programs, February 25, 1999, Library of Congress internet transcript.

[17] Phillp E. Coyle III, Director of Operational Test and Evaluation, Department of Defense, Annual Report for FY1999, Section VI, February 2000.

[18] THE WHITE HOUSE

Office of the Press Secretary, Fact Sheet, "National Missile Defense," September 1, 2000.

[19] Congressional Budget Office (CBO), "Budgetary Implications of National Missile Defense," April 2000, pp. 6-10.

[20] Congressional Budget Office (CBO), "Budgetary Implications of National Missile Defense," April 2000, pp. 15-22.

[21] Congressional Budget Office (CBO), "Budgetary Implications of National Missile Defense," April 2000, pp. 31-35.

22 General Accounting Office, National Missile Defense: Schedule and Technical Risks Represent Significant Development Challenges, GAO/NSIAD-98-28 (December 1997).

[23] GAO/T-NSIAD-98-164, "Combating Terrorism," April 23, 1998, P. 3.

[24] 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

[25] GAO/T-NSIAD-98-164, "Combating Terrorism," April 23, 1998, P. 4.
[26] GAO/T-NSIAD-98-164, "Combating Terrorism," April 23, 1998, P. 6.

[27] GAO/T-NSIAD-00-145, p. 5.

[28] Center for Nonproliferation Studies, Monterey Institute of International Studies, "Agency Structures for Terrorism Response," 1999, http://www.cns.miis.edu/research/cbw/response.htm

[29] White House, Office of the Press Secretary For Immediate Release, "Funding for Domestic Preparedness and Critical Infrastructure Protection," Fact Sheet, January 22, 1999.

[30] Executive Office of the President, Office of Budget and Management, "Annual Report to Congress on Combating Terrorism," May 2000

[31] 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

[32] 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

[33] 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

[34] 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

[35] 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

[36] Washington Post - Letters to the Editor, Standing Tall Overseas, August 17, 2000; Page A-28.

[37] Center for Nonproliferation Studies, Monterey Institute of International Studies, "Agency Structures for Terrorism Response," 1999, http://www.cns.miis.edu/research/cbw/response.htm

[38] National Commission on Terrorism, "Countering the Changing Threat of International Terrorism," June, 2000

[39] 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

[40] First Annual Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving the Use of Weapons of Mass Destruction, I. Assessing the Threat, December 15, 1999, www.rand.org/organization/nsrd/terrpanel/

[41] National Commission on Terrorism, "Countering the Changing Threat of International Terrorism," June, 2000

[42] 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

[43] Department of Defense, Office of Combating Terrorism Policy and Support, Combating Terrorism Activities, FY2001, Washington, DC, January 14, 2000.

[44] Department of Defense, Combating Terrorism Activities, Office of Combating Terrorism Policy and Support, Programs, Resources and Assessments Directorate, p. 352.

[45] See Department of Defense, Combating Terrorism Activities, Office of Combating Terrorism Policy and Support, Programs, Resources and Assessments Directorate, pp. 296-297.

[46] Department of Defense, Office of Combating Terrorism Policy and Support, Combating Terrorism Activities, FY2001, Washington, DC, January 14, 2000, p. 193.

[47] Department of Defense, Office of Combating Terrorism Policy and Support, Combating Terrorism Activities, FY2001, Washington, DC, January 14, 2000, p. 213.

[48] United States General Accounting Office, "Combating Terrorism: Action Taken but Considerable Risks Remain for Forces Overseas," GAO/NSIAD-00-181, July 19, 2000, http://www.gao.gov/new.items/ns00181.pdf

[49] United States General Accounting Office, "Combating Terrorism: Action Taken but Considerable Risks Remain for Forces Overseas," GAO/NSIAD-00-181, July 19, 2000, http://www.gao.gov/new.items/ns00181.pdf

[50] United States General Accounting Office, "Combating Terrorism: Action Taken but Considerable Risks Remain for Forces Overseas," GAO/NSIAD-00-181, July 19, 2000, http://www.gao.gov/new.items/ns00181.pdf

[51] Department of Defense, Combating Terrorism Activities, Office of Combating Terrorism Policy and Support, Programs, Resources and Assessments Directorate, pp. 343-350.

[52] 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

[53] 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

[54] Department of Defense, Office of Combating Terrorism Policy and Support, Combating Terrorism Activities, FY2001, Washington, DC, January 14, 2000.

[55] 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

[56] 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

[57] 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

[58] William S. Cohen, Department of Defense, "Annual Report to the President and the Congress," 2000, http://www.dtic.mil/execsec/adr2000/chap7.html

[59] 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

[60] 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

[61] 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

[62]Department of Defense, Combating Terrorism Activities, Office of Combating Terrorism Policy and Support, Programs, Resources and Assessments Directorate, p. 384.

[63] 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

[64] Department of Defense, Office of Combating Terrorism Policy and Support, Combating Terrorism Activities, FY2001, Washington, DC, January 14, 2000, p. 361.

[65] 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

[66] 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

[67] William S. Cohen, Department of Defense, "Annual Report to the President and the Congress," 2000, http://www.dtic.mil/execsec/adr2000/chap7.html

[68] 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

[69] Cragin, Charles, "Defense Leaders Commentary: The Facts on WMD Civil Support Teams," March 31, 2000, http://www.defenselink.mil/news/Mar2000/n0331200_20003311.html

[70] Department of Defense, Combating Terrorism Activities, Office of Combating Terrorism Policy and Support, Programs, Resources and Assessments Directorate, p. 369.

[71] Department of Defense, Combating Terrorism Activities, Office of Combating Terrorism Policy and Support, Programs, Resources and Assessments Directorate, p. 375.

[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] Department of Defense, Combating Terrorism Activities, Office of Combating Terrorism Policy and Support, Programs, Resources and Assessments Directorate, p. 394.

[74] Cragin, Charles, "Defense Leaders Commentary: The Facts on WMD Civil Support Teams," March 31, 2000, http://www.defenselink.mil/news/Mar2000/n03312000_20003311.html

[75] Department of Defense, Combating Terrorism Activities, Office of Combating Terrorism Policy and Support, Programs, Resources and Assessments Directorate, pp. 325 and 338.

[76] Department of Defense, Combating Terrorism Activities, Office of Combating Terrorism Policy and Support, Programs, Resources and Assessments Directorate, pp. 378-382.

[77] Department of Defense, Combating Terrorism Activities, Office of Combating Terrorism Policy and Support, Programs, Resources and Assessments Directorate, p. 326.

[78] Department of Defense, Combating Terrorism Activities, Office of Combating Terrorism Policy and Support, Programs, Resources and Assessments Directorate, p. 382.

[79] 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

[80] Center for Nonproliferation Studies, Monterey Institute of International Studies, "Agency Structures for Terrorism Response," 1999, http://www.cns.miis.edu/research/cbw/response.htm

[81] 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

[82] 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

[83] 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

[84] 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

[85] 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

[86] 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

[87] Center for Nonproliferation Studies, Monterey Institute of International Studies, "Agency Structures for Terrorism Response," 1999, http://www.cns.miis.edu/research/cbw/response.htm

[88] 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

[89] 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

[90] 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

[91] 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

[92] 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

[93] 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

[94] 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

[95] 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

[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] Center for Nonproliferation Studies, Monterey Institute of International Studies, "Agency Structures for Terrorism Response," 1999, http://www.cns.miis.edu/research/cbw/response.htm

[98] 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

[99] 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

[100] 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

[101] 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

[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] National Commission on Terrorism, "Countering the Changing Threat of International Terrorism," June, 2000

[105] 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

[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] Department of Health and Human Services, "Medical Response in Emergencies: HHS Role," May 18, 2000, http://www.hhs.gov/news/press/2000pres/20000518a.html

[108] 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

[109] 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

[110] 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

[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] National Commission on Terrorism, "Countering the Changing Threat of International Terrorism," June, 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] 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

[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, "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

[119] National Commission on Terrorism, "Countering the Changing Threat of International Terrorism," June, 2000

[120] National Commission on Terrorism, "Countering the Changing Threat of International Terrorism," June, 2000

[121] United States General Accounting Office, "Combating Terrorism: Linking Threats to Strategies and Resources," GAO/T-NSIAD-00-218, July 26, 2000, http://www.gao.gov/new.items/ns00218t.pdf

[122] National Domestic Preparedness Office, "Blueprint for the National Domestic Preparedness Office," http://www.ndpo.gov/blueprint.pdf

[123] National Domestic Preparedness Organization website, http://www.ndpo.gov/responders.htm

[124] 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

[125] First Annual Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving the Use of Weapons of Mass Destruction, I. Assessing the Threat, December 15, 1999, www.rand.org/organization/nsrd/terrpanel/

[126] United States General Accounting Office, "Combating Terrorism: Linking Threats to Strategies and Resources," GAO/T-NSIAD-00-218, July 26, 2000, http://www.gao.gov/new.items/ns00218t.pdf

[127] Department of Justice, Office of Justice Program, Office for State and Local Domestic Preparedness Support website, http://www.ojp.usdoj.gov/osldps/

[128] 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

[129] 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

[130] 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

[131] 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

[132] 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

[133] 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

[134] 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

[135] 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

[136] United States General Accounting Office, "Combating Terrorism: Linking Threats to Strategies and Resources," GAO/T-NSIAD-00-218, July 26, 2000, http://www.gao.gov/new.items/ns00218t.pdf

[137] 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

[138] National Commission on Terrorism, "Countering the Changing Threat of International Terrorism," June, 2000

[139] 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

[140] 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

[141] Federal Bureau of Investigation, ANSIR website, http://www.fbi.gov/programs/ansir/ansir.htm

[142] 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

[143] 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

[144] 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

[145] 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

[146] 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

[147] 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

[148] 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

[149] 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

[150] 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

[151] 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

[152] National Commission on Terrorism, "Countering the Changing Threat of International Terrorism," June, 2000

[153] Ambassador Michael Sheehan, Office of the Coordinator for Counterrrorism, Testimony to the Senate Foreign Relations Committee, June 15, 2000, http://www.state.gov/www/policy_remarks/2000/000615_sheehan_terrorism.html

[154] 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

[155] 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

[156] 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

[157] 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

[158] 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

[159] 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

[160] National Commission on Terrorism, "Countering the Changing Threat of International Terrorism," June, 2000

[161] 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

[162] 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

[163] 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

[164] "National Plan…." Page 122
[165] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 6.
[166] "National Plan for Information Systems Protection, Version One" January 2000, p. 126.
[167] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 3.
[168] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 7.
[169] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, pp. 17-18.
[170] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 78.
[171] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 17.
[172] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 70.
[173] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 69.
[174] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 23.
[175] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 23-24.
[176] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 23.
[177] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 18.
[178] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 23-24.
[179] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 24.

[180] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 24.
[181] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, pp.26-27.
[182] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 27.
[183] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 37.
[184] Federal Information Security: Actions Needed to Address Widespread Weaknesses (GAO/T-AIMD-00-135, March 29, 2000)p. 2.

[185] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 69.
[186] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 71.
[187] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 69.
[188] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 71.
[189] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 30.
[190] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, pp. 71-72.
[191] *Information Security: Many NASA Mission-Critical Systems Face Serious Risks* (GAO/AIMD-99-47, May 20, 1999) p. 1.
[192] *Information Security: Many NASA Mission-Critical Systems Face Serious Risks* (GAO/AIMD-99-47, May 20, 1999) p. 2.
[193] *Information Security: Many NASA Mission-Critical Systems Face Serious Risks* (GAO/AIMD-99-47, May 20, 1999) p. 2.

[194] *Information Security: Many NASA Mission-Critical Systems Face Serious Risks* (GAO/AIMD-99-47, May 20, 1999) pp. 16-17.
[195] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, pp. 72, 75.
[196] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 40.
[197] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 41.
[198] Walter Pincus, "Defense Department Computers Vulnerable to Attack," Washington Post, December 8, 2000, Internet edition.
[199] Walter Pincus, "Defense Department Computers Vulnerable to Attack," Washington Post, December 8, 2000, Internet edition.
[200] http://www.defenselink.mil/pubs/ *Depsecweb.pdf*
[201] Walter Pincus, "Defense Department Computers Vulnerable to Attack," Washington Post, December 8, 2000, Internet edition.
[202] Walter Pincus, "Defense Department Computers Vulnerable to Attack," Washington Post, December 8, 2000, Internet edition.
[203] Walter Pincus, "Defense Department Computers Vulnerable to Attack," Washington Post, December 8, 2000, Internet edition.
[204] Gerry J. Gilmore, "DoD Taps Reservists To Fill New Info Ops Units," American Forces Press Service, December 8, 2000.

[205] GAO/AIMD-99-107 "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999, p. 14-15.
[206] GAO/AIMD-99-107 "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999, Appendix I. pp. 24-25.

[207] GAO/AIMD-99-107 "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999, p. 17-18.

[208] GAO/AIMD-99-107 "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999, p. 8.
[209] GAO/AIMD-99-107 "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999, p. 3.
[210] GAO/AIMD-99-107 "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999, p. 5.
[211] GAO/AIMD-99-107 "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999, pp. 8-12.
[212] GAO/AIMD-99-107 "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999, pp. 12.
[213] GAO/AIMD-99-107 "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999, p. 13.
[214] GAO/AIMD-99-107 "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999, p. 13.
[215] GAO/AIMD-99-107 "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999, p. 14.
[216] Federal Information Security: Actions Needed to Address Widespread Weaknesses (GAO/T-AIMD-00-135, March 29, 2000) p. 3.
[217]"Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 34-35.
[218] "Annual Report to Congress on Combating Terrorism: Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection" May 18, 2000, p. 73.
[219] Federal Information Security: Actions Needed to Address Widespread Weaknesses (GAO/T-AIMD-00-135, March 29, 2000)p. 3.