AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

COMBATING TERRORISM: ASSESSING THREATS, RISK MANAGEMENT AND ESTABLISHING PRIORITIES

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

JULY 26, 2000

Serial No. 106–253

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

74–263 DTP WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512–1800 Fax: (202) 512–2250
Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. MCINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
BOB BARR, Georgia
DAN MILLER, Florida
ASA HUTCHINSON, Arkansas
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin
HELEN CHENOWETH-HAGE, Idaho
DAVID VITTER, Louisiana

HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee
JANICE D. SCHAKOWSKY, Illinois

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JAMES C. WILSON, *Chief Counsel*
ROBERT A. BRIGGS, *Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS

CHRISTOPHER SHAYS, Connecticut, *Chairman*

MARK E. SOUDER, Indiana
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
DAVID M. MCINTOSH, Indiana
MARSHALL "MARK" SANFORD, South Carolina
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
HELEN CHENOWETH-HAGE, Idaho

ROD R. BLAGOJEVICH, Illinois
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
JOHN F. TIERNEY, Massachusetts
THOMAS H. ALLEN, Maine
EDOLPHUS TOWNS, New York
BERNARD SANDERS, Vermont (Independent)
JANICE D. SCHAKOWSKY, Illinois

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

LAWRENCE J. HALLORAN, *Staff Director and Counsel*
R. NICHOLAS PALARINO, *Senior Policy Analyst*
JASON CHUNG, *Clerk*
DAVID RAPALLO, *Minority Counsel*

CONTENTS

	Page
Hearing held on July 26, 2000	1
Statement of:	
Bremer, Ambassador Paul, chairman, National Commission on Terrorism; Michael Wermuth, Rand Corp., senior policy analyst; John Parachini, Monterey Institute of International Studies, executive director; and W. Seth Carus, National Defense University, senior research professor	42
Rabkin, Norman, General Accounting Office, Director, National Security and International Affairs Division, accompanied by Stephen Caldwell, Assistant Director; and Raphael Perl, Congressional Research Service, Specialist in International Affairs	5
Letters, statements, etc., submitted for the record by:	
Blagojevich, Hon. Rod R., a Representative in Congress from the State of Illinois, letter dated July 26, 2000	97
Carus, W. Seth, National Defense University, senior research professor, prepared statement of	82
Parachini, John, Monterey Institute of International Studies, executive director, prepared statement of	57
Perl, Raphael, Congressional Research Service, Specialist in International Affairs, prepared statement of	25
Rabkin, Norman, General Accounting Office, Director, National Security and International Affairs Division, prepared statement of	7
Shays, Hon. Christopher, a Representative in Congress from the State of Connecticut, prepared statement of	3
Wermuth, Michael, Rand Corp., senior policy analyst, prepared statement of	47

COMBATING TERRORISM: ASSESSING THREATS, RISK MANAGEMENT AND ESTABLISHING PRIORITIES

WEDNESDAY, JULY 26, 2000

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 1 p.m., in room 2247, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shays and Blagojevich.

Staff present: Lawrence Halloran, staff director and counsel; J. Vincent Chase, chief investigator; R. Nicholas Palarino, senior policy advisor; Thomas Costa, professional staff member; Jason M. Chung, clerk; David Rapallo, minority counsel; and Earley Green, minority assistant clerk.

Mr. SHAYS. The hearing will come to order. Earlier today we heard testimony in closed session from those familiar with very specific and very sensitive aspects of the threats posed by terrorists to U.S. citizens and property at home and abroad. That information provided some depth and clarity to the subcommittee's ongoing oversight of governmentwide terrorism issues.

But terrorism also has a very public face. Using fear and panic as weapons, terrorists seek to amplify and transform crimes against humanity into acts of war. The growing and changing threat of terrorism requires an ongoing public discussion of the appropriate strategy, priorities and resources to protect public health and national security.

That discussion brings us here this afternoon. As this point in the evolution of our post cold war response to the new realities of a dangerous world, we should have a dynamic, integrated assessment of the threat posed by foreign and domestic-origin terrorism. We should have a truly national strategy to counter the threat. And to implement that strategy, we should have a clear set of priorities to guide Federal programs and funding decisions.

But for reasons of bureaucratic Balkanization, program proliferation, and a tendency to skew threat assessments toward worst-case scenarios, we still lack those important elements of a mature, effective policy to combat terrorism. In place of a national strategy, the administration points to an accumulation of event driven Presidential decision directives wrapped in a budget-driven 5-year plan.

Congress has also contributed to the fragmentation and shifting priorities in counterterrorism programs, responding to crises with new laws and increased funding, but failing to reconcile or sustain those efforts over time.

Yesterday, the House passed the Preparedness Against Terrorism Act of 2000 (H.R. 4210) to elevate and better focus responsibility for Federal programs to combat terrorism. If enacted into law, the bill should provide greater structure and discipline to the $11 billion effort to deter, detect and respond to terrorism. But any rearrangement of boxes on the organizational chart will only be effective if those involved are able to distinguish between theoretical vulnerabilities and genuine risks, and set clear priorities.

So we asked our witnesses this afternoon to join our public oversight of these pressing issues. As the administration and Congress attempt to refine threat and risk assessments, formulate strategic goals and target program funding, this subcommittee will continue to rely on their experience and their insights. We welcome them and look forward to their testimony, and you have been sworn in because in our closed door hearing you were all sworn in. So we can just have you begin.

[The prepared statement of Hon. Christopher Shays follows:]

DAN BURTON, INDIANA
CHAIRMAN

BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
JOHN L. MICA, FLORIDA
THOMAS M. DAVIS, VIRGINIA
DAVID M. McINTOSH, INDIANA
MARK E. SOUDER, INDIANA
JOE SCARBOROUGH, FLORIDA
STEVEN C. LaTOURETTE, OHIO
MARSHALL "MARK" SANFORD, SOUTH CAROLINA
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
ASA HUTCHINSON, ARKANSAS
LEE TERRY, NEBRASKA
JUDY BIGGERT, ILLINOIS
GREG WALDEN, OREGON
DOUG OSE, CALIFORNIA
PAUL RYAN, WISCONSIN
HELEN CHENOWETH-HAGE, IDAHO
DAVID VITTER, LOUISIANA

ONE HUNDRED SIXTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051
TTY (202) 225–6852

HENRY A. WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
ROBERT E. WISE, JR., WEST VIRGINIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
CHAKA FATTAH, PENNSYLVANIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
HAROLD E. FORD, JR., TENNESSEE
JANICE D. SCHAKOWSKY, ILLINOIS

BERNARD SANDERS, VERMONT
INDEPENDENT

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382
GROC.NS@mail.house.gov
http://www.house.gov/reform_ns/

Statement of Rep. Christopher Shays

July 26, 2000

Earlier today we heard testimony in closed session from those familiar with very specific and very sensitive aspects of the threats posed by terrorists to U.S. citizens and property at home and abroad. That information provided some depth and clarity to the Subcommittee's ongoing oversight of government-wide terrorism issues.

But terrorism also has a very public face. Using fear and panic as weapons, terrorists seek to amplify and transform crimes against humanity into acts of war. The growing and changing threat of terrorism requires an ongoing public discussion of the appropriate strategy, priorities and resources to protect public health and national security.

That discussion brings us here this afternoon. As this point in the evolution of our post-Cold War response to the new realities of a dangerous world, we should have a dynamic, integrated assessment of the threat posed by foreign and domestic-origin terrorism. We should have a truly national strategy to counter the threat. And, to implement that strategy, we should have a clear set of priorities to guide federal programs and funding decisions.

But for reasons of bureaucratic balkanization, program proliferation, and a tendency to skew threat assessments toward worst case scenarios, we still lack those important elements of a mature, effective policy to combat terrorism. In place of a national strategy, the administration points to an accumulation of event-driven Presidential Decision Directives wrapped in a budget-driven five-year plan.

Congress has also contributed to the fragmentation and shifting priorities in counter-terrorism programs, responding to crises with new laws and increased funding but failing to reconcile or sustain those efforts over time.

Yesterday, the House passed The Preparedness Against Terrorism Act of 2000 (H.R. 4210) to elevate and better focus responsibility for federal programs to combat terrorism. If enacted into law, the bill should provide greater structure and discipline to the 11 billion dollar effort to deter, detect and respond to terrorism. But any rearrangement of boxes on the organizational chart will only be effective if those involved are able to distinguish between theoretical vulnerabilities and genuine risks, and set clear priorities.

So we asked our witnesses this afternoon to join our public oversight of these pressing issues. As the administration and Congress attempt to refine threat and risk assessments, formulate strategic goals and target program funding, this Subcommittee will continue to rely on their experience and their insights. We welcome them and look forward to their testimony.

Mr. SHAYS. Mr. Rabkin.

STATEMENTS OF NORMAN RABKIN, GENERAL ACCOUNTING OFFICE, DIRECTOR, NATIONAL SECURITY AND INTERNATIONAL AFFAIRS DIVISION, ACCOMPANIED BY STEPHEN CALDWELL, ASSISTANT DIRECTOR; AND RAPHAEL PERL, CONGRESSIONAL RESEARCH SERVICE, SPECIALIST IN INTERNATIONAL AFFAIRS

Mr. RABKIN. Thank you, Mr. Chairman. With me is Steve Caldwell, who has been responsible for managing much of the GAO work, examining the Federal efforts to combat terrorism. We are pleased to be here this afternoon to discuss the use of threat and risk assessments to help prioritize and focus Federal resources to combat terrorism. This is an important issue because over 40 Federal agencies are involved, and the amount of Federal spending for combating terrorism will rise to $11 billion in the next fiscal year.

I would like to summarize the three main messages of my statement. The first message concerns the nature of the threat. How likely is it that a terrorist will use a chemical or biological weapon against the United States? The subcommittee was briefed this morning about the intelligence communities views on the threat Americans face from terrorist groups. When thinking about the threat, it is important to recognize that terrorists would face many difficulties using dangerous chemical or biological materials. First, the required components of chemical agents and highly infective strains of biological agents are difficult to obtain.

Second, in most cases, specialized knowledge is required in the manufacturing process and in improvising an effective delivery device for most chemical and nearly all biological agents that would likely be used in terrorist attacks. Finally, terrorists may have to overcome other obstacles to successfully launch an attack that would result in mass casualties such as unfavorable meteorological conditions and personal safety risks.

Our point is that policymakers should keep these inherent difficulties in mind when considering how the United States should act to prepare for and defend against these threats. Also, intelligence agencies should balance their assessments of the threat with the discussion of the difficulty in manufacturing and delivering it.

Our second message is the need to use threat and risk assessments to help develop a national strategy and help prioritize and focus program investments to combat terrorism. Much of the Federal effort to combat terrorism has been based upon vulnerabilities which are unlimited rather than on an analysis of credible threats which are limited. Some agencies have used and are still using worst case scenarios to plan and develop programs. For example, the Department of Health and Human Services began to establish a national pharmaceutical and vaccine stockpile that did not match intelligence agencies estimates of the more likely agents that terrorists might use. On the other hand, the Justice Department has started to develop a national threat and risk assessment. Justice is also supporting efforts of State and local governments to assess the threats they may face and the risks inherent in the choices they have on how to respond to those threats.

I would like to add that we remain concerned about whether the executive branch will develop a comprehensive national strategy for combating terrorism. In December, 1998, the Attorney General issued a 5-year plan that has many of the features that we would like to see in a national strategy. The recent update no longer include time lines, relative priorities or performance measures. In addition, the FBI, through the National Domestic Preparedness Office and the National Security Council, are also planning to develop national strategies. We also have concerns about who is in charge. As you know, in May 1998, Presidential Decision Directive 62 established the national coordinator for security, infrastructure protection, and counterterrorism in the National Security Council. However, H.R. 4210, which passed the House yesterday, will create a President's council on domestic terrorism preparedness in the White House with authorities similar to those of a drug czar. In addition, the Senate Appropriations Committee has proposed elevating the NPDO to a higher status within the Justice Department to be headed by an assistant attorney general.

My final message is how other countries allocate resources and determine funding priorities to combat terrorism. Foreign countries also face terrorist threats and have to develop programs and priorities to combat terrorism. In our April 2000 report to the subcommittee, we discussed how five foreign countries, Canada, France, the United Kingdom, Israel, and Germany, are organized to combat terrorism, including how they develop programs and direct resources. Our overall conclusions were that first, foreign officials believed that terrorist attacks are unlikely for a variety of reasons, including the reason that terrorists would face in producing and delivering chemical or biological weapons. Second, because of limited resources, these foreign governments make funding decisions for programs to combat terrorism based upon the likelihood of terrorist activity actually taking place, not on overall vulnerability to terrorist attacks.

And finally, also due to resource constraints, these officials said that they maximize their existing capabilities to address a wide array of threats before they create new capabilities or programs to respond to such attacks.

Mr. Chairman, this completes my oral statement, and Mr. Caldwell and I will be glad to answer your questions.

Mr. SHAYS. Thank you.

[The prepared statement of Mr. Rabkin follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m.
Wednesday,
July 26, 2000

COMBATING TERRORISM

Linking Threats to Strategies and Resources

Statement of Norman J. Rabkin, Director
National Security Preparedness Issues
National Security and International Affairs Division

GAO/T-NSIAD-00-218

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here to discuss our prior work and observations regarding the terrorist threat and the use of threat and risk assessments to help prioritize and focus resources to combat terrorism. This is an important issue because over 40 federal agencies are involved and the amount of federal spending for combating terrorism has risen to over $11 billion (as requested in the President's fiscal year 2001 budget). With so many agencies involved and so many resources at stake, ensuring that these funds are wisely and effectively used is both a challenge and an imperative. For more than 3 years we have evaluated and reported on a number of issues concerning federal programs and activities to combat terrorism. A list of related GAO products appears at the end of this statement.

Our testimony will first highlight important information on the threat, focusing specifically on the threat of terrorist attacks involving chemical, biological, radiological, or nuclear (CBRN) materials.[1] The second issue we will discuss is the need to use threat and risk assessments to help develop a national strategy and help prioritize and focus program investments to combat terrorism. Finally, we will share our observations on how other countries allocate resources and determine funding priorities to combat terrorism.

Summary

The first step in developing sound programs to combat terrorism is to develop a thorough understanding of the terrorist threat. U.S. intelligence agencies track and analyze terrorist threats, including the threat of terrorists using CBRN weapons or agents. In our view, some of the public statements intelligence community officials have made about the terrorist CBRN threat do not include important qualifications to the information they present. For example, terrorists would have to overcome significant technical and operational challenges to successfully make and release many

[1] For the purpose of this testimony, we will use the term CBRN instead of the more common but less precise term "weapons of mass destruction." While some agencies define weapons of mass destruction to include only chemical, biological, radiological and nuclear weapons, others define it to include large conventional explosives.

chemical or biological agents of sufficient quality and quantity to kill or injure large numbers of people without substantial assistance from a foreign government sponsor. These types of qualifications are important because, without them, policy makers in both the executive or legislative branch may get an exaggerated view of the terrorist CBRN threat.

The second step in developing sound programs is to conduct a threat and risk assessment that can be used to develop a strategy and guide resource investments. Much of the federal efforts to combat terrorism have been based upon vulnerabilities rather than an analysis of credible threats. For example, agencies have used and are still using improbable "worst case scenarios" to plan and develop programs. The executive branch has made progress implementing our recommendations that threat and risk assessments be done to improve federal efforts to combat terrorism. Such assessments could be an important tool in developing a national strategy and focusing resources. While there has been a major effort to develop a national strategy, we are concerned about a lack of accountability and the potential proliferation of different strategies.

Foreign countries also face terrorist threats and have to develop programs and prioritize resources to combat terrorism. In our April 2000 report to this Subcommittee, we discuss how five foreign countries are organized to combat terrorism, including how they develop programs and direct resources.[2] Officials in the five countries we visited told us that because of limited resources, they make funding decisions for programs to combat terrorism on the basis of the likelihood of terrorist activity actually taking place, not the countries' overall vulnerability to terrorist attacks. For example, each country may be vulnerable to a CBRN attack, but officials believe that such attacks are unlikely for a variety of reasons, including the difficulties terrorists would face in producing and delivering these type of weapons. Due to resource constraints, these foreign officials said their countries maximize their existing capabilities to address a wide array of threats, including emerging threats like CBRN, before they create new capabilities or programs to respond to such attacks.

[2] *Combating Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism* (GAO/NSIAD-00-85, Apr. 7, 2000).

Background

Intelligence and law enforcement agencies continuously assess the foreign and domestic terrorist threats to the United States. To be considered a threat, a terrorist group must not only exist, but have the intention and capability to launch attacks.[3] The U.S. foreign intelligence community, which includes the Central Intelligence Agency (CIA), the Defense Intelligence Agency, and the State Department's Bureau of Intelligence and Research, monitors the foreign-origin terrorist threat to the United States. In addition, the Federal Bureau of Investigation (FBI) gathers intelligence and assesses the threat posed by domestic sources of terrorism. According to the U.S. intelligence community, conventional explosives and firearms continue to be the weapons of choice for terrorists. The intelligence community (both foreign and domestic agencies) reports an increased possibility that terrorists may use CBRN agents in the next decade.

Understanding the Nature of the Terrorist Threat

The first step in developing sound programs to combat terrorism is to develop a thorough assessment of the terrorist threat. In doing such an assessment, it is important to recognize that terrorists would face many difficulties using CBRN materials. To get a balanced view, policymakers need to understand the qualifications when they design programs to combat terrorism. Based upon our reading of the classified threat documents, such as national intelligence estimates, such qualifications include the fidelity and amount of credible intelligence, the terrorists' intentions versus their capabilities, whether the target is military or civilian, whether the target is international or domestic, and whether the enemy is a government or terrorists without foreign government sponsorship.

[3] Other factors to consider in analyzing threats include a terrorist group's history, targeting, and the security environment they operate in.

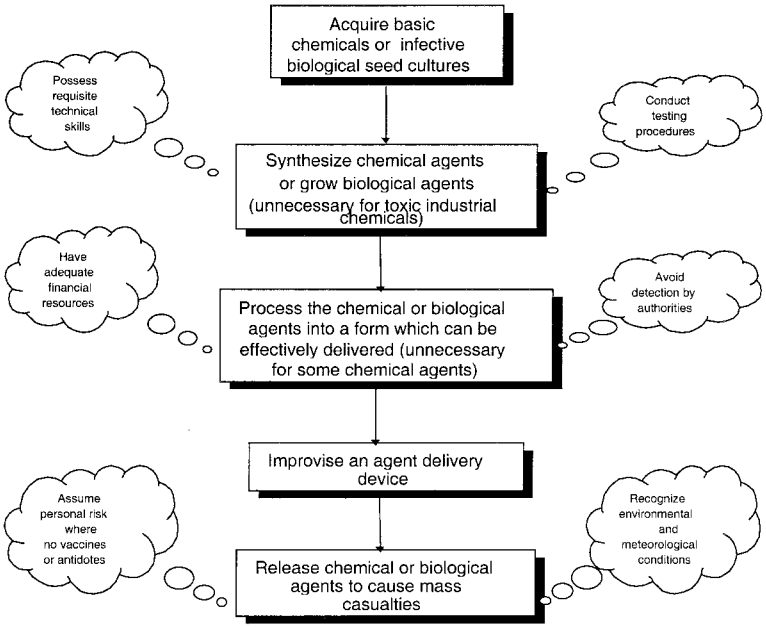
Terrorist Face Significant Challenges to Using Some CBRN Materials

Some past public statements by intelligence agencies do not include the challenges that terrorists would face in using CBRN materials. Moreover, in open testimony and public documents, the CIA has indicated that it was relatively easy for terrorists to produce and use CBRN agents.[4] Our work— which examined information from classified sources— showed that terrorists would have to overcome significant technical and operational challenges to successfully make and release chemical or biological agents of sufficient quality and quantity to kill or injure large numbers of people without substantial assistance from a foreign government sponsor.[5] In most cases, specialized knowledge is required in the manufacturing process and in improvising an effective delivery device for most chemical and nearly all biological agents that could be used in terrorist attacks. Moreover, some of the required components of chemical agents and highly infective strains of biological agents are difficult to obtain. Finally, terrorists may have to overcome other obstacles to successfully launch an attack that would result in mass casualties, such as unfavorable meteorological conditions and personal safety risks. Figure 1 summarizes stages and obstacles that terrorists would face in developing, producing, weaponizing, and disseminating chemical and biological materials.

[4] The Director of Central Intelligence made statements about terrorist interests in CBRN weapons without any mention of the challenges they would face in open testimony before the Senate Select Committee on Intelligence and other committees every year from 1996-2000. For example, CIA's June 1997 unclassified and published response to the Senate Select Committee on Intelligence stated that... "The relative ease with which some chemical, biological and radiological weapons can be acquired or produced in simple laboratories make them potentially attractive to terrorists. Delivery and dispersal techniques are also effective and relatively easy to develop."

[5] See *Combating Terrorism: Observations on the Threat of Chemical and Biological Terrorism* (GAO/T-NSIAD-00-50, Oct. 20, 1999, and *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks* (GAO/NSIAD-99-163, Sept 7, 1999).

Figure 1: Stages for Terrorists to Conduct Chemical and Biological Terrorism and Obstacles to Overcome



Source: GAO's analysis of technical data and discussions with chemical and biological warfare experts.

These types of qualifications are important because, without them, decision makers in both the executive or legislative branch, may get an exaggerated view of the terrorist threat, particularly as it relates to CBRN materials.

Need to Link Threats to Strategies and Resources

The second step in developing sound programs is to conduct a threat and risk assessment that can be used to develop a strategy and guide resource investments. We have seen some progress by the executive branch in conducting threat and risk assessments, developing a national strategy, and tracking resources. However, in all these areas additional work needs to be done.

Justice and FBI Are Making Some Progress on Threat and Risk Assessments

In prior reports, we have recommended that the federal government conduct multidisciplinary and analytically sound threat and risk assessments to define and prioritize requirements and properly focus programs and investments in combating terrorism.[6] Threat and risk assessments are decision-making support tools that are used to establish requirements and prioritize program investments. Without the benefits that a threat and risk assessment provides, some agencies have been relying on worst case scenarios to generate countermeasures or establish their programs. 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). 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 terrorist might use.[7] In our current work for this subcommittee, we are continuing to find that worst case scenarios are being used in planning efforts to develop programs and capabilities. For example, an interagency group led by the Federal Emergency Management Agency is using mass casualty scenarios, which appear at odds with intelligence threat data and the technical

[6] *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments* (GAO/NSIAD-98-74, Apr. 9, 1998) and *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks* (GAO/NSIAD-99-163, Sep. 7, 1999).

[7] *Combating Terrorism: Observations on Biological Terrorism and Public Health Initiatives* (GAO/T-NSIAD-99-112, Mar. 16, 1999).

obstacles that terrorists would face. These scenarios are being used to develop federal agency response teams to deploy to CBRN incidents.

The Department of Justice and the FBI have started to make progress in implementing our recommendations that threat and risk assessments be done at both the local and national level. 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.[8] 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. 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.

Justice Makes Mixed Progress in Developing a National Strategy

As we have previously testified, we believe there needs to be a federal or national strategy on combating terrorism that has a clear desired outcome. Such an outcome would provide a goal to be achieved and allow measurement of progress toward that goal. The Attorney General's 5-year interagency plan on counterterrorism and technology crime is the current document that most resembles such a national strategy. This plan

[8] *Fiscal Year 1999 State Domestic Preparedness Equipment Program, Assessment and Strategy Development Tool Kit*, May 15, 2000. This document was published by the Department of Justice's Office for State and Local Domestic Preparedness Support.

represents a substantial interagency effort to develop a national strategy for counterterrorism, but we have some concerns about the recent update to that plan. The updated plan has some improvements over the original plan— for example it provides more specificity as to which agencies will perform what tasks. However, in some ways the updated plan reduces the accountability of agencies in performing their mission to combat terrorism. For example, the updated plan does not include prioritization of actions, performance indicators, or timeframes that were included in the original plan. In addition, the plan still does not link its recommended actions to budget resources, although the original plan indicated that this would be addressed in updated versions. Finally, the updated plan still focuses on actions needed without citing a clear desired outcome that the nation is trying to achieve.

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. As you know, Chairman Shays has co-sponsored a bill (H.R. 4210) to set up a new office that would, among other things, coordinate a single integrated national strategy.[9]

OMB Tracks Resources to Combat Terrorism

Once threat and risks have been assessed and a strategy has been developed, agencies can focus programs and spending appropriately. We have previously testified on the increase in the

[9] For our comments on this proposed legislation, see *Combating Terrorism: Comments on Bill H.R. 4210 to Manage Selected Counterterrorist Programs* (GAO/T-NSIAD-00-172, May 4, 2000).

number of federal programs and the rapid increase in federal funding.[10] Proposed spending to combat terrorism, as requested in the President's fiscal year 2001 budget, is about $11.3 billion.[11] In earlier testimonies, we reported on Office of Management and Budget (OMB) efforts to track budgeting and spending by counterterrorist and CBRN programs. The OMB reports on governmentwide spending and budgeting to combat terrorism are a significant step toward improving the management and coordination of these complex and rapidly growing programs and activities. Through these reports, the executive branch and Congress have strategic oversight of the magnitude and direction of federal funding for this priority national security and law enforcement concern. According to OMB's most recent report (May 18, 2000), agencies have a new review process to compare programs across agency lines to help identify duplication and prioritize programs— which is required by law and has been lacking in OMB's earlier efforts to track spending. We have not done a detailed evaluation of this new OMB cross-agency review process, but we plan to do so in our ongoing work for this Subcommittee. We are still concerned that such efforts, in the absence of a national strategy with defined and measurable outcomes, could be used to justify higher budgets for all programs to combat terrorism rather than to establish governmentwide requirements and prioritize programs to focus resources.

An Illustration of How Threat and Risk Assessments May Be Useful

Several public and private sector organizations use threat and risk assessments to manage risks and identify and prioritize their security requirements.[12] Given the lack of a completed national level threat and risk assessment, we cannot point to any specific results at the national level. However, here are some hypothetical examples of how a threat and risk assessment could be used. If

[10] *Combating Terrorism: Observations on Federal Spending to Combat Terrorism* (GAO/T-NSIAD/GGD-99-107, Mar. 11, 1999) and *Combating Terrorism: Observations on Growth in Federal Programs* (GAO/T-NSIAD-99-181, June 9, 1999).

[11] According to OMB's May 2000 report, the $11.3 billion is divided into two broad categories: combating terrorism ($9.3 billion, which includes $1.6 billion directly related to weapons of mass destruction) and critical infrastructure protection ($2 billion).

[12] Detailed examples of how threat and risk assessments can be done, and how specific organizations have used them, appear in *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments* (GAO/NSIAD-98-74, Apr. 9, 1998).

the results of the analysis indicate that terrorists are most likely to use toxic industrial chemicals, the best investments could be to strengthen federal and state hazardous material response teams. If the results indicate a high likelihood of terrorists using biological agents, then the best investment could be to strengthen the public health infrastructure (e.g., surveillance system). If the results indicate that terrorists may target nuclear storage facilities, then the best investment could be to strengthen the physical security at federal and private nuclear facilities. On the other hand, if the analysis shows that conventional threats of bombing are the most likely threat against current vulnerabilities, then investments might best be focused on strengthening bomb squads at local police jurisdictions. We recognize that a national level threat and risk assessment will not be a panacea for all the problems we have reported about federal counterterrorism programs. However, we believe that such a threat and risk assessment could provide a strategic guide and force multidiscipline participation in planning, developing, and implementing programs to combat terrorism.

Foreign Countries Focus on Most Likely Threats and Leverage Existing Resources

Foreign countries that we have examined focused their resources against credible threats, not vulnerabilities. In addition, they leverage their existing resources, rather than create new capabilities, to respond to emerging threats like CBRN. In preparing our April 2000 report on how five foreign countries are organized to combat terrorism, we visited Canada, France, Germany, Israel, and the United Kingdom. We met with a broad array of national-level government officials whose organizations had a significant role in combating terrorism. During these discussions, we spoke with the foreign officials about how they analyzed threats and allocated resources for these programs.[13] While the officials we met with discussed resource levels in general, none of the five countries specifically tracked spending on programs to combat terrorism. Such spending was imbedded in other accounts for other areas such as law enforcement, intelligence, and defense. In addition, none of the five countries conducted formal threat and risk assessments of the type we have

[13] Since we did not have audit authority in the five countries, we relied on the cooperation of foreign officials to conduct our work and we usually did not have access to their internal documents. As a result, our report described how countries manage their programs, but did not independently evaluate the effectiveness of their efforts.

advocated for the federal government in our reports and testimony.

Countries Focus Resource Allocations on Credible Threats, Not Vulnerabilities

The five countries we reviewed receive terrorist threat information from their civilian and military intelligence services and foreign sources. Using various means, each of the countries' intelligence services continuously assess these threats to determine which ones are credible. That is, which potential threats could result in terrorist activity and require countermeasures, which ones may be less likely to occur but may emerge later, and which ones are unlikely to occur. Officials in all countries told us that because of limited resources, they make funding decisions for programs to combat terrorism based on the likelihood of terrorist activity actually taking place, not the countries' overall vulnerability to terrorist attack. For example, each of the countries may be vulnerable to a CBRN attack by terrorists, but officials believe that such attacks are unlikely to occur in the near future for a variety of reasons, including the current difficulty in producing and delivering these type of weapons.

Countries Leverage Existing Capabilities to Respond to Emerging Threats

For less likely but emerging threats, such as terrorists using CBRN materials, officials in the five countries told us that they generally try to maximize their existing capabilities for responding to such threats, rather than create new programs or capabilities. For example, the same capabilities used to respond to a fire, industrial explosion, or chemical spill would be leveraged for a terrorist incident involving CBRN weapons. In addition, officials in each country said that additional capabilities from neighboring states, provinces, cities, or national governments could be used by local authorities if the situation exceeded their capabilities.

Mr. Chairman, that concludes my prepared statement. I would be happy to answer any questions at this time.

GAO Contacts and Staff Acknowledgments

For future contacts about this testimony, please contact Norman J. Rabkin, Director for National Security Preparedness Issues, National Security and International Affairs Division at (202) 512-5140. Individuals making key contributions to this testimony include Stephen L. Caldwell, Lorelei St. James, Deborah Colantonio, and Richard McGeary.

Related GAO Products

Combating Terrorism: Action Taken But Considerable Risks Remain For Forces Overseas (GAO/NSIAD-00-181, July 19, 2000).

Combating Terrorism: Comments on Bill H.R. 4210 to Manage Selected Counterterrorist Programs (GAO/T-NSIAD-00-172, May 4, 2000).

Combating Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism (GAO/NSIAD-00-85, Apr. 7, 2000).

Combating Terrorism: Issues in Managing Counterterrorist Programs (GAO/T-NSIAD-00-145, Apr. 6, 2000).

Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training (GAO/NSIAD-00-64, Mar. 21, 2000).

Combating Terrorism: Chemical and Biological Medical Supplies Are Poorly Managed (GAO/T-HEHS/AIMD-00-59, Mar. 8, 2000).

Combating Terrorism: Chemical and Biological Medical Supplies are Poorly Managed (GAO/HEHS/AIMD-00-36, Oct. 29, 1999).

Combating Terrorism: Observations on the Threat of Chemical and Biological Terrorism (GAO/T-NSIAD-00-50, Oct. 20, 1999).

Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attack (GAO/NSIAD-99-163, Sept. 7, 1999).

Combating Terrorism: Analysis of Federal Counterterrorist Exercises (GAO/NSIAD-99-157BR, June 25, 1999).

Combating Terrorism: Use of National Guard Response Teams is Unclear (GAO/T-NSIAD-99-184, June 23, 1999).

Combating Terrorism: Observations on Growth in Federal Programs (GAO/T-NSIAD-99-181, June 9, 1999).

Combating Terrorism: Analysis of Potential Emergency Response Equipment and Sustainment Costs (GAO/NSIAD-99-151, June 9, 1999).

Combating Terrorism: Use of National Guard Response Teams Is Unclear (GAO/NSIAD-99-110, May 21, 1999).

Combating Terrorism: Issues to Be Resolved to Improve Counterterrorist Operations (GAO/NSIAD-99-135, May 13, 1999).

Related GAO Products

Combating Terrorism: Observations on Biological Terrorism and Public Health Initiatives (GAO/T-NSIAD-99-112, Mar. 16, 1999).

Combating Terrorism: Observations on Federal Spending to Combat Terrorism (GAO/T-NSIAD/GGD-99-107, Mar. 11, 1999).

Combating Terrorism: FBI's Use of Federal Funds for Counterterrorism-Related Activities (FYs 1995-98) (GAO/GGD-99-7, Nov. 20, 1998).

Combating Terrorism: Opportunities to Improve Domestic Preparedness Program Focus and Efficiency (GAO/NSIAD-99-3, Nov. 12, 1998).

Combating Terrorism: Observations on the Nunn-Lugar-Domenici Domestic Preparedness Program (GAO/T-NSIAD-99-16, Oct. 2, 1998).

Combating Terrorism: Observations on Crosscutting Issues (GAO/T-NSIAD-98-164, Apr. 23, 1998).

Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments (GAO/NSIAD-98-74, Apr. 9, 1998).

Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination (GAO/NSIAD-98-39, Dec. 1, 1997).

Combating Terrorism: Efforts to Protect U.S. Forces in Turkey and the Middle East (GAO-T-NSIAD-98-44, Oct. 28, 1997).

Combating Terrorism: Federal Agencies' Efforts to Implement National Policy and Strategy (GAO/NSIAD-97-254, Sept. 26, 1997).

Combating Terrorism: Status of DOD Efforts to Protect Its Forces Overseas (GAO/NSIAD-97-207, July 21, 1997).

(702086)

Ordering

Orders by Internet

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal

Contact one:

Web site: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

1-800-424-5454 (automated answering system)

Mr. SHAYS. Mr. Perl.

Mr. PERL. Thank you, Mr. Chairman. Threat assessment is integrally linked to dramatic changes taking place in the global economy and the technology infrastructure. These changes may influence and affect terrorist goals, tactics, organizations and weaponry. As the United States grows stronger economically, militarily and politically, our enemies may be even more tempted to attack our Nation with asymmetric weaponry. The evolving threat raises important questions regarding the structure, organization, preparedness and ability of governments to respond to a threat that has been characterized as more difficult, diffuse, and dangerous. We must ask ourselves, does the way we look at the problem reflect the real world? The global economy is bringing together deregulation, trends toward deregulation, open borders and enhanced movement of people, goods and services. We are witnessing the spread of democracy, the spread of capitalism and free trade and global access to information and new technologies. These trends provide opportunities for the terrorist as well. This globalization facilitates the ability of individual terrorist and terrorist groups to operate in a relatively unregulated environment, and the development of the world economy and modern communication systems have made it possible for small groups and even private individuals to fund terrorism at a level available previously only to States. Today, many of the advantages historically available to counterterrorism forces, even those with large resources, are potentially neutralized by instantaneous secure communications available to the terrorist through Internet and other technologies.

Many believe that terrorism is increasingly assuming a national security dimension. On the other hand, what some have characterized as a new and growing opportunistic relationship between terrorism and organized crime could well result in an increased role for law enforcement and terrorist threat assessment. A growing concern is that when faced with a growing number of anonymous terrorist acts, authorities may be unable to quickly and definitively assign responsibility, therefore, neutralizing the effectiveness of any potential deterrent action. Another concern is what are the unintended consequences of our counterterrorism assumptions and policies. By hardening military targets and Embassies overseas, U.S. commercial sites or residential sites may become more likely targets.

Today, simply by implied threats, terrorists can cause the expenditure of hundreds of millions of dollars by governments, but on the other hand, ignoring threats by groups that have engaged in terrorism in the past is generally not thought to be an acceptable policy option. A major challenge facing us is not to lose the creativity, spontaneity and boldness of individual agency threat assessments in the dynamics of the interagency process; but on the other hand, in the interagency process, relative data and relevant data is reviewed and exchanged and working relationships among personnel are strengthened and improved. Some experts have looked to the drug czar model in seeking to reform government structures to deal with terrorism. And increasingly, terrorist organizations are looking to the drug trade for a source of funding.

The Office of National Drug Control Policy, we have heard a lot about it today, is unique in the Federal bureaucracy and emerging international and domestic responsibilities and in providing policy direction to operations through the budget process. A strong director with a strong personality and strong backing from a President has been said to command the respect of a 500-pound gorilla in the interagency community.

Others, however, suggest that the effectiveness of the drug czar's office in bringing together the diverse elements of the interagency community is mixed at best. A substantial challenge lies ahead for the counterterrorism community. A concept may be increasingly gaining ground to limit the presence of U.S. personnel at Embassies overseas.

Critical to threat assessment is the need to get smarter, not just protecting against from threats from outsiders, but smarter about threats posed by people with legitimate access. This includes acts of carelessness by insiders. A chain is only as strong as its weakest link. The need to continue efforts to enhance our vigilance, to minimize potential threats posed by outsiders working at Embassies and military installations overseas is strong.

Critical to threat assessment is a better understanding of the countries and cultures where foreign terrorists are bred and operate. Some experts have suggested including know your money in agency's budgets. This and the establishment of an interagency counterterrorism reserve contingency fund may warrant consideration. However, other experts are concerned about lack of accountability such a fund may offer and the fact that money may be spent for purposes other than intended. One of the most important challenges facing the counterterrorism community is to ensure that our antiterrorism efforts are fully coordinated. The Oklahoma City bombing and other events have demonstrated that terrorism is not limited to those areas where we are prepared for it.

The challenges facing us in assessing threats, allocating resources, and ensuring an effective congressional role in counterterrorism policy are complex. But inherent in challenges are opportunities to bring together the diverse elements of the counterterrorism community. Thank you.

Mr. SHAYS. Thank you, Mr. Perl.

[The prepared statement of Mr. Perl follows:]

Perl

Terrorism: Threat Assessment in a Changing Global Environment
Statement of Raphael Perl, Specialist in International Affairs, Congressional Research Service, before the House Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations, July 26, 2000.

Mr. Chairman and Members of the Subcommittee.

In my capacity as a specialist at the Congressional Research Service [CRS], I welcome the opportunity to appear here today to address the issue of Combating Terrorism: Assessing Threats, Risk Management, and Establishing Priorities.

Introduction

Terrorism threat assessment is integrally linked to dramatic changes taking place in the global economy and its technology infrastructure. These changes may directly influence and effect terrorist goals, tactics, organizations and weaponry. As the United States grows stronger, economically, politically, and militarily, our enemies may be tempted even more to attack our nation with asymmetric weaponry.

The evolving threat raises important issues regarding the structure, organization, preparedness and ability of governments to respond effectively to threats which have been characterized by some as more dangerous, diffuse, and difficult to prevent. Central to policy formulation and implementation are issues of centralization of leadership–centralization of the threat assessment process, centralization and coordination of policy planning, coordination and implementation, and accountability to Congress. Coordination of counterterrorism efforts also involves non-conventional and preemptive activities within existing policy constraints.

The way the government deals with issues, defines problems, and is structurally organized to deal with them, can have a strong impact on threat assessment, policy planning and implementation, and allocation of resources. Structures and mindsets that have been successful in one time period in history may be less successful in others. We must ask ourselves– does the way we look at the problem reflect the realities of today's world?

There is no universally accepted interagency definition of terrorism in law. Terrorism is defined in law differently in different contexts. To some degree governments have established an artificial compartmentalized way of looking at terrorism as a phenomenon distinct and separate in and of itself. There was much to be said for this in past years, but perhaps, in today's rapidly changing, more fluid and interconnected environment, our approaches should be reexamined. What some have characterized as a new and growing opportunistic relationship between terrorism and organized crime could well result in an increased role of law enforcement in terrorist threat assessment and a need for readjustment of concepts, responsibilities and capabilities, and methodologies. A central characteristic used to distinguish terrorism from common crime is the willingness of terrorists to go after often random innocent targets without limit for some greater cause.

It may well be that a trend is emerging where the magnitude of the threat and "pain" factor of the act, and not the motivation behind it, defines terrorism as a practical matter. The greater damage or trauma an act or threat can cause– the greater the level of shock, panic and fear it can instill– the more likely it may be viewed by the public and in the policy community as terrorism.

Many have argued the need to better prioritize, focus, and target resources for combatting terrorism. In this regard, the recently released report of the congressionally mandated National Commission on Terrorism recommends that: "The President and Congress should reform the system for reviewing and funding departmental counterterrorism programs to ensure that the activities and programs of various agencies are part of a comprehensive plan." The Commission recommends that: "The executive branch official responsible for coordinating counterterrorism efforts across the government should be given a stronger hand in the budget process." The Commission recommends as well that "Congress should develop mechanisms for a comprehensive review of the President's counterterrorism policy and budget."

My remarks are divided into five parts. First, I review developments taking place in the global environment which impact on terrorist activity and the government's response. *Second,* I will discuss emerging threats. *Third,* I will describe how the federal government is structured to respond to the threat of terrorism. *Fourth,* I will look at the "drug czar" policy coordinating model which some have suggested may have features transferable from the counterdrug arena to the counterterrorism arena. I will then discuss some challenges facing the counterterrorism community.

Globalization's Impact on Terrorist Operations and Government Responses.

In the United States addressing terrorist threats and government responses often involves tension between–or balancing of –civil liberties and effective detection of, and response to terrorist threats or acts.

At the beginning of the twenty-first century, ancient hatreds and modern hostilities that were submerged or frozen during the cold war are asserting themselves. Volatile areas include the former Soviet Union, the Balkans, Afghanistan, and the Middle East. One force in particular, radical Islamist movements, is of rising concern as a source spawning terrorist groups. In an expanding information age, information about weapons and tactics becomes widely available to terrorists.

The world is changing in other ways, too. The global economy is bringing trends towards deregulation, open borders, and enhanced movement of people, goods, and services. We are witnessing the spread of (1) democracy; (2) capitalism and free trade; and (3) global access to information and new technologies. This globalization facilitates the ability of individual terrorists, terrorist groups, and support networks to operate in a relatively unregulated environment. The development of the world economy and modern communications systems have made it possible for small groups and even private individuals to fund terrorism at a level possible previously only to states.

Today's terrorism does not constitute military power. Terrorism is assessed as posing only a small direct threat to our national survival, but its impact over time on U.S. foreign policy interests and U.S. national security may be far greater. Domestically, successful terrorist acts could erode the public's faith in the government's ability to provide a fundamental service: security and protection for its citizens.

In formulating threat assessments, experts look beyond the immediate impacts of such tragedies as the World Trade Center, Oklahoma City, and U.S. Embassy bombings in East Africa to how terrorism and the threat of terrorism affects our actions in the longer run. International terrorists seek to undermine what the

renowned military strategist, Clausewitz, called our "center of gravity." In this case, our national will to stay committed in world affairs.

To some degree other societies, such as Israel, Ireland, Peru and Colombia, have learned to live with casualties from terrorism. But each society decides for itself. For example, we in the United States have also learned to live with violence and casualties in some contexts. In 1998 we had more than 41,000 deaths nationwide ascribed to traffic accidents and more than 17,000 murders. In other instances, even a small number of casualties can have major policy consequences. For example, when 18 U.S. Army rangers in Somalia were killed, we pulled out, creating what some critics see as a poor precedent and a damaging image for U.S. foreign policy.

An important question is: to what degree does terrorism undermine our will, or ability to be an active leader in international affairs? The fact is that in the post cold war era U.S. national interests in a region may not be crystal clear. Thus, public support for U.S. engagement may be weak. Our participation in international coalitions is particularly controversial and force protection is an integral component of mission success. A case in point is the U.S. peacekeeping presence in Lebanon during the 1980's which was withdrawn after terrorists blew up the U.S. marine barracks there.

Our policy makers now face a dilemma. Some national leaders make the case that the acceptable level of terrorism against the United States is zero. However, as a practical matter, we cannot be strong everywhere, and the determined terrorist will always have some opportunity to create a newsworthy incident.

The availability of weapons and weapons delivery systems has historically had a profound impact on the political, social and physical structure of societies. Today we see dramatic changes in potentially available highly destructive weapons systems. Speed and coordination of operations are essential to both terrorists and counterterrorist organizations. Many of the advantages historically available to counterterrorist forces–even those with large resources– are potentially neutralized by instantaneous secure communications available to terrorists through the internet and other technology.

Although the response to terrorism will always have a strong and growing law enforcement component, many believe that terrorism is increasingly assuming a national security dimension. Some argue that never before in history has information and technology to harm so many been so readily available worldwide. They see as unprecedented the challenge to defend against deadly weapons systems and discover those responsible for their use. Never before has the threat been so diffuse and difficult to define, manage, and contain, they argue. Others see this concern as highly exaggerated. They argue against the practicality of committing substantial resources to defend against "speculative," "low probability" threats, even should the negative consequences of any such successful terrorist acts be high.

Terrorist Threat Is Changing as Is Our Perception of It

Insurgency and limited guerilla warfare were threats that characterized the cold war environment. Terrorism may become a major threat that characterizes the post cold war environment. Terrorism is a threat that many believe we are likely to see more-- and not less-- of. And as we move into the twenty-first century, the terrorist has better weapons against a more vulnerable world.

A number of assumptions, right or wrong, appear to underlie community thinking on threat assessment. Included are, *first,* that threat assessment must focus more immediately on non-state actors as this is where the real threat currently emanates. *Second,* that the near-term potential for use of weapons of mass destruction by such groups or individuals is low, but, if employed, chemical weapons would be a likely choice of agents; and *third,* that if biological agents are employed, they are likely to be employed against humans --not agricultural crops or livestock--and to be deadly agents (e.g., anthrax) and not agents designed to wear down a nation or to test delivery/dissemination systems (e.g., flu).

A growing concern is that, in the wake of a growing number of future anonymous terrorist acts, authorities may be unable to quickly and definitively assign responsibility, thereby neutralizing any deterrent effect prosecution or military retaliation or economic sanctions may hold. Another concern is that terrorists, through cybertechnology, will at some point attempt to damage U.S. critical infrastructure. Many analysts worry that that the magnitude of catastrophic terrorism could reach a degree where a lead military role would be required necessitating the need for advance planning for contingencies where targets may be hard to anticipate.

Another area worthy of further exploration is what are the unintended consequences of our counterterrorism assumptions and policies. By hardening military targets and embassies overseas, will U.S. commercial sites or residential sites become more likely targets; by telling terrorists who thus far have been using bombs and bullets, that we expect catastrophic terrorism by exotic agents, are we encouraging such activity; and by telling states that we see the threat shifting to non-state sponsors–could we be encouraging clandestine state- sponsored activity?

For half a century, the U.S. perceived the threat of terrorism first and foremost as an overseas issue. Today, this appears to be changing especially with incidents such as the bombing of the World Trade Center in New York.

For a third of a century, we were able to link international terrorism to sponsorship of specific groups by foreign nations. Today, we see a new breed of terrorist: one who does not work for any established organization and who is not known to be an agent of any particular state sponsor.

In the past, terrorism was viewed as politically motivated. Today, religious, ethnic, and national motivations and beliefs, not subject to compromise or negotiation, form the basis of an increasing number of terrorist acts against U.S. personnel, property, and interests. In the future, we may also see more instances of economically motivated terrorism--so called "terrorism for profit".

Traditionally, terrorism has been seen as physical violence, causing death, destruction and fear by guns and bombs. In the future, additional, more-sophisticated forms of destruction such as computer virus system sabotage and extortion are possible.

Traditionally, the immediate aim of terrorist acts was often to gain publicity for the terrorist's cause. Terrorists were quick to claim public responsibility. Today, more terrorists seek to remain anonymous. Inflicting pain on the "enemy" seems often to be the terrorists' goal, rather than drawing publicity to a cause.

Also, traditionally, the terrorist relied on elementary weapons and explosives technology, causing relatively small-scale destruction. Today, some see access by terrorist groups to advanced explosives technology, and access to chemical,

biological, and possibly even nuclear technology that could raise casualty levels substantially as a real possibility.

Today, simply by implied threats, terrorists can cause the expenditure of hundreds of million dollars by governments. On the other hand, ignoring threats by groups that have engaged in terrorism is generally thought not to be an acceptable policy option.

Federal Counterterrorism Response Structures

The federal counterterrorism response structure has been well documented by the General Accounting Office [GAO] in its September 1997 study on Federal Agencies Efforts to Implement National Policy and Strategy and by CRS, among other places, in its internal electronic web page briefing book for Congress.

In brief: The chain of command on anti-terrorism planning runs from the President through the National Security Council (NSC), a representative of which chairs a senior interagency Terrorism Security Group (TSG). The State Department is designated the lead agency for countering terrorism overseas; the Justice Department's Federal Bureau of Investigation (FBI) is the lead agency for domestic terrorism; and the Federal Aviation Administration is the lead for hijackings when a plane's doors are closed. These roles were reaffirmed by Presidential Decision Directive (PDD) No. 39 in June 1995. PDD 62 (Protection Against Unconventional Threats) and PDD 63 (Critical Infrastructure Protection) of May 22, 1998: (1) established within the NSC a National Coordinator for Security, Infrastructure Protection, and Counterterrorism who also provides "advice" regarding the counterterrorism budget; (2) established within the NSC two Senior Directors who report to the National Coordinator--one for infrastructure protection and one for counterterrorism; (3) established a new inter-agency working group primarily focused on domestic preparedness for weapons of mass destruction (WMD) incidents; and (4) laid out the architecture for critical infrastructure protection. Intelligence information is coordinated by an Intelligence Committee, chaired by a representative of the CIA.

An informal NSC chaired teleconference on threat assessment takes place usually twice a week at the Assistant Secretary level. Representatives from the Department of State, the FBI, and the CIA are regular participants. Interagency data exchange on threat advisories is accomplished by a data base and classified communications system linking key analysts in the intelligence community.

Looking at some foreign organizational models, at least six countries studied–Canada, France, Germany, India, Israel, and the United Kingdom–share common structural elements in their approach to terrorism.

These include: (1) centralization of decisionmaking (i.e., one lead ministry) with coordinating mechanisms; (2) guidelines for clear designation of agency in charge during a terrorist incident; (3) strategies with a strong intelligence component; and (4) executive branch oversight mechanisms. Resource allocations are targeted generally at likely threats rather than potential vulnerabilities and the trend is for nations generally to rely on existing capabilities, mechanisms, and programs rather than to create new ones.

Unlike the concept of jointness of command built into the U.S. national military establishment, the civilian side of the U.S. government functions more as a hierarchy of committees. Each agency has a clearly defined separate piece of the action and at the end of the day a final product is put together that works well. Efficiency,

however, may break down when interdisciplinary issues are involved and in today's global technological, information-age issues that were traditionally separated are increasingly intertwined.

In this regard, an important question arises: Is the executive branch properly structured to put together an integrated threat driven counterterrorism strategy? How best does one achieve desired levels of leadership, cooperation, coordination, and accountability? A major challenge facing those tasked with counterterrorism threat assessment and planning is not to lose the creativity, spontaneity, and boldness of individual agency threat assessments. Should domestic terrorism grow, the number of agency programs brought into the process to respond to the threat or its aftermath can be expected to grow as well, even further complicating efforts at strategy integration.

In the interagency process, critics argue that being a team player is a prized and encouraged value. Creative dissent is not. In the interagency process, they believe that negotiation, compromise, and a homogenized least common denominator rule. In the interagency process, the perspectives of a small agency with limited political clout may easily be overlooked. Many see the alternative as a more centralized approach. While potential shortfalls are also inherent in centralized power structures, internal structural obstacles to decisive action are generally not among them.

On the other hand, consensus is far from inherently a negative phenomenon. The interagency process for counterterrorism threat assessment and counterterrorism policy formulation has advantages. Whether accepted or not, all relevant data is reviewed and exchanged, working relationships among personnel are developed, appreciation and understanding of sister agency missions and viewpoints are enhanced, dissent to written products is allowed in the form of footnotes, mechanisms for higher level policy disputes resolution are in place, and in instances where the process is directed from the White House, prompt and strong decisionmaking is more readily implemented.

The "Drug Czar" Model

Some experts have looked to the "Drug Czar" model in seeking to reform government structures to fight terrorism. Counternarcotics efforts have forced local, state and federal agencies to build operable, cooperative, inter-agency relationships. The need to build and maximize similar relationships to deal with terrorism exists and some have suggested that the "drug czar" [White House Office of National Drug Control Policy (ONDCP)] model may have applicability to the counterterrorism arena. Legislation is currently before Congress on this issue [H.R. 4210].

Drugs and terrorism are both multifaceted and interdisciplinary issues. They cut across traditional bureaucratic and subject jurisdictions and structures. Both drugs and terrorism have strong national security and law enforcement components, they have military components, border control components, economic and trade components, medical components, and agricultural components. Today there are some 50 federal agencies with some degree of counterdrug responsibilities and at least 12 federal agencies with important counterterrorism responsibilities.

Drug trafficking and terrorism are illegal clandestine activities with strong national security and law enforcement threat components and operational similarities. Terrorists, like drug traffickers, need weapons and engage in violence to achieve goals. Terrorists, like drug traffickers, are often involved in hiding and laundering sources of funds. Both terrorists and drug traffickers operate transnationally and

often get logistical and operational support from local ethnic satellite communities. Both groups often rely on the criminal community for support: they may need smuggled weapons, forged documents and safe houses to operate effectively. Finally, both groups need a steady cash flow to operate. In the case of terrorists, where state sources of funding are rapidly diminishing, drug trafficking is an attractive funding option. Increasingly, terrorist organizations are looking to criminal activity and specifically the drug trade as a source of funding. The FARC in Colombia are but one of many cases in point.

Differences exist, however, between drugs and terrorism. The drug trade has a strong demand component. In contrast, there is no addiction-based international demand for terrorism. Profit drives the drug trade. Terrorists do need money to operate, but for the terrorist, funding generally is a means to an end and not an end in itself. Political ideology, radical religious viewpoints, alienation, or revenge, and not a desire for financial profit, usually drive terrorist activity.

The Office of National Drug Control Policy, the so-called "drug czar's" office, is a coordinating office in the Executive Office of the President established by Congress in 1988 by P.L. 100-690. The office is charged with: (1) establishing policies, objectives, and priorities for the national drug control program; (2) promulgating a National Drug Control Strategy; (3) coordinating agency implementation of the strategy; and (4) developing [with the advice of the program managers of agencies] a consolidated national drug control budget proposal to implement the strategy which shall be transmitted to the President and Congress.

The Office is unique in the federal bureaucracy in its merging of international and domestic responsibilities in bringing together the law enforcement, intelligence, foreign policy/national security policy, and domestic health communities–all of which are components of the counterterrorism community as well. Although the office is a policy office without an operational mandate, it does provide policy direction to operations. This is accomplished through the budget process in the form of planning guidance and recommendations on how to prepare for existing and emerging threats. By exercising its budget process review role, ONDCP performs budgetary integration of the operational aspect of interdiction activities of such agencies as the Coast Guard, the Customs Service, and the Departments of Defense and State.

The Director of the Office, though not a formal statutory voting member of the NSC, as the President's key drug policy adviser, is the principal adviser to the NSC on national drug control policy [E.O. 12280]. The Director also chairs an interagency working group (IWG) on international counternarcotics policy charged with ensuring development and coordination of such policy. Other agencies are required by law to provide ONDCP, upon the request of the Director, with such information as may be required for drug control and the Director of Central Intelligence is specifically required by law to render full assistance and support to ONDCP.

The Director's budget certification power–although often unpopular with individual agencies–wields considerable clout in terms of policy input and integration. In preparing the National Strategy, ONDCP staff, in consultation with agency personnel who are often detailed to ONDCP, define the mission and the threat in terms of needs, goals and objectives. Targets and measures of effectiveness [MOE's] are established. ONDCP annually provides agencies with policy initiatives which reflect the goals and objectives of the strategy which are presumably threat driven and which ONDCP would like to see reflected in agency budgetary priorities. Agencies respond with individual budget packages which the Director may certify as adequate to

accomplish the strategy's goals and objectives. If certified, the budget goes to the President. If decertified, the agency resubmits to ONDCP. The process for resolution of disagreements usually involves OMB, the White House Chief of Staff, and the Director. If not resolved, a meeting with the President, the Agency Head, an OMB representative, and the Director is scheduled. Reportedly, the last five meetings of this nature have been resolved in favor of ONDCP's position.

Supporters of strong drug czar concept find favor in the current structure in that it permits the Director to serves as both a national and international Administration spokesperson on drug policy issues. From the congressional viewpoint, an attractive component of the drug czar model is accountability to Congress. Unlike the current counter terrorism policy/leadership structure under NSC direction, the Drug Czar is confirmed by Congress and testifies regularly before congressional committees. Moreover, when Congress reauthorized ONDCP in 1988, it enacted specific targets that the drug strategy was required to meet. Congress could consider setting targets for counterrorism policy if it deemed this an effective approach. For those who favor a centralized coordination/control drug policy model, the Drug Czar's budget certification authority, an authority not shared by NSC staff, is seen as a favorable asset. A Director with a strong personality and strong backing from a President has been said to command the respect of a "500 pound gorilla" in the interagency community.

Others, however, suggest that the effectiveness of the drug czar's office in integrating the diverse and multifaceted federal counterdrug community has been mixed at best. Also, in a "czar" type structure, perhaps more so than in other bureaucratic structures, changes in leadership could significantly impair or enhance the effectiveness of a national leadership effort. Nevertheless, this area is one that might be further explored as Congress considers alternative approaches to dealing with terrorism.

Challenges for the Counterterrorism Policy Community

A substantial challenge lies ahead for the counterterrorism policy community. In past years, when terrorism was largely the product of direct state sponsorship, policymakers were able to diminish prospects for the United States becoming a target by exercising a credible deterrent on potential state sponsors. Today, however, many terrorist organizations and individuals appear to act independently from former and present state sponsors, thereby diluting our ability to deter them. On the other hand, without support structure implied by state support, this threat may be much less formidable.

There appears to be an increasing tendency to limit the presence of U.S. personnel overseas at a time when constraining the threat of terrorism may require a significant increase in overseas presence of law enforcement and intelligence assets.

Some have suggested that policy planners need to incorporate factors relating to the impact of terrorist incidents or campaigns, not only into the domestic policy equation, but also into the foreign and defense policy equation. Some view mechanisms such as the Defense Department's [DoD's] "bottom-up" review as providing possible vehicles for organizing, funding, and training for antiterrorism and counter-terrorism related missions. They believe that potential contributions from such institutions as our nation's nuclear weapons laboratories to terrorism threat analysis might be more fully explored.

A continuing need is seen to sustain a credible deterrent against potential state sponsors, but also important, appears to be the need to develop and sustain an

increasingly proactive deterrent against terrorist groups and individuals operating independently. Developing deterrents against independent groups may diminish the probability of use of weapons of mass destruction by terrorists and the potential for their use as a retaliatory measure by U.S. policymakers.

Other challenges facing the counterterrorism policy community include:

- how to strengthen intelligence & law enforcement relationships in a manner consistent with their respective missions.
- how to better share information and ways of combating terrorist groups in a timely fashion with other nations.
- and how to insure that the possibility of terrorist actions by groups and individuals is taken into account when we formulate our foreign, defense, and domestic policy planning.

To meet the evolving threats, experts recommend programs to develop:

- inexpensive, simple, effective, chemical, biological and explosives weapons detectors.
- an antiterrorism curriculum for law enforcement, security, and emergency response community personnel that can be taught on a national basis.
- more effective computer security systems.

Critical to threat assessment is the need for abundant, timely and useable intelligence, about potential terrorist sponsors, perpetrators, activities and targets, as well as intelligence to help develop our own targets to deter or punish state sponsors. In this regard, the development of long term human source intelligence [HUMINT] is often cited as a vital component in building our ability to preempt attacks.

Critical to threat assessment is the need to get smarter, not just in protecting against the threat from outsiders, but smarter about the threat posed by people with legitimate access. This includes acts of carelessness by insiders. A chain is only as strong as its weakest link. We need to continue our efforts to enhance our vigilance to minimize any potential threats posed by third country nationals– for example, threats posed by outsiders working at U.S. embassies and military installations overseas.

Critical to threat assessment is a better understanding of the countries and cultures where foreign terrorists are bred and operate. This includes understanding the root causes of unrest that give rise to terrorism. It is important to understand such factors when we plan how to combat terrorist groups on an operational level. And it is important to understand such factors when planning to prevent or respond to specific terrorist attacks.

Threat assessment is an ongoing evolving process. As the threat changes, it may change slowly, but it may also change unexpectedly, radically, rapidly, and dramatically. To meet changing or unanticipated threats, strategies and missions may need to change, and allocation of resources may need to shift as well. Such circumstances require a certain fluidity of policy. Forward-looking planning, flexibility and periodic review thus become important policy components. A community mindset which encourages challenging of policy coupled with practical

exercises designed to test policy and policy assumptions may contribute to policy relevance. Some experts have suggested that designation of "no year" money in an agency's budget account and establishment of an interagency counterterrorism reserve contingency fund may be options which warrant consideration. Other experts are concerned over lack of accountability such a process may contain and the fact that money might be spent for purposes other than intended.

One of the most important challenges facing the counterterrorism policy community is to ensure that our anti-terrorism efforts are fully coordinated. When push comes to shove, agencies still do an awful lot of "ad hocing". The Oklahoma City bombing and other more recent events have demonstrated that terrorism is not limited to those areas where we are prepared for it.

As we move into the first decade of the new millennium, terrorism may receive increased attention in the foreign policy, national defense, and law enforcement communities. As we assess and formulate our international and national commitments, policymakers are likely to consider possible impacts of terrorism on those commitments and on public and political support vital to those commitments. The challenges facing us in assessing threats, allocating resources, and insuring an effective congressional role in counterterrorism policy are complex. But inherent in challenges are opportunities to bring together the diverse elements of the counterterrorism community to share information, experiences, ideas, and creative suggestions about how to effectively deal with this growing national security, law enforcement, and public policy concern.

Mr. SHAYS. When I get back, I am going to ask staff to ask questions. Unfortunately, I am not allowed to let them do it while I am not here. I am going to quickly vote and hustle back here. So we stand in recess.

[Recess.]

Mr. SHAYS. I will call this hearing to order and I would like to recognize the committee counsel, Mr. Halloran.

Mr. HALLORAN. Thank you.

Mr. Rabkin, I want to go through some parts of your written statement and get you to amplify a little bit. In discussing the limitations and technical challenges that terrorists might face in trying to use chemical or biological weapons and radiological weapons in particular, you said that they are not often in public statements. Do you find them included in internal discussions or internal documents?

Mr. RABKIN. A lot of the supporting documentation which is usually classified contains much more of a discussion of these reality factors. It is just in some public statements there is not much qualification given, just that these groups can make these weapons and are likely to use them.

Mr. HALLORAN. Is it your judgment that those limitations are realistically reflected in net threat assessments that are used, more realistic than in the public statements?

Mr. RABKIN. I am not in a position to say that they made a net assessment. The net intelligence estimates are a term of art that means certain things. My understanding is that most of these qualifications are reflected in those kinds of documents.

Mr. CALDWELL. I have one other thing that I want to add. Our statement says that some officials are not including these qualifications. In some public statements we have seen them. The head of the Defense Intelligence Agency before the Senate Intelligence Committee had some of these kinds of qualifiers in there, but we don't find them made in statements by DCI and others, and those hold the most overall weight when people are assessing the threat of chemical or biological terrorism.

Mr. HALLORAN. On page 6, you say that you have recently seen some progress in terms of assessing threat assessment? Can you amplify that a little more?

Mr. RABKIN. First, on a broad and macro level we recommended that the Justice Department, through the FBI, do a net intelligence estimate of the threat from chemical and biological terrorism domestically, domestic sources to complement an assessment that had been done by the CIA regarding that threat from foreign sources. The Justice Department has started the process for preparing that estimate.

Also, when we talk about risk assessments being done at a State and local level, the analytical basis for making these kinds of risk assessments, taking threats and understanding the vulnerabilities of the assets that are at risk, some of the countermeasures that are possible and weighing the costs against the threats, the structure for doing that has been—the Justice Department has prepared some materials that would be helpful to State and local governments and are providing those to the government, so at the State

and local levels, the risk assessments can be done and the funding decisions that come from them can be more analytically based.

Mr. HALLORAN. So using that tool, the Justice Department might prevent local risk assessments from being simply laundry lists of vulnerabilities?

Mr. RABKIN. That is the hope. Certainly, the structure is there. How it is being used remains to be seen. As a coordinator, the Justice Department can help State and local governments through the use of best practices and not have them reinvent the wheel. Here is a tool that can be used if they want to.

Mr. HALLORAN. The FBI testimony which is not classified, they gave us an unclassified version of it, describes or discusses your recommendations and says at one point that a net or a comprehensive threat assessment such as you recommend would be inherently too broad based to provide much value. Instead, the FBI have concentrated on providing more focused threat assessments for major special events. Do you agree with that?

Mr. RABKIN. I think there is room for both. What we are talking about provides broad oversight as to whether the threat is increasing, whether there are certain aspects of the threat that are becoming more pronounced than others and can make some of the more strategic decisions about the level of funding that Congress ought to be providing, where it is being directed, and whether there is adequate research and development being conducted, etc.

On a more operational or tactical level, the FBI is right, they have to remain up to date, not that these broader assessments cannot be routinely updated, but as a particular threat develops for a particular location or a particular event, I think that the FBI and other intelligence agencies, by focusing at that level, can deal with that issue. What we were talking about was much more strategic, and so therefore, I think there is room for both.

Mr. HALLORAN. Your statement says in your current work, you continue to find worst case scenarios are being used to develop planning capabilities, and one example in your statement was the selection of items for the pharmaceutical stockpiles. Can you give us some other examples where worst case scenarios are driving program planning?

Mr. CALDWELL. On the CBRN response teams, we have found that the Federal Emergency Management Agency has put together some scenarios to plan which teams and what size and how they would respond, which is using worst case scenarios, in terms of mass casualties and things that are not based, in our view, in terms of validated intelligence, nor the science behind the threat in terms of some of the difficulties, and whether this kind of attack would even be feasible. Again, those are potentially being used to decide which Federal teams need to be beefed up, and so potentially, where resources would be developed.

Mr. HALLORAN. Mr. Perl, in your statement, you talk about the drug czar model, and you gave two sides of a good argument. What might be inept about that model when tried to apply to the terrorism issue?

Mr. PERL. What might be inept in the way that the model currently exists would be the need for the office to get ongoing authorization from Congress. There are advantages from the viewpoint of

congressional control, but in terms of the respect and clout that you have in the interagency community, there is a concern that this particular institution outside the community might not be around in a few years, maybe we can simply wait it out. That would be one problem.

Another potential problem from the perspective you are asking me to portray would be the drug czar's office, and this is something good, but on the flip side, it could be a problem. The drug czar's office has a staff of 124 people plus some detailees. One of the things that one needs to consider in making these decisions is how much staff does one need. So, for example, the current structure in the NSC does not have 123 people working on terrorism.

Now, the size of the budget for the drug czar's office—for the drug war and the size for the terrorism war is relatively compatible in terms of numbers. There is not great differences in terms of resources being committed, and many different segments of the Federal community are involved and the State and local communities and international interaction. So lack of staffing can be a serious problem to the effectiveness of an office of that type.

At the same time, people in the drug czar's office would argue for more flexibility in staffing, that Congress currently on the appropriations process has put a limit of 124 people, and each additional full-time employee slot needs authorization from Congress. So from the perspective of people in an office of that type, they would like usually to have more flexibility. Of course, from the viewpoint of congressional oversight, this enables the Congress to control the size of the office and influences kind of its growth.

Mr. HALLORAN. Your work on foreign government or foreign approaches to this problem, did you find a more—in any instances, a more comprehensive order or unified threat assessment process than you found here?

Mr. RABKIN. The answer is no.

Mr. CALDWELL. The answer is no. I think when we talked to countries about how they came up with their decisions in terms of leveraging existing resources rather than creating new programs and capabilities, some of that process might have gone into their decisions on other areas. For example, they make decisions that they had robust disaster management assets in place or robust hazardous materials, emergency response capabilities, and perhaps because they had already made those types of investments, they decided that those were the ones that they would then leverage to deal with the terrorist involving chemical or biological materials.

Mr. HALLORAN. Thank you.

Mr. SHAYS. Thank you. We are joined by Mr. Blagojevich, but I would like counsel to ask questions on this side. David Rapallo has some questions.

Mr. RAPALLO. Mr. Rabkin, on the importance of a threat and risk assessment, it is comprehensive and includes threats to national, international and military resources. Is it your position that any prioritization or any attempt by the administration to put programs in order based on the funding levels is flawed without this type of assessment?

Mr. RABKIN. I wouldn't say that it is flawed, but I think it could benefit any decisionmaking process on where additional dollars are

going or would help—would be helped by having this kind of an assessment. It would also be helpful over time, as threat changed or as the overall risk threat level changed, it would be helpful in identifying whether the funding level needed to change accordingly.

Mr. RAPALLO. Would any proposed change that the administration suggests not be as comprehensive?

Mr. RABKIN. I would say until we have a comprehensive assessment which would better guide, and until we have a national strategy in place that would better guide some of these resource decisions, I don't think that it is wise just to suspend making those decisions. The government has to do what it feels best, the agencies are in a position, although it may not be well coordinated and focused on a commonly accepted goal, but at least they are moving forward in some fashion. I don't think that it would be responsible just to stop that and wait until we got a strategy, a plan, or better assessment.

Mr. RAPALLO. One of the later panelists has in his written testimony a quote by CIA Director George Tenet before the Senate, saying chemical and biological weapons pose arguably the most daunting challenge for intelligence collections and analysis. There are and will remain significant gaps in our knowledge. As I have said before, Tenet said before, there is continued and growing risk of surprise.

I am wondering is a comprehensive threat and risk analysis with threats to national, international and military targets even possible? And if it is, would that lose too much detail to be useful?

Mr. RABKIN. I think it becomes a question of defining how much detail is going to be in it, but I think it would be possible. It would seem to me to be a compilation of what is known about that threat that Mr. Tenet was talking about. That kind of information is very helpful in making this kind of an analysis and assessment.

As they fill in the gaps, as they get more—as the intelligence community gets and analyzes more information about this and learns more about it, they can use that for the assessment to better direct the efforts and resources of the rest of the executive branch.

Mr. RAPALLO. Mr. Perl, do you have any thoughts on this that you would like to add?

Mr. PERL. No.

Mr. RAPALLO. One thing that we don't complete a threat and risk assessment for is to identify duplication. Do you see any duplicative efforts as far as intelligence gathering and that sort of thing related to what we heard this morning?

Mr. RABKIN. I don't have any evidence of duplication. We have not looked at whether the intelligence community is duplicating efforts in their data gathering and analysis activities. We have noted duplication in other areas, first responder training, for example, and have reported to this committee on that. But not on the intelligence side.

Mr. PERL. You previous question on whether I have any thoughts, that is, on the previous panels this morning, the issue of the need for flexibility was raised. The variability of the threat, the changing nature of it and the need for flexibility in our response. And one of the concerns is that if one does long-term planning, there will always be a certain amount of disconnect between real

immediate threats and the long-term planning. So whatever the process is, there has to be—it would be important to build in a process of periodic review and some flexibility in the way funds can be shifted.

Mr. RAPALLO. You don't think that exists with the working groups within the NSC structure?

Mr. PERL. Budget cycles tends to be a little bit longer. The working groups have the ability to move things around, but now when there are shortfalls, what happens is that the process is usually, or hopefully from the agency perspective, made up by the supplemental appropriations process. To some degree, I am not suggesting that agencies wouldn't take actions in the national interest because they may not have the funding for it, but whenever agencies take actions, funding is a consideration.

Mr. RAPALLO. Thank you.

Mr. SHAYS. Gentlemen, I would like to just throw out one type of threat. Please tell me how it fits into the overall response to terrorism and that is, the military's determination that they need to immunize all military personnel with anthrax. Would a comprehensive sense of what our threat is get us to be able to put that in some focus?

Mr. RABKIN. The policy decision that Secretary Cohen made to require that all military personnel be immunized against anthrax was based on the military context, the likelihood that military troops would be involved in a situation where state enemies would use anthrax as a biological weapon. And that the only viable alternative, the only viable option for them to use was vaccination; that because of the detection period and the kind of time that takes place and the delay in recognizing symptoms, that that was the only solution.

The more information that DOD has about who has anthrax and who is in terms of state enemies and who is likely to use it provides more justification or more information upon which that policy can be reviewed. Similarly, other information about the safety and efficacy of the vaccine and the administration period, the troubles that the manufacturer is having providing an adequate supply of the vaccine, all of these bits of information that were not available when the original decision was made, can also be useful in revisiting the decision. So I think as most policy decisions, just about any policy decision, the more information you have, the more you can reflect on whether it is an appropriate decision and whether it needs revisiting.

Mr. SHAYS. Does anyone else want to respond before I followup?

Mr. PERL. I agree, basically it is a question of the probability and the reality of anthrax being employed, and this is a decision that the Secretary of Defense has made. I am not qualified to make that decision. But if it is a high probability, logically, it would seem that U.S. troops should be vaccinated because this is a very contagious disease.

Mr. SHAY. That is my followup. Is the vaccine a modern vaccine or a 1950's vaccine, and can we reproduce it to cover all of our troops. But it gets into that fact that we have civilians and to what extent should civilians who are in these theaters be vaccinated. I am just trying to get a sense of how a master focus on the threat,

a master plan focus on the threat, integrates the response that the military has to have and the whole argument that the military has to respond to it, that this is a biological agent that can be produced by a terrorist in those theaters. For instance, the State Department people, do we require State Department people to take this vaccine?

Mr. PERL. Not to my knowledge.

Mr. RABKIN. It is voluntary at the State Department.

Mr. SHAYS. I am trying to get a sense in your judgment of how we integrate what the military sees versus—and the threat to their own military personnel versus all other Americans.

Mr. RABKIN. If we talk about the model that the Department of Defense used to make the decision, they assess likelihood that the threat would be used, the consequences if it were used, they looked at alternatives, is there any alternative available that could be used other than a vaccine to allow the troops to survive such an attack and be effective, and the decision was made back in 1997, I think, based on information and assumptions at that time.

Mr. SHAYS. And they left out some very important aspects. They left out the aspect whether they should proceed with an older generation vaccine or develop a new one. They left out whether they should do a vaccine where they knew they could have supply, and the reason that I am asking is not to critique the Department of Defense, but to understand if a comprehensive threat analysis would lead us into the same mistake or whether we would have been spared the mistake the military has made. The military has made a mistake. They have approximately 1 month's supply to 6 months, depending on to what extent they use it.

I am asking, in your judgment, a comprehensive analysis of the need and a coordinated effort would have enabled us to, in responding to terrorism, come to a different response or to take into consideration things that the military left out?

Mr. RABKIN. I am not ready to agree that the military made a mistake when it passed the policy. There certainly have been problems in implementing the policy in terms of securing a continuous supply of the vaccine to be able to administer it as it was intended.

Mr. SHAYS. Let me ask you not to—I'm not trying to make a major point. You are not prepared to say that they made a mistake, because you don't have the knowledge, or that you have the knowledge but just don't know what the conclusion is. Is this something that you have any—do you have significant expertise on this issue?

Mr. RABKIN. GAO has done some work on this issue, both in terms of the safety and efficacy of the vaccine as well as the administration of the program, and I am speaking from that basis, the work that we have done.

We have not reached the conclusion, Mr. Chairman, that the Department of Defense made a mistake in adopting the policy that it did. We have reached conclusions about—there are unanswered questions about the safety and efficacy of the vaccine. There were improvements needed in education of the troops about the vaccine, about adverse reporting—reporting of adverse reactions to the vaccine, etc.

But in the context of the threat and risk assessment, I think that if you apply the model that we are talking about of a threat and

risk assessment and risk management to the specific issue of military troops facing a potential biological or anthrax threat in a combat situation, I can see how the decision was made. And that model was used and we may not agree with the way that the decision was made and the assumptions.

Mr. SHAYS. I guess my problem, in my judgment, after having countless hearings on this issue, whatever model they used, was a flawed model, in my judgment. I am not saying that GAO has made that determination. I just wanted to know if the model that we will use for the civilian world will be a bit different, and in response to terrorism, because they are running out and they may not get a supply for a year plus. They are having a facility produce this that has to be solely dedicated to produce this, because it is a 1950's vaccine, so they can't produce anything else in that plant or certainly that area than this 1950's vaccine. I get the sense of your response.

Mr. PERL. You raise a very interesting question. I am not an expert on chemical and biological warfare per se, but an important issue here is to what degree does military threat analysis input get factored into the health community's decision whether or not to issue vaccines nationwide.

Mr. SHAYS. Right. Or to what extent is there the likelihood that anthrax will be introduced into this country and what obligation do we have to deal with that in this country, and are we preparing for that?

Mr. RABKIN. That is the issue that I think the threat and risk assessment process and procedures would have to deal with. Take the information from the intelligence community about what is the risk to the United States, to the citizens of the United States for a terrorist attack using anthrax. If and when they get to the point that they feel that is an imminent, or enough of a potential that we need to do something about it, then we start considering alternatives and what is available. What are some of the countermeasures that are potential, and what are the costs and efficacy of those countermeasures and those policy decisions could be made. Maybe we need better technology.

Mr. SHAYS. Who would make that decision? I realized in the process of asking that question I don't know who would make that decision.

Mr. RABKIN. Under the legislation passed yesterday, it might be that council on domestic terrorism preparedness, because part of their responsibility would be to take information about the threat and to make risk assessments and to oversee some of the investment decisions that are being made, and it would have representation from the different communities, both the intelligence community, the health response community, the military community. So that might be an avenue for making that decision.

If you look back at swine flu, for example, and how decisions were made back in the 1970's on that issue, it is an interagency—information comes up from the agencies and decisions are made at the highest level in the executive and legislative branch.

Mr. SHAYS. The difference is, one was to respond to a natural threat versus one that would be responding to a terrorism threat, and it introduces some major policy decisions.

Let me ask you, is there anything that you would like to respond to that we didn't ask? Something that you prepared for that you think is important for us to know?

Mr. RABKIN. One of the issues that we wanted to get across was the need for a national strategy.

Mr. PERL. I think the committee has done a wonderful job in covering the issues.

Mr. SHAYS. We appreciate you for coming this morning and this afternoon.

Mr. RABKIN. Thank you for the opportunity to testify.

Mr. SHAYS. We will move now to the second panel. I call our second panel, Ambassador Paul Bremer, chairman, National Commission on Terrorism; former Ambassador at large for counterterrorism; and Mr. Michael Wermuth, RAND Corp., senior policy analyst; Mr. John Parachini, Monterey Institute of International Studies, executive director; and Mr. W. Seth Carus, National Defense University, senior research professor.

I am going to ask you to stand and I will swear you in.

[Witnesses sworn.]

Mr. SHAYS. Ambassador, go ahead.

STATEMENTS OF AMBASSADOR PAUL BREMER, CHAIRMAN, NATIONAL COMMISSION ON TERRORISM; MICHAEL WERMUTH, RAND CORP., SENIOR POLICY ANALYST; JOHN PARACHINI, MONTEREY INSTITUTE OF INTERNATIONAL STUDIES, EXECUTIVE DIRECTOR; AND W. SETH CARUS, NATIONAL DEFENSE UNIVERSITY, SENIOR RESEARCH PROFESSOR

Mr. BREMER. Thank you. The National Commission on Terrorism delivered its report to Congress and to the President on June 5. We addressed the threat as we saw it, among other things, and the main point that we made in that report was that the threat is changing and becoming more serious, and we paid particular attention to catastrophic terrorism.

I was asked to comment on three areas of interest to this committee: First, the development of threat assessments; second, the question of whether it would be valuable to have a national threat assessment; and then a few words on the budget process.

On the development of threat assessments, it is obvious that good intelligence is the very heart of an effective counterterrorism policy. You can't have a counterterrorism policy without good intelligence, particularly if you want to prevent attacks, and we focused on preventing attacks in our commission. The commission that Governor Gilmore chairs is looking at dealing with the consequences of attacks. We focused on prevention.

In no area is intelligence more difficult and more dangerous and important than terrorism. We examined the Federal Government's look at intelligence rather in depth, and we had two concerns, both of which related to the capability and independence of intelligence analysis.

The first one, Mr. Chairman, was the question of whether or not the creation of the counterterrorism center at the CIA in the mid 1980's by putting together people from both the DI side and the DO side of the agency would, in some way, impinge on the intelligence

side's ability to make objective analysis of the terrorist threat. There was a concern that by being, in effect, co-housed with the operations people, the intelligence people might become either overwhelmed by the tactical operational demands of the operations side of the counterterrorism center, or become, in effect, less pure in their intelligence outlook, that their actual analysis would become tainted in some way by being associated with the operations people.

The second concern we looked at was whether it was wise of the government to disestablish the National Intelligence Officer for Terrorism which was done in the early 1990's. And we were concerned——

Mr. SHAYS. Where did that office——

Mr. BREMER. That office was a member of the National Intelligence Council [NIC]. It was disestablished in 1991, but don't quote me on the year.

The concern there was that the issue would lose its place at the high table of the intelligence community, the NIC, and would we lose the capability, therefore, to conduct strategic level analyses of the terrorist threat?

The results of our study was that we believe that the counterterrorism center at CIA has, in effect, been successful at integrating the DI side of the House without impinging on its ability to conduct objective and useful intelligence analysis of the foreign threat.

In fact, they established a group within the counterterrorist center, which is dedicated solely to doing that, and until recently, that group was headed by a person from another agency, which gives it a good life and some independence.

On the question of the national intelligence officer, we talked to all of the consumers around town and found, in fact, that they were very satisfied with the outcome of the counterterrorism center at CIA and did not believe, which sort of surprise me, that we should reestablish a national terrorist officer. And so we did not recommend that in our commission. We believed that as long as the CTC core group can keep its independence, there is no reason to change the setup. We did make some recommendations relating to how we go about collecting intelligence aboard and which are somewhat beyond the area I was requested to talk about today.

Second, would there be value in having a national threat assessment, the question that you asked this morning and again this afternoon. We examined the FBI's handling of intelligence comparable to looking at the CIA's handling of intelligence abroad, and concluded that the FBI does a good job of disseminating threat warnings, immediate threat warnings when they are received. They get these out to the community quickly.

The FBI is less good on understanding and disseminating more general intelligence relating to the terrorist threat. Part of this is a cultural issue. The FBI is a law enforcement agency. Their job, they are trained to make cases, they are prosecutors and they want to be sure when they collect evidence as they call, intelligence, as you might otherwise call it, that they have a good chain of custody over that evidence and they don't, therefore, have an instinct to share it out.

We made recommendations here also related to the FBI establishing a cadre of officers who would, in fact, disseminate that intelligence.

We took note of the repeated suggestions by the GAO over the past few years that the Department of Justice produce an integrated national threat assessment. To my knowledge, this has not been done. I think, Mr. Chairman, that such a threat assessment could be useful in giving Congress a tool to evaluate whether the budgets for counterterrorism put forward by the Federal Government are well considered in light of the likely threats and not the vulnerabilities. And I recognize the difficulty of producing such a national assessment, and I know that the agencies have a preference for doing a sort of rolling assessment, as you heard this morning, rather than doing—it seems to me that it is not an either/or question. I think you basically have to do both. I don't think that there is a choice.

I think a national assessment would be good if it could be put together and give a view as to whether the GAO's model is the right model, but it should not be beyond the wit of man to figure out how to have a national assessment when, taking off my chairman's hat at the commission and speaking as a taxpayer, when I see a budget of $11 billion and rising, as your colleague used to say, we are getting into real money now. It seems to me that Congress has a legitimate question to know whether that money is being well spent.

On funding for counterterrorism, we did not have time, Mr. Chairman, to look deeply into that $11 billion budget. We did reach some conclusions about the individual budgets of CIA, FBI and NSA, which are in our report, but it did seem to us that the budget process at both ends of Pennsylvania Avenue is pretty flawed. In the executive branch the problem is that the national coordinator, and I don't know if this is going to be solved in this legislation that is before the House, the national coordinator lacks budget authority and political responsibility, and it seems to me whatever solution there is to the problem of coordinating a national strategy, it must be directed by somebody who is politically responsible, therefore nominated and approved with the advice and consent of the Senate and somebody who has real budget authority.

Down at this end of Pennsylvania Avenue, congressional oversight is fragmented among at least 12 committees in both Houses, so we recommended that both ends of Pennsylvania Avenue need to get more focused on this. Basically those are my opening remarks, Mr. Chairman.

Mr. SHAYS. Thank you.

Mr. Wermuth.

Mr. WERMUTH. Thank you, Mr. Chairman. I will also be brief, and I can probably be very brief by simply identifying myself with your opening remarks and passing to the next witness, and will likewise address threat assessments and the benefit of having an integrated threat assessment. I agree with Ambassador Bremer that the international piece works pretty well. We should be fairly comfortable that the process works well. You can argue and sometimes experts do argue with conclusions that are reached in some of those contexts, but the process is tested and proven and we can

have some comfort in that through the national intelligence estimate process that is conducted with the support of the CTC and the Central Intelligence Agency.

Currency perhaps is another question. Given the fluid and ambiguous nature of potential threats from terrorists, you may ask whether the process, perhaps, is too lengthy and too cumbersome to provide a level of currency as threats may change from time to time in the international context. And as we have heard already today, and as I am sure you heard in closed session this morning, I am certainly not as comfortable about how that process works on the domestic front.

The FBI has that responsibility. You have already heard that the FBI is taking some steps to fulfill that responsibility more effectively, but as Ambassador Bremer has mentioned and Mr. Rabkin mentioned, they have not gotten there yet. Likewise, in my written testimony, I used the term "cultural issue" in describing perhaps the FBI's full lack of understanding of how this process works. There are some collaborative efforts. I think it was probably mentioned in Mr. Turchie's unclassified testimony about how the FBI, at least, is swapping fairly senior people with the Central Intelligence Agency in an effort to learn more about good analytical processes, best practices, if you will, in trying to craft threat assessments that are relevant, that are comprehensive enough to be able to help lead some of the decisions, both in the executive branch and in the legislative branch, in terms of priorities and particularly for funding applications. But they are still not there yet, and I was, likewise, taken by the paragraph that your counsel mentioned in one of his questions earlier about the fact that the FBI doesn't believe that a broad threat assessment will be very useful.

I just happen to disagree with that and agree with Mr. Rabkin and Ambassador Bremer that you can have both. You can have a broader assessment that will help guide some of the broader priorities and resource decisions as well as having the more operational and tactically focused threat and warning pieces that would go along with that.

So we really don't have a fully integrated assessment yet, one that is seamless from the international into the domestic, recognizing that there are some restrictions and barriers about how you do all of that. But we really do need one, in my opinion, and we can do a better job of it, the government can do a better job of it, all of the agencies, and, in my view, do that without infringing on civil liberties, without being intrusive or overreaching where the agencies are concerned, and without violating the very clear restrictions on the foreign intelligence's community ability or restriction prohibitions on them from collecting intelligence domestically.

As to the Chair's question, is funding to combat terrorism being properly directed? I am afraid I have to answer that with a question. How can we tell? You have heard all of the witnesses say it so far. We don't have a national strategy. We don't even have a comprehensive Federal piece of a national strategy, and no amount of touting of Presidential decision directives or macro budget submission like came up here on May 18th, the Attorney General's 5-year plan, where I am not sure where that stands now, none of

that amounts to a national strategy. There is no good coordination mechanism. The NDPO, the National Domestic Preparedness Office, simply has not worked. It was probably misplaced in the first place, buried that far down in the structure of the FBI without the kind of political accountability and authority that they needed. There is no one in charge. Interagency working group meetings, endless meetings, is simply not sufficient, in my view, to resolve the problem.

I know, Mr. Chairman, that you have been frustrated before in hearings, including one that I attended on March 22nd, where you asked some senior Federal officials who is in charge, and you really didn't get a clear answer because it is not clear, even at the Federal level, who is in charge.

So we need to find a way to get our collective Federal act together and then provide the national leadership to bring in the State entities to craft a nationally oriented strategy that can be used by every response entity everywhere in the country.

Mr. Chairman, with that I will stop. Thank you again for giving me the opportunity to participate today.

Mr. SHAYS. Thank you.

[The prepared statement of Mr. Wermuth follows:]

Statement of

Michael A. Wermuth

Before the

Subcommittee on National Security, Veterans Affairs, and International Relations

Of the

Committee on Government Reform

On

"Combating Terrorism: Assessing Threats, Risk Management, and Establishing Priorities"

United States House of Representatives
106th Congress, 2nd Session

July 26, 2000

Michael A. Wermuth
RAND
1200 South Hayes Street
Arlington, Virginia 22202-5050
703-413-1100

RAND is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. This statement is based on a variety of sources, including research conducted at RAND. However, the opinions and conclusions expressed are those of the author and should not be interpreted as representing those of RAND or any of the agencies or others sponsoring its research.

STATEMENT OF MICHAEL A. WERMUTH

Mister Chairman and distinguished Members of the subcommittee, thank you for giving me the opportunity to submit the following statement to you on the issue of efforts to combat terrorism.

The threats from potential terrorists to U. S. citizens and U.S. national interests, both at home and abroad, cover a broad spectrum of both potential *sources* – individuals and groups, state-sponsored or not, foreign and domestic – as well as potential *agents* and *devices* – chemical, biological, radiological, nuclear, and conventional weapons and explosives. Unlike our experience during the Cold War, when our primary enemy was the Soviet Union, and our ways and means of keeping track of that enemy's capabilities and intentions was fairly well defined and executed, threats from terrorists are much more diverse, much more vague, and constantly evolving and mutating.

As a result, the old ways of doing business, especially in the context of intelligence collection and dissemination, and the analytical processes that apply in that context, are not in many ways appropriate or effective where terrorism is involved, especially from non-state actors. What is now required are some innovative approaches, some new means of collaboration,

---

Michael Wermuth is a Senior Policy Analyst at RAND, and is the project director for the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, established by Section 1405 of the National Defense Authorization Act for Fiscal Year 1999 (PL 105-261). He served as Deputy Assistant Secretary of Defense for Drug Enforcement Policy from 1989 to 1993, as the senior official in the Department of Defense dedicated exclusively to the Drug Interdiction and Counterdrug Activities program and to interagency coordination of the department's programs and activities to implement the President's National Drug Control Strategy. Mr. Wermuth had previously served as Principal Deputy Assistant Attorney General for Legislative Affairs, where he was directly involved in crafting and negotiating major pieces of legislation dealing with federal criminal and civil law. Mr. Wermuth served as Chief Counsel and Legislative Director for United States Senator Jeremiah Denton of Alabama, during the Senator's entire tenure in the U. S. Senate. Mr. Wermuth has also worked in the private sector as a consultant on issues involving various agencies of the U.S. Government, and has been involved in several joint venture enterprises. Before coming to the Nation's Capital, Mr. Wermuth was in the private practice of law in Mobile, Alabama, as a partner of Wilkins, Druhan & Wermuth. Mr. Wermuth's military experience, including both active and reserve duty with the U. S. Army, spanned more than 30 years before his retirement as a Reserve Colonel in 1999. He commanded at the company, battalion, and group level. He is a graduate of the U. S. Army War College, and his military awards and decorations include the Legion of Merit, five awards of the Meritorious Service Medal, four awards of the Army Commendation Medal, and the NATO Medal. He is also a recipient of the Secretary of Defense Award for Outstanding Public Service from Secretary Dick Cheney. Mr. Wermuth received his Bachelor of Science in Commerce and Business Administration from the University of Alabama, and his Juris Doctor from the University of Alabama School of Law. He is admitted to the practice of law in Alabama and in the District of Columbia, and before several U. S. Courts of Appeal and the Supreme Court of the United States.

RAND IS A NONPROFIT INSTITUTION THAT HELPS IMPROVE POLICY AND DECISIONMAKING THROUGH RESEARCH AND ANALYSIS. THIS STATEMENT IS BASED ON A VARIETY OF SOURCES, INCLUDING RESEARCH CONDUCTED AT RAND. HOWEVER, THE OPINIONS AND CONCLUSIONS EXPRESSED ARE THOSE OF THE AUTHOR AND SHOULD NOT BE INTERPRETED AS REPRESENTING THOSE OF RAND OR ANY OF THE AGENCIES OR OTHERS SPONSORING ITS RESEARCH.

potentially the removal of some historical barriers – certainly in the bureaucratic context, perhaps in the legal and regulatory context as well.

I am acutely aware of the potential for over-zealousness, for government over-reaching, for the ostensible justification for intrusive efforts that could trample on the civil liberties of our citizens, as well as those from or in other countries. But I am equally as convinced that, with proper planning, with oversight from the Congress and other entities with responsibilities to ensure the appropriateness and legality of government actions, we can and must move forward on a broad front, to ensure that everything that can be done – within the boundaries of our Constitutional protections – is being done to protect our citizens, our property, indeed our very way of life, from potential perpetrators of terrorist acts.

There are increasingly new programs and new funding – at all levels of government: local, state, and Federal -- for improving our capabilities to *respond* to a terrorist attack. But I believe few will argue with the proposition that what we want is not to have to respond. First and foremost, our goal should be to deter potential terrorists from wanting to strike in the first place. Failing that, we should have sufficient capabilities to prevent the terrorist incident, which requires sufficient resources and efforts to identify potential terrorists, to detect their nefarious plans far enough in advance to do something about them, and then to preempt or interdict them before they attack. It is only if all of the above fail that our response mechanisms will come into play. Having said that, I fully support efforts to prepare adequately for an effective response, in the event that a terrorist attack does occur.

For despite our very best efforts, it is unlikely that we can ever assure the American people that we will always be able absolutely to identify every individual terrorist or terrorist groups, to detect their plans in advance, and to stop them before they strike. It is unlikely – and most Americans would, I believe, agree with the proposition – that we could have identified Timothy MacVeigh as a potential terrorist, and detected his plans in advance, in order to be able to stop his attack at the Alfred P. Murrah Federal Building in Oklahoma City in April of 1995 – certainly not with the processes in place at that time. In the future, and with forethought and innovation, perhaps we can do a better job of identifying the "Timothy MacVeighs" among us.

We managed to escape the days and hours around the turn of the century without an actual terrorist attack inside our borders. We can be thankful for that, in large measure due to some very skillful and well-coordinated law enforcement efforts, but also to some extent from just plain luck. We were lucky that Ahmed Ressam let his nerves get the better of him when he tried to cross over from Canada into Washington State on December 14, and that well-trained INS agents picked up on the nervous "profile" and were relentless until he was in custody. We were lucky that Lucia Garofalo and her companion, Bouabide Chamchi, were clumsy in their attempt to cross into Vermont from Canada on December 19, and fell into the clutches of equally astute law enforcement agents. We can also be thankful that communication and coordination among agencies at various levels of government – from New York, to Boston, to San Francisco – resulted in the arrest or detention, and will likely lead to further prosecutions, of other alleged

members of foreign terrorist cells. That result was positive, in part, due to some good analysis that had been done prior to those two "triggering" incidents.

We can also thank Federal, state, and local officials for uncovering and stopping an attack on two huge propane storage tanks near Sacramento, California by local "militia" members, which could have killed hundreds – perhaps thousands – of their fellow citizens in surrounding communities. And another local "militia" member, alleged to have been plotting to blow up power plants and transmission lines, was arrested in Florida in early December of last year. These are good signs; but we can, in my opinion, do much better.

Mr. Chairman, in your letter of invitation to me to testify today, you asked that witnesses address certain specific questions, the first of which has to do with how terrorist threat assessments are developed and kept current. In the following paragraphs, I will attempt to answer that question, as well as questions about the existence of an "integrated threat and risk assessment, incorporating the terrorist threat to military installations and forces, the international threat, and the domestic terrorist threat against which government-wide funding priorities can be compared," and also the "benefits of having an integrated threat assessment."

Let me state, first of all, that I am generally familiar with the processes used by both of the preeminent Federal agencies responsible for these products: The Central Intelligence Agency for foreign threats, and the Federal Bureau of Investigation (FBI) for threats domestically (from both foreign and domestic sources). That knowledge is based on my prior government service and, more recently, with work that I have done on domestic terrorism issues. In the latter case, that knowledge proceeds from briefings to which I have been party, as well as discussions with several agency officials. I know that Members of this subcommittee have, earlier today, received classified testimony that likely describes those processes in considerably more detail, and which hopefully have addressed the answer to the question much more fully than, perhaps, I can in this testimony.

My general comment about the international threat and risk assessments being done within the Intelligence Community, with respect to threats to U.S. citizens and other U.S. interests abroad, and in connection with potential foreign threats that may be exported to our country, is that the current process for doing that is reasonably good. People, including policy makers and subject matter experts, may – and do on occasion – disagree with some of the conclusions contained in those assessments, but the processes for how the assessments, including National Intelligence Estimates (NIE), are developed and the data used in those assessments is relatively sound. Currency is another question: Given the fluid and ambiguous nature of the potential threats for terrorists, and the fact that new groups and individuals, with both motive and capability to perpetrate some level of terrorist attack, seem to emerge much more frequently, the Congress and other policy makers have every reason to ask whether the assessments are frequent enough. If the current structure and formal processes for conducting such assessments are too rigid or too entrenched in Cold War analytical mechanisms to provide timely assessments, perhaps some different, more streamlined process is in order.

My opinion about how that process works on the domestic front, and on the effectiveness or the timeliness of the products that are intended to flow from that process, is not as sanguine. The FBI has that responsibility; and while it is now taking some steps to fulfill that responsibility more effectively, it has not yet fully accomplished the mission. The General Accounting Office has come to the same conclusion. In its authoritative report last fall,[1] GAO noted that the FBI has not "captured in a formal, authoritative, written assessment[2]" terrorist threats domestically, from both foreign and domestic sources; and I concur in those findings.

The United States will always be vulnerable in almost limitless ways. We are an open society, with relatively open borders to foreign visitors. The length of our borders and the sheer amount of commerce and tourism that floods through our ports each day, makes it virtually impossible to detect every agent or device that a terrorist may try to bring into our country. But just because we are vulnerable in any number of ways, does not necessarily mean that a current threat exists to exploit that vulnerability. That makes good intelligence – appropriately collected and properly analyzed – all the more critical. But that, of course, is not enough. Threat assessments must be matched to vulnerabilities in order to complete valid risk assessments at various points in time. Only through that process will we be able to determine the priorities for emphasis for our efforts and, therefore, the dedication of resources.

Mr. Chairman and Members, part of the problem here is "cultural." The FBI is the foremost law enforcement agency in the world, but therein lies the heart of the cultural issue: Gathering investigative information for prosecution is dramatically different than collecting and analyzing threat information. The FBI clearly has a lot more to learn about intelligence analysis, and threat and risk assessments. But I am heartened by the word that the FBI and the CIA have formed a relatively new collaborative effort, which is designed to help the FBI learn more about the tested and proven methods of intelligence analysis by other entities in the Intelligence Community. And I am convinced that that has been and can continue to be done without crossing the bright line established in law and regulation that prohibits our foreign intelligence collection and analytical agencies from engaging in domestic collection.

I was struck a few months ago by an illustrative story that someone related to me. A few years back, as the story goes, a member agency of the Intelligence Community asked a Federal law enforcement agency if it could have limited access (certain information redacted) to the law enforcement agency's closed drug investigative files. By only looking at closed files, the intelligence agency would not be potentially interfering with an on-going investigation or prosecution. Although the law enforcement agency was puzzled by the request to look at closed files, some good work by seasoned intelligence analysts produced from those files an almost complete picture of the structure and inner-workings of one of the world's largest drug cartels.

---

[1] "Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks," U.S. General Accounting Office, September 1999 (GAO/NSIAD-99-163).
[2] Ibid, p.3.

Mr. Chairman, I have seen a recent unrestricted and unclassified document produced by the FBI, which purportedly is intended to address part of this problem. It is titled "Chemical and Biological Agent National Level Risk Assessment," and is apparently in at least partial response to earlier GAO findings, questions and specific direction from the Congress,[3] and the FBI's and Department of Justice's own acknowledgements that more needs to be done.[4] That two-page document is, however, only a broad statement of the FBI "mission" and "process" (the two major subheadings in the document) for such an assessment. And that description of mission and process is fatally flawed in one critical area. The document describes an assessment that is directed at evaluating various chemical and biological agents that terrorists may use to "create mass casualties," and analyzing the capabilities of a "non-state sponsored (sic) domestic actor" to use them. The critical element missing is that the plan makes no mention at all of motives or intentions. Assessments that do not consider in depth terrorists' motives and intentions, along with capabilities, are in my opinion virtually worthless.

The FBI document also does not provide any specificity or detail, other than a short list of tasks, as to how a process will be developed and implemented to accomplish the objectives. There needs to be, in my view – and most likely in classified form – a full description of that process, so that every participating entity, to include the field agents of the FBI and other participating or contributing Federal, state, and local agencies, is fully aware of the requirements and the anticipated products. Such a comprehensive description of the process will also allow for appropriate Congressional oversight.

In a recent letter on the subject to the Chairman of your full committee, Assistant FBI Director John Collingwood noted many legal and practical restrictions and difficulties in conducting the type of comprehensive domestic assessment that could be compared to a National Intelligence Estimate in the foreign context. While many of Mr. Collingwood's points may be well taken, the task is not, in my view and the view of others who work this issue almost daily, as seemingly insurmountable as that letter might suggest. It is true that the well-established civil rights and liberties of U.S. persons must be protected as part of that process. It may well be true that certain laws and guidelines need to be reviewed, collaboratively between the Executive and Legislative Branches – perhaps even with some scholarly judicially-based input – to determine if minor modifications or adjustments are in order. In my view, we can make improvements without even raising the suggestion that our government is attempting to be more intrusive. As an example, if current laws and guidelines prevents the FBI or other law enforcement agencies from collecting (even with appropriate judicial oversight) and analyzing information on a single individual terrorist – the "lone wolf" in FBI jargon – such as the "Unabomber," Theodore Kaczynski, then perhaps some tweaking of the rules may be in order. I am convinced that that

[3] *E.g.*, Section 1404, National Defense Authorization Act for Fiscal Year 1999, Public Law 105-261 (H.R. 3616, 105th Congress, 2nd Session), October 17, 1998.

[4] See letter FBI Assistant Director John E. Collingwood to the Honorable Dan Burton, Chairman, House Committee on Government Reform and Oversight, dated March 22, 2000; and letter from Assistant Attorney General Stephen Colgate, to GAO, dated July 16, 1999, reproduced in GAO/NSIAD-99-163, op. cit., at page 33.

and other adjustments to authorities can be made, while fully protecting our cherished civil rights.

Fundamentally, therefore, we do not have that integrated threat and risk assessment incorporating terrorist threats to military installations and forces, including international threats and domestic terrorist threats. Hopefully, the benefits from having such an integrated threat assessment are self-evident. Current, comprehensive, well-analyzed information, and the virtually seamless sharing of that information (recognizing the protections and restrictions that must be observed in the process), will likely add to the understanding of the nature of the various threats at any point in time. But the process must be a continual one; in today's global environment, threats may well change at virtually the same speed as changes in technology. Threat and risk assessments must keep pace.

The foregoing may be taken as hypercritical of the FBI. Let me state again my sincere admiration for that agency. I have had the opportunity on more than one occasion to work closely with the FBI. There is no lack of good intention at the Bureau; it will be a learning process, and I am convinced that constant improvement will be made. My comments are intended to be constructive in the continuing pursuit of more effectiveness in the collective efforts to combat terrorism.

Mr. Chairman, I will now briefly answer the Chairman's last question – "How do other countries allocate resources and determine funding priorities to combat terrorism?" – before coming back to the next to last question. While the more extensive work that I have done in this field has been on U.S. domestic efforts to combat terrorism, I have studied several comparative analyses of other countries' efforts in this arena. Israel is perhaps the most instructive, as it is one country that, for obvious reasons, has been required to devote a lot of attention and resources to the issue. Without delving in to all of the specifics, let me simply say that Israel has several advantages and some additional authorities, when compared to the United States, with which to combat its terrorism problems. First, its internal structure – *e.g.,* Israeli law enforcement organized on a national hierarchy, compared to our Federal, state, and local independent entities -- helps to facilitate its efforts against terrorism, from policy, to planning, to resourcing, to command and control during an incident. Second, Israel does not have some of the same civil liberties protections that we enjoy; and we must assume that the American people do not want us to go down a road that would lessen those protections that we have.

A senior official of our national government is purported to have remarked recently that "Americans will willingly give up some of their civil rights" if a catastrophic terrorist event occurs. Mr. Chairman, I believe that, with proper planning and oversight, reasonable men and women, at all levels of government and from the private sector, can find ways to improve our own efforts to combat terrorism without having to resort to such measures.

In conclusion, Mr. Chairman and Members, I will also respond briefly in this written submission to the Chairman's next to last question in the letter of invitation to testify today: "Is

funding to combat terrorism being properly directed?" My first response to that question is, pardon me, with a question: "How can anyone tell?" In the absence of a true national strategy, ones that has an identifiable end state (or end states over time), with clearly articulated goals and objectives to reach the end state(s), and that specifically identifies priorities to support the accomplishment of those goals and objectives, the Congress is likely to continue to have hearings – *ad infinitum* and *ad nauseum* – repeating the same question. If you believe in the premise, as I and many others do, that the initial, and in some cases, the only response will come from the courageous men and women on the front lines of public safety every day – the local responders from fire services, law enforcement, emergency medical technicians, public health, primary medical care, emergency management – then a strategy must be developed with them primarily in mind. We currently have no such strategy. And no amount of touting Presidential Decision Directives (PDDs),[5] the Attorney General's Five-Year Interagency Counterterrorism and Technology Crime Plan,[6] or the recent budget submission jointly compiled by OMB and the NSC staff,[7] nor all of them taking collectively, can amount to a true national strategy.

Moreover, the Executive Branch structure, for dealing with the various aspects of just the Federal efforts aimed at combating terrorism, continues to be in disarray. There is no effective coordination structure in place for overseeing the plans, programs, and budgets of the various agencies involved, which in turn means that Congressional grants of authority and resources are likewise not well coordinated and focused. Unless and until we can get the Federal act together, and provide some coherence and cohesion to all of the Federal processes – threat and risk assessments, Federal assistance to State and local entities, various types and appropriateness of responses by Federal entities (including the U.S. Armed Forces), coordination of the application of all our capabilities – we are unlikely to achieve a truly integrated and fully coordinated national effort.

Mr. Chairman and Members, I could devote many more pages to this latter topic, but I will at this point close with an expression of appreciation to the subcommittee for giving me this opportunity to testify, and with the offer to answer questions from any of you, either orally or in detailed written form.

---

[5] E.g., PDD 39 and PDD 62.
[6] September 1999; "interagency" presumably means Federal interagency.
[7] Annual Report to Congress on Combating Terrorism, May 18, 2000.

Mr. SHAYS. Mr. Parachini.

Mr. PARACHINI. Thank you, Mr. Chairman, for convening this hearing. There are a number of things ongoing and have been ongoing since 1995, and now is an appropriate time to push back and evaluate what are we doing right and wrong. I think what is missing from our national discussion on terrorism is a regular national predecessor. How much is enough remains an open question.

As one renowned scholar in the terrorism field has noted, without a firm understanding of the threat based on rigorous ongoing reviews of an evolving or changing terrorist behavior and capabilities, continued efforts to address this problem may prove as ineffective as they are misplaced. So a comprehensive threat assessment that integrates information on both domestic and international terrorist threats are a baseline tool.

At the moment, far too much of the government's policy on terrorism is driven by perceptions of worst case scenarios. Inordinate attention to vulnerabilities may be skewing resources in ways that do not effectively add to the government's efforts to protect our personnel and the facilities of private businesses and citizens at home or overseas. Producing a comprehensive and integrated national threat assessment which takes into account vulnerabilities as well as the capabilities and motivations of terrorists, will improve our national understanding of the threat and should inform the President and the Congress, as they decide upon investments, in short and long-term programs. Policymakers prioritize spending and programming emphasis via a variety of tools, but intelligence is an essential one. The view of the intelligence community should serve as a critical baseline. Without a regular comprehensive and integrated threat assessment of security challenges posed by terrorism, policymakers will draw conclusions on raw and finished intelligence that comes across their desks. A regular terrorism threat assessment will lessen the possibility that long-term investments in program decisions are made according to the vicissitudes of raw intelligence and ensure, that at least on a regular basis, there is an intelligence community benchmark calibrating that threat.

The OMB annual report on the spending is a useful document, but it is not a substitute for a national strategy. The various Presidential decision directives are useful, but in themselves a collection of documents put together at different times do not amount to a national strategy. So a national strategy is needed, and before you can have a national strategy, at least one of the tools has to be a comprehensive national threat assessment.

Let me turn to the budget such that I can point out some elements of the OMB's report that should be improved with a national threat assessment, and hopefully this committee will work with the executive branch to improve the dialog on the U.S. terrorism policy. If you look at the various OMB annual reports on spending, you will find that the numbers do not track from year to year. That is one thing of clarification that would be very valuable, I think, for helping both the Congress provide adequate oversight to the American people and scholars like myself to track what the administration is doing, and it might help the administration keep on track what they are doing. This is not an easy task. OMB has made a great effort and the product is sound. It could be better.

When you look at the overall budget figures thinking about a more thorough threat assessment, one of the things that comes to my mind about a national strategy is that we need to shift the emphasis about what we are doing. We are focused too much in my opinion on the back end of the problem, after an event has happened, and we need to think about a slight emphasis toward the front end. How can we prevent and preempt an attack from ever happening in the first place?

The amount of dollars spent for things at the back end are more than at the front end. We need to shift the emphasis. I realize that we always want to hedge against the unexpected of something that we never want to happen, and lives can be saved if we are better at responding, but we have gone overboard in my opinion, because we don't have a good sense of a threat and we are worried about worst case, and so we spend too much on the back end, on the after event mop-up, and not enough is spent on providing the intelligence and law enforcement resources to try to prevent these events from ever happening in the first place.

Let me conclude by indicating two things. In the rapid budget increases that have occurred in the last 3 and 4 years, it is very hard to evaluate whether budget increases of 300 percent or 500 percent in various programs within department and agencies are appropriate, out of kilter or out of control. And at least a common threat assessment on a periodic basis would help provide a benchmark to help figure that out.

Finally, in the research and development area, which is the most difficult, because some of the investments that you make now don't bear fruit for many years into the future, we have got to have at least some consensus that we are investing in the right things at this point in time.

And at least some periodic regular national threat assessment would be a helpful way to ensure that. Thank you, Mr. Chairman.

Mr. SHAYS. Thank you very much, Mr. Parachini. Your statement was fairly long. I appreciate you summarizing it. But it's an excellent statement, and that, of course, as will the others, be in the record.

[The prepared statement of Mr. Parachini follows:]

Statement of

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

Before the House Subcommittee on National Security, Veterans Affairs, and International Relations

Combating Terrorism:

Assessing Threats, Risk Management, and Establishing Priorities

July 26, 2000

Mr. Chairman,

I want to thank you, other committee members, and your staff for inviting me to share my views on how the United States assesses the threat posed by terrorism and allocates its resources to meet it. The United States government has moved rapidly to address the dangers posed by new trends in terrorism that emerged in the last decade. With local responder training ongoing in many cities around the nations, the establishment of the Joint Task Force, and a number of important R&D program underway, now is an appropriate time to review national efforts and make improvements where necessary.

While I believe the United States has made great strides in recent years to enhance federal, state and local capabilities to combat terrorism, particularly terrorist use of weapons of mass destruction (WMD), I am concerned that many of the efforts launched in the mid-1990s need to be reconsidered. I particularly fear that our national anxiousness to address the so-called "New Terrorism" may be inadvertently adding to the danger. As a result, we are spending big, but not spending smart (See Figure 1). There clearly are new trends in terrorist behavior. But we must make sure that we are drawing accurate lessons from the past and guarding against future developments that are credibly in the realm of possibility and not merely reflections of our wildest nightmares.

In addition to the committee's important oversight function, I strongly urge the committee and its staff to engage in a regular dialogue with the executive branch on this issue. As a nation, we are more likely to be most effective in combating the threat of terrorism if a variety of government and private institutions are working on this problem. There are no silver bullets, no special individuals and no single institution for defeating terrorism. To check the threat posed by domestic and international terrorism will require sustained effort by many different entities.

I. Terrorism Threat Assessments and Risk Management Strategies

The United States currently lacks a comprehensive and integrated intelligence assessment to inform policymaker thinking on how to prioritize spending decisions to support the government's programs to combat terrorism. The General Accounting Office (GAO) has indicated repeatedly that part of the problem with the current executive branch approach to terrorism is the lack of "threat and risk assessments that would suggest priorities and appropriate countermeasures."[1] The GAO's observation is extremely important and should be addressed in a serious manner. The importance of the GAO view is that we lack a reasoned basis for making a case that we are spending too little, too much or just enough to combat terrorism. How much is enough remains an open question. As one renowned scholar succinctly noted, "without a firm understanding of the threat based on rigorous, ongoing reviews of evolving or changing terrorist behavior and capabilities, continued efforts to address this problem may prove as ineffective as they are misplaced."[2]

The last formal National Intelligence Estimate (NIE) on terrorist threats occurred three

years ago. While this estimate was broad in scope, it was not intended to serve as a national assessment to assist policymakers in calibrating government efforts and spending decisions. Currently there is no single person who serves as a National Intelligence Officer (NIO) for terrorism. In a de facto fashion, the Director of Center Intelligence's (DCI) Counterterrorist Center generally serves this role. Given the jurisdictional restraints on the Central Intelligence Agency, the Counterterrorist Center cannot assemble an assessment that combines information on both domestic and international terrorism.

With a security threat as fluid and elusive as terrorism, the challenge of crafting effective short and long term measures is very difficult. Intelligence on terrorist threats is significantly different than intelligence on military threats from nation-states. Intelligence on the military programs of nation-states is comparatively more static and large enough to be covered by a variety of intelligence means. Numerous intelligence assessments on the threat posed by ballistic missiles have been conducted in recent years.[3] Similarly, a number of special commissions have also sought to provide the Congress, the President and the American people with their view of the threat.[4] These assessments have contributed to the national debate on the threat posed by ballistic missiles and the measures that may be required to address the threat. The short and long-term measures addressing the proliferation of ballistic missiles bear significant financial implications for the country.

While the threat posed by terrorism is much more difficult to gauge, analysis of the threat certainly deserves as thorough a review. Several special commissions have contributed to our collective understanding of the threat posed by emerging trends in terrorism, but their mandates have not specifically focused on assessing the threat. What is missing from our national discussion on how to best combat terrorism is a regular, comprehensive threat assessment that integrates assessment of both domestic and international terrorist threats.

Without a regular, comprehensive and integrated threat assessment of the security challenge posed by terrorism, policymakers draw conclusions on raw and finished intelligence information that comes across their desks. Policymakers prioritize spending and programming emphasis via a variety of tools, but intelligence is an essential one. The view of the intelligence community should serve as a critical baseline for the decisions of policymakers.

Policymakers should not assemble the intelligence assessment in a piecemeal and episodic fashion. Rather, policymakers should have the benefit of a regular, comprehensive and integrated terrorism threat assessment that informs both short-term and long-term policy decisions. Moreover, given the transnational and increasingly loose networks of individuals conducting terrorist acts, policymakers must have a picture of both domestic and international terrorist threats. Examining one set of threats in isolation from the other may hinder early identification of key warning signs.

A regular, comprehensive, and integrated threat assessment will help ensure that intelligence information that withstands the scrutiny of the entire intelligence community informs

program and spending decisions. While policymakers can call upon portions of the intelligence community at any given time for information, a regular, comprehensive and integrated community-wide assessment would provide a process and a document that they take into account when making program and spending decisions.

The Congress should consult with the President about modalities for generating a comprehensive and integrated terrorism threat assessment on a regular basis. One option, and the best in my opinion, is to have the Interagency Intelligence Committee on Terrorism conduct a comprehensive and integrated assessment every year or two. Another option is to establish a National Intelligence Officer for terrorism. In order to ensure that the assessment integrated information on foreign terrorism with domestic terrorism, it is worth considering an equivalent officer in the Federal Bureau of Investigation. Given the constitutional restrictions, the FBI's Counterterrorism Threat Assessment and Warning Unit may be the proper office to charge with stitching together the assessments of foreign and domestic terrorist threats. And finally, a third option and in my opinion the least desirable option, is for the National Security Council to generate an assessment based on the information it reviews from existing intelligence assessments. In a de facto fashion, this is what currently occurs. The only difference is that a formal NSC assessment might accompany the Office of Management and Budget's Annual Report to Congress on Combating Terrorism.

A regular terrorism threat assessment will lessen the possibility that long-term investment and program decisions are made according to vicissitudes of raw intelligence and ensure that at least on a regular basis there is a community benchmark calibrating the threat. Finally, and importantly, assembling this report on a periodic basis requires appropriate resources to meet the increased tasking on the intelligence community. Too often the intelligence and law enforcement communities are given new responsibilities without the resources to carry them out and they end up pulling resources from other existing duties and stretching personnel beyond desirable limits.

Creating a national strategy to address a threat for which there is not a clear consensus on the magnitude of the threat leaves the task of crafting a strategy without context. In recent years, United States policy to combat the threat of terrorist use of weapons of mass destruction has been driven by perceptions of vulnerability to such attacks rather than the likelihood. A comprehensive threat assessment would presumably factor in capabilities and motivations in addition to vulnerabilities. The inordinate focus of our antiterrorism policy on vulnerabilities and worst-case planning may skew precious federal resources to less critical aspects of the terrorism problem.

The recent scare over the vulnerability of the national monuments is just the most recent example of how the lack of a comprehensive assessment of threat that takes into account the likelihood of an attack can be exploited by government bodies seeking to call attention to their budgetary needs.[5] News reporting on a study conducted by a private contractor for the National Park Services just prior to the our national Independence Day, as hundreds of thousands of Americans planned to visit our national monuments, was a case of threat manipulation for budgetary benefit in the extreme.[6] The release of information from this report just prior to this

national holiday and prior to the conclusion of the congressional budget process seems hardly a coincidence. As two private experts pointed out in the news reporting, the National Park Police are not alone in our nation's Capitol when it comes to protecting the city from terrorist attacks, nor is it possible to completely eliminate all vulnerability. Addressing the communications or overtime needs of the National Park Service should be possible without scaring citizens away from visiting national monuments on Independence Day or unnecessarily drawing attention to vulnerabilities that might be exploited by individuals or groups with malicious designs.

Basing threat perception on vulnerabilities and gearing much of our terrorism response capabilities according to worst-case scenarios is skewing our approach to terrorism. A number of problems stem from a focus on vulnerabilities and worst-case response planning. First, the historical record on terrorism and the intelligence community both suggest that conventional explosives continue to be the weapon of choice for terrorists.[7] Low consequence attacks with multiple-use chemicals and non-contagious biological agents trails behind conventional explosives as the likely weapon of choice. There is a low probability of high consequence attacks that may involve the full range of unconventional weapons materials.

Second, by focusing on the low probability, high consequence events we may tend to categorize too many of them involving unconventional weapons materials as federal events when state and/or local resources may be more appropriate.[8] Given the potential for demands on federal assets to meet American interest abroad as well as at home, they should be saved for when they are appropriately required.

Third, frequent discussion about our vulnerabilities draws attention to them. Most of the WMD cases the FBI investigated in recent years were anthrax hoaxes. Our public communication about the terrorist threat is inadvertently eliciting threats that distract our resources from real attacks by determined terrorists.[9]

Fourth, we must guard against inflating the potential of this threat to such a large degree that we create conflicts between funding for antiterrorism measures at home and important missions for our military abroad. Inordinate concern about catastrophic domestic terrorism may lead policymakers to call upon the military to perform missions at home that should be the domain of non-military service government organizations. Mission dilution of our military is something that constantly warrants the attention of the President and the Congress. We should keep the military's missions few and well defined such that it can perform at the highest level of effectiveness.

An open society such as ours cannot eliminate completely danger from all aspects of life. Prudent risk assessments will help us reduce the danger and improve our ability to respond in the unlikely event of an attack. We accept risk in many other areas of American society that result in the tragic loss of life. We want to guard against any terrorist attack that not only threatens the lives of our citizens, but also calls into question the authority of our government. This balance can be achieved at acceptable cost bearing in mind some risk.

Both executive and legislative branches of government seek to address the threat posed by catastrophic terrorist attacks. Senior officials say that they will accept criticism for being over-prepared and over-compensating for the threat.[10] Some congressional staff suggest that the political danger of being parsimonious with spending to combat terrorism is too great to do anything but prepare for the worse-case scenario. While some hedge against the unpredictability of the future is commendable, we must not confuse prudent measures with efforts to avoid political blame for failure to take necessary precautions. Government has a responsibility to prepare for unlikely events that could produce catastrophic consequences. However, a balance must be struck between responsible preparedness and mere political hedging.

A comprehensive terrorism threat assessment will presumably be informed by a thorough analysis of past terrorist incidents with unconventional weapons. Far too many policymakers and researchers rendering assessments about terrorist use of unconventional weapons focus on what they *imagine* terrorists could do, not on what they have done in the past, which leads them to substitute their thinking for that of the terrorists. Acknowledging that history is not a perfect guide to the future and that government has a responsibility to take precautions against even unlikely eventualities, there must be some baseline, some historical context in order to consider potential eventualities.

II. Comprehensive Terrorism Threat Assessment and a National Strategy for Combating Terrorism

A comprehensive terrorism threat assessment is an essential component for crafting a national strategy for combating terrorism. A national strategy should guide the creation of programs and allocations of resources to implement the strategy. The report submitted by the Director of the Office of Management and Budget (OMB) pursuant to section 1051 of the Fiscal Year 1998 National Defense Authorization Act (Public Law 105-85) entitled "Director of the Office of Management and Budget's Annual Report to Congress on Combating Terrorism" (hereafter "the OMB Annual Report") provides a useful basis for congressional and public review of the executive branch's policies and programs.[11] The year 2000 version of this report does describe a sound budget review process.[12] The document as a whole is a considerable improvement over previous versions of the report.

The OMB Annual Report notes that the Clinton administration's terrorism policy is outlined in Presidential Decision Directives (PDD) 39, 62 and 63 and specific agency guidance such as the Attorney General's "Five-Year Interagency Counter-Terrorism Plan." These documents, issued over the course of the last several years, form a basis for a national strategy. The current budget review process described in the OMB annual report is not a substitute for a comprehensive threat assessment. Both a comprehensive threat assessment and a sound budget review process are needed. However, they do not amount to a national strategy. PDD-39 was issued in 1995 shortly after the sarin attack on the Tokyo subway and the bombing of the Murrah

Federal Building in Oklahoma City. PDD-62 and PDD-63 were issued in 1999. Each document was prepared at a different time, in reaction to terrorist events or developing circumstances, or designed to address specific policy gaps and meet new circumstances confronting the United States. A collection of policy documents is simply not equivalent to a national strategy like that recommended by the Gilmore commission.[13] If this national security threat is as important as the President and many of his advisors suggest, then a comprehensive strategy is an important roadmap to guide programmatic and budgetary aspects of governmental activities.

III. US Funding to Combat Terrorism

The OMB Annual Report provides a useful basis for congressional and public review of the executive branch's spending on antiterrorism and counterterrorism.[14] Funding to combat terrorism is difficult to segment into sub-categories, separating funding that specifically addresses WMD from other non-WMD related programs. Undoubtedly there is overlap that requires a judgment call as to which federal dollar spent contributes to a particular activity. The OMB is to be commended for generating this useful document.

Each annual version of the Report prepared by the OMB and submitted to the Congress provides more budgetary detail on US antiterrorism and counterterrorism activities than the previous year's version.[15] Not only does this high degree of budgetary transparency serve as a modest testament to the strength of the American political system, it creates the basis for congressional and public review that is vital to sustaining a consensus on government policy in this important area of national security.

The 2000 OMB Annual Report states that "information gleaned since the submission of the FY 2001 budget" and the submission of the Report indicates the nature of the terrorism threat has increased. Further explanation of the increased threat in the period -- February 2000 to May 2000 -- is not provided. The OMB Annual Report argues that this augmented threat is the justification for an amendment to the budget amounting to $235.5 million submitted in conjunction with the report.[16]

How financial resources are allocated serves as a critical indicator of actual, as opposed to declared, policy implementation. The OMB Annual Report is a valuable tool for understanding the direction, scope and dimensions of USG efforts to combat terrorism. However, in order to ensure that these reports serve their full potential in the future, the OMB should strive to be consistent from year to year.

An imperfection in the OMB Annual Reports over the course of the past three years is that the dollar figures described as enacted in past years are not consistent from year to year. Presumably the OMB can account for the discrepancies, by grouping items under the spending category in one report from that of the following year. For example, in the Report's general mission category of Law Enforcement and Investigative Activities, the 1999 version of the OMB

Annual Report indicates that $2.587 billion was enacted in 1999, there was a supplemental appropriation of $350 million, and that the FY 2000 requested amounted to $2.757.[17] Yet, the OMB Annual Report for 2000 indicates that $2.687 was enacted in 1999 and $2.797 was requested.[18] Thus, the 1999 dollar amount for this category plus the supplemental does not equal the amount the 2000 OMB Annual Report indicates as "enacted" in 1999, nor are the "requested" figures equivalent between the two annual reports. The confusions these apparent discrepancies sow must be rectified in future annual reports to Congress.

Clearly defining the spending items under each spending category may be one way to improve the value of these annual reports. Some analysts argue that the only way to truly understand what has been spent from year to year is to examine the Treasury accounts per department and agency. By tracking the spending according to the Treasury accounts the Congress could determine not only how it agreed with the executive branch on how funds would be spent, but also would actually see how the executive branch implemented the spending as directed by annual budget acts.

IV. Important Budget Issues

A constructive dialogue between the President and the Congress on funding to combat terrorism is critical. At present the dialogue seems satisfactory, but there is room for improvement. On the part of the executive branch, the President's representatives should consult more regularly and transparently with the Congress. On the part of the Congress, the process should be streamlined and rationalized. The plethora of committees with jurisdiction over portions of the budget supporting the government's programs to address the terrorist threat makes the consultation process cumbersome. The National Commission's recommendation that the appropriation committees in each house of Congress assign an individual staff member to track funding for combating terrorism is a useful suggestion.[19]

1. Shifting Funding Emphasis to Prevention and Preemption

Tremendous improvements have been made in our national preparedness to respond to mass casualty terrorism incidents, particularly those involving weapons of mass destruction. More progress is required and training of the next generation of local responders and officials at all levels of government will remain an ongoing task. The focused emphasis on improving capabilities to respond to a WMD attack on American soil followed the Tokyo subway attack. At the time, there was tremendous fear that Aum Supreme Truth's attack marked the start of a new pattern of sub-national terrorist activity involving unconventional weapons. Since the Tokyo subway incident much has been learned about the attack and the cult, which should help recalibrate the magnitude of the danger of sub-national groups and WMD terrorism.[20]

Putting aside the question of whether the US is allocating too little or too much funding to combat terrorism, and considering the figure of $9.3 billion requested by the Clinton administration for Fiscal Year 2001, a shift in programmatic emphasis and funding seems

warranted at this stage in the evolution of American terrorism policy. Increasing emphasis should be place on the front end of the problem, by preemption and prevention of attacks, with less emphasis placed on the back end in post-attack consequence management. The OMB Annual Report notes that from 1998 to 2001 spending for preparing for and responding to terrorist acts increased from $126 million to $627 million, an increase of 398%.[21] This shift is particularly relevant for funding relating to WMD terrorism and incident response (See Figure 2). The increase in funding for preparing for and responding to WMD terrorist acts increased from $89 million in 1998 to $566 million three years later, an increase of 536% (See Figure 3).[22] In contrast, funding for law enforcement and investigative activities has increased only $6% over the same period. While the President has asked for significant increases in this area of funding over the last two years, the end result has been only a modest increase.

Comparatively modest increases in law enforcement, intelligence and diplomatic tools may dollar per dollar contribute more to diminishing the threat. Using the OMB Annual Report's language, this means shifting emphasis from downstream investments to upstream investments. Currently, 82% of the funding goes to these downstream investments and 18% to upstream investments.[23] Some downstream investment, such as R&D into pharmaceuticals and improvements in facilities security, may entail huge costs, while more FBI agents and CIA case officers might be comparatively less. Thus, the percentage balance in favor of antiterrorism measures as opposed to counterterrorism measures is understandable. Yet, a comparatively modest shift in funding emphasis would greatly enhance our effort to preempt and prevent attacks, while not neglecting defensive measures.

The law enforcement and intelligence communities perform critical "front end" missions to combat terrorism. While both communities have received extra tasking with the increased concern about the dangers of new terrorist trends, neither has benefited from a sustained increase in funding support to fundamentally change their impact on the problem. Intelligence is the front line of defense against terrorism. The more we know about a security threat from the front line, the more tools we can assemble to address the challenge.

The State Department deserves special mention as a potential tool in the government's effort to combat terrorism. For comparatively modest amounts of funding the State Department could play a larger role to prevent terrorist attacks. Collaboration with allies to thwart attacks and pressure states that aid terrorism could hem in the problem in important ways. The intelligence community and the Department of Defense can also play an important role by collaborating with their counterparts in foreign countries to thwart attacks before they occur and sap the resources that terrorist group need to wage their attacks. Finally, it may be helpful to establish a separate line item in the State Department for combating terrorism. Currently, funding for terrorism is lumped in with the Department's Nonproliferation, Anti-terrorism, Demining and Related Programs Account (NADR). As a result of the other programs in this account, sustained support for the Department's activities is precarious.

By suggesting a shift in the emphasis of spending, I am not proposing that domestic

preparation to respond to terrorist incidents be diminished significantly or discontinued. It is my view that a more systematic approach to assessing the threat and devising programmatic guidelines with the benefit of a comprehensive and integrated threat assessment will lead to a recalibration of the threat we face in the short and medium term. It is important to establish a balance of spending that can be sustained over time and this balance will, in my opinion, require a shift in funding emphasis.

In regard to domestic preparation and response mission, the balance should shift from programs unique to terrorism to be broadened in a way to that will meet the challenges of a wider range of public disasters. Wise spending on defensive measures will have a dual-use capability that benefits American society today and serves as an asset to deter, detect or respond to a terrorist incident. Funding to improve the health and agricultural surveillance systems to guard against disease outbreaks is an example of dual-use benefit spending. Capabilities that benefit society at the moment of a catastrophic attack may be warranted, but they should be considered with a clear sense of spending trade-offs.

2. Sustainability of US Terrorism Policy

It is vitally important to forge a consensus on those essential programs and provide adequate support for them. Sustained support is particularly important in the areas of law enforcement and intelligence. Critical to the effectiveness of these mission areas is the development and retention of good personnel. The law enforcement and intelligence communities must be directed to make combating terrorism an organizational priority that is reflected in the value of such work for career advancement. Furthermore, it is important to enable personnel working terrorism issues to develop the needed expertise. Frequent rotation or multi-tasking prevent personnel from building valuable expertise.

Funding for improving the protection of our embassies abroad is one area where our inability to provide adequate funding over a sustained period of time is particularly disturbing.[24] Funding for embassy security always seems to go up the year after American embassy has been bombed and then the funding tapers off each year thereafter until another bombing occurs. The OMB Report notes that since military installations abroad have become tough targets for terrorists, there is some evidence that American embassies are preferred targets.[25] Both the Congress and the President should strive to sustain funding in this area.

3. Funding in the Medical Response Area

The Department of Health and Human Services (HHS) has received the most significant increases in funding in the shortest period of time (See Figure 4). The research agenda for many HHS programs is especially challenging. It is a Department that critically needs the grounding of a comprehensive threat assessment and the guidance of a national terrorism strategy. For example, the intelligence community has not always agreed upon the list of biological agents the US is most likely to confront. Thus, the priority list of biological agents for which vaccines and

antibiotics should be developed changed repeatedly. The implications of these changes is that it is very difficult to know what vaccines and antidotes should be developed if there is not a solid consensus on the most likely agents we may face. The research and development for these prevention and response tools could take many years, if not decades. Thus, these spending decisions require considerable care and scrutiny.

At the other end of the task spectrum for HHS is mental health response to terrorist incidents, both real and threatened, which has not received the support it should. How to manage the problem of the "worried well" and the mental trauma American society might experience in the event of a catastrophic terrorist attack deserves greater priority and financial support. The Tokyo subway attack and other mass casualty terrorist attacks suggest that hospitals will need to deal with many multiples more people with psychosomatic disturbances than physical injuries.

How to manage the onslaught of the psychosomatic and psychologically injured public must be addressed if the health system has any chance of treating the physically wounded. Our official communication about the threat of terrorism, particularly WMD terrorism, has increased rather than reduced concern. Anthrax hoaxes dramatically increased in the United States after the initial Nunn-Lugar-Domenici local responders training sessions began, as Secretary of Defense Cohen held up a bag of sugar at a news conference to indicate how little anthrax would be needed to kill thousands in a city, and as a result of the government's poorly handled detention of Larry Wayne Harris, who had anthrax vaccine in the back of his car. More sober official communications about the potential danger of WMD terrorism and our preparations might have limited the tremendous increase in unconventional weapons threats and hoaxes. The vastly different strategies in New Jersey and New York for dealing with the West Nile virus suggest that effective communication with the public about the nature of an outbreak can mean the difference between creating public concern and maintaining public order and confidence.[26]

4. R&D Spending

R&D spending poses the greatest long-term policy challenge. The search for future tools to address the full range of terrorist threats, particularly those stemming from the use biological weapons, is critical. But given the time required for new technologies to mature, special care must be taken to ensure that each yearly research dollar contributes to future technological advancements.

The R&D spending related to weapons of mass destruction (WMD) deserves special attention (See Figure 5). There are significant differences in how the OMB annual reports depicted R& D spending from one year to another. The 1999 OMB Annual Report, for example, lists very different figures for the Department of Energy R&D spending than those listed in the 2000 OMB Annual Report for the same years.

Finally, the R&D spending category of "Other" has consistently outpaced all other mission categories. Some means of characterizing the variety of activities covered by the "Other" R&D

category must be found. Proper oversight of the R&D budget is difficult without greater detail.

5. Managing Rapid Budget Increases

The President and the Congress responded rapidly to the prospect of an increase in terrorist activity on American soil and the potential use of unconventional weapons materials. In several instances, government departments and agencies received significant budget increases to "stand up" important programs. The Departments of Health and Human Services has received enormous increases in budget authority for antiterrorism and counterterrorism programs in the last few years. Managing such rapid increases in funding is bound to present formidable challenges.

A thorough review of the three or four government programs that received the most significant percentage increases is important to the integrity of the government's overall effort (See Figures 6 and 7). Challenges about the propriety of the increases and their effective allocation could stall important programs at a crucial stage of development. Alternatively, if fast growing programs have gone off track, it is important to identify these problems before sunk costs drive spending decisions more than wise policy.

6. Funding the Department of Justice's National Domestic Preparedness Office

PDD-62 designates the Department of Justice (DOJ) as the lead agency for handling domestic terrorism crisis. While allocation of financial resources is not the only way to indicate policy priorities, the lack of support for DOJ's terrorism offices is conspicuous by its absence. The 2000 OMB Annual Report does not discuss the National Domestic Preparedness Office (NDPO) in any meaningful detail. Appropriately, the task of local and state responder training will transition from the military as designated by earlier Nunn-Lugar-Domenici legislation to the DOJ's NDPO. Based on questions regarding the NDPO's funding and its operational pace, neither the executive branch nor the Congress seems to have fully endorsed the mission of this new office. This sends exactly the wrong signal to State and Local officials at precisely the moment they look to the Federal government to bring some leadership to this daunting new challenge.

V. Other Nations' Approaches to Combat Terrorism

The GAO's report on other nation's approaches to combating terrorism is a valuable contribution to improve the formulation and implementation of a national terrorism policy.[27] Examining the policies and practices of other nations, particularly those with experience who have suffered a greater number of terrorist attacks than the United States, is valuable. The most important finding of the report that should inform our national approach to the problem is how other countries view the terrorism threat in context. The nations survey by the GAO all took into account the likelihood of an attack and did not focus as intensively on vulnerabilities. They adapt their intelligence, physical protection measures, and law enforcement activities to the changing

nature of the threat. Vulnerabilities are taken into account, but the likelihood that terrorists will exploit vulnerabilities is a significant component of their preparation.

Given the greater historical experience with terrorism on their national territory, the publics of the countries surveyed accept periodic casualties without a significant loss in public confidence of the government. In the United States, we aim as a society to take whatever measures deemed appropriate to protect our entire territory, every citizen, and all public and private facilities from any and all malicious and intentional attack. Our national desire for protection against ballistic missiles is another expression of this desire that is not shared to the same degree by other nations, including many of our key allies. Furthermore, more Americans die from alcohol related traffic accidents or food-borne illness than terrorist incidents. Political support has not surged to ensure that the government take meaningful actions to reduce these casualty rates.

Taking note of the limitations of such an analysis will help American policy put this international comparison in perspective. While the GAO clearly indicates that they did not conduct a comparative study, the value of their findings lies in the potential for comparison with the United States. At this moment, the United States stands as the preeminent power with global influence and responsibilities. The countries considered in the GAO analysis are regional powers. As the sole global power the United States attracts admiration, envy and antipathy. Periodically, the US government, American companies and American citizens may be a terrorist target for no other reasons than the perception of the country's global power.

Second, two of the countries included in the GAO analysis, Israel and the United Kingdom, struggle with acute terrorism problems stemming from their presence on disputed territories. American forces stationed abroad face a somewhat similar threat environment, but it is not nearly as acute or as constant. The security environments in the Middle East and Northern Ireland have changed in the last few years due to improvements in the political dialogues of the parties concerned. The United States does not face any analogous circumstances that could lead to a significant lessening of the terrorist threat

Conclusion

A comprehensive threat assessment that integrates information on both domestic and international terrorist threats is an essential baseline tool for informing a national strategy on terrorism, which the US currently lacks. At the moment, far too much of the government's policy on terrorism is driven by perceptions of vulnerability and planning for worst-case scenarios. Inordinate attention to vulnerabilities and worst-case scenarios may be skewing resources in ways that do not effectively add to the government's effort to protect our personnel and facilities, private businesses, and citizens at home and abroad. Producing a comprehensive and integrated national threat assessment that takes into account vulnerabilities to attack as well as the capabilities and motivations of terrorists will improve our national understanding of the threat and should inform the President and the Congress as they decide upon investments in short and long

term programs to combat terrorism.

---

[1] U.S. General Accounting Office. *Combating Terrorism: Observations on Federal Spending to Combat Terrorism.* Statement of Henry L. Hinton, Jr., Assistant Comptroller General, National Security and International Affairs Division, Before the Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, U.S. House of Representatives, March 11, 1999, p. 13.

[2] Bruce Hoffman, The Debate Over Future Terrorist Use of Chemical, Biological, Radiological and Nuclear Weapons, in *Hype or Reality?: The "New Terrorism" and Mass Casualty Attacks,* ed. Brad Roberts, (Alexandria, VA: The Chemical and Biological Arms Control Institute, 2000), p. 220.

[3] DCI National Intelligence Estimate President's Summary, "Emerging Missile Threats to North America During the Next 15 Years", PS/NIE 95-19, November 1995, (http://www.fas.org/spp/starwars/offdocs/nie9519.htm) (July 24, 2000). "NIE 95-19: Independent Panel Review: Emerging Missile Threats to North America During the Next Fifteen Years", OCA 96-1908, December 23, 1996, (http://www.fas.org/irp/threat/missile/oca961908.htm) (July 24, 2000) (hereafter referred to as the Gates Panel). Report of the Commission To Assess The Ballistic Missile Threat To The United States, Pursuant to P.L. 201, 104th Congress, July 15, 1998, (hereafter referred to as the Rumsfeld Commission.) National Intelligence Council, *Foreign Missile Developments and the Ballistic Missile Threat to the United States Through 2015*, September 1999

[4] National Commission on Terrorism, *Countering the Changing Threat of International Terrorism*, June 2000 (Hereafter referred to as "The National Commission Report"). First Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, (hereafter referred to as the Gilmore Commission Report), *I. Assessing the Threat,* December 15, 1999.

[5] National Park Service, Report to Congress pursuant to P.L. 105-391 National Parks Omnibus Management Act 1998, "Law Enforcement Programs Study: United States Park Police," March 8, 2000, pp. 13-15.

[6] Arthur Santana, "Monuments Are Found Vulnerable to Attack," *Washington Post*, July 2, 2000, p. A1.

[7] For a recent study of the incidents of chemical and biological weapons terrorism frequently cited in the scholarly literature see, Jonathan B. Tucker, ed., *Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, (Cambridge, Massachusetts: MIT Press, 2000). For a recent summary of recent intelligence community rankings of terrorism threats see, U.S. General Accounting Office. *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks,* (GAO/NSIAD-99-163), September 1999.

[8] The Gilmore Commission Report, p. 21.

[9] A CIA Middle East specialist offer wise commentary on this topic just prior to the year 2000 celebration: Reuel Marc Gerecht, "Alarm Abets the Terrorists," *New York Times*, December 23, 1999, p A-29.

[10] Michael Dobbs, "Key Player in U.S. Terror War," *Washington Post*, April 2, 2000, p. A1.

[11] Annual Report to Congress on Combating Terrorism, "Including Defense Against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection," May 18, 2000 (hereafter "The 2000 OMB Annual Report").

[12] The 2000 OMB Annual Report, p. 6.

[13] The Gilmore Commission Report, pp. 53-55.

[14] The federal funding information from the report and other federal documents can be found at the web site of the Monterey Institute's Center for Nonproliferation Studies: (http://cns.miis.edu/research/cbw/terfund.htm) (July 24, 2000).

[15] The two earlier versions of the OMB Annual Report were the following: The Office of Management and Budget report pursuant to P.L. 105-85, Government-wide Spending to Combat Terrorism, March 12, 1998 (hereafter ; and, The Office of Management and Budget report pursuant to P.L. 105-85, March 3, 1999. (Hereafter these reports will be referred to respectively as The 1998 OMB Annual Report and the 1999 OMB Annual Report).

[16] The 2000 OMB Annual Report, p. 3.

[17] See The 1999 OMB Annual Report, p. 6.

[18] The 2000 OMB Annual Report, p. 48.

[19] The National Commission Report, p. 36.

[20] The Gilmore Commission, pp. 40-50. See also, Milton Leitenberg, "The Experience of the Japanese Aum Shinryko Group and Biological Weapons," in *Hype or Reality?: The "New Terrorism" and Mass Casualty Attacks,* ed. Brad Roberts, (Alexandria, VA: The Chemical and Biological Arms Control Institute, 2000), pp. 159-172.

[21] The 2000 OMB Annual Report, p. 11.

[22] The 2000 OMB Annual Report, p. 13.

[23] The 2000 OMB Annual Report, p. 53.

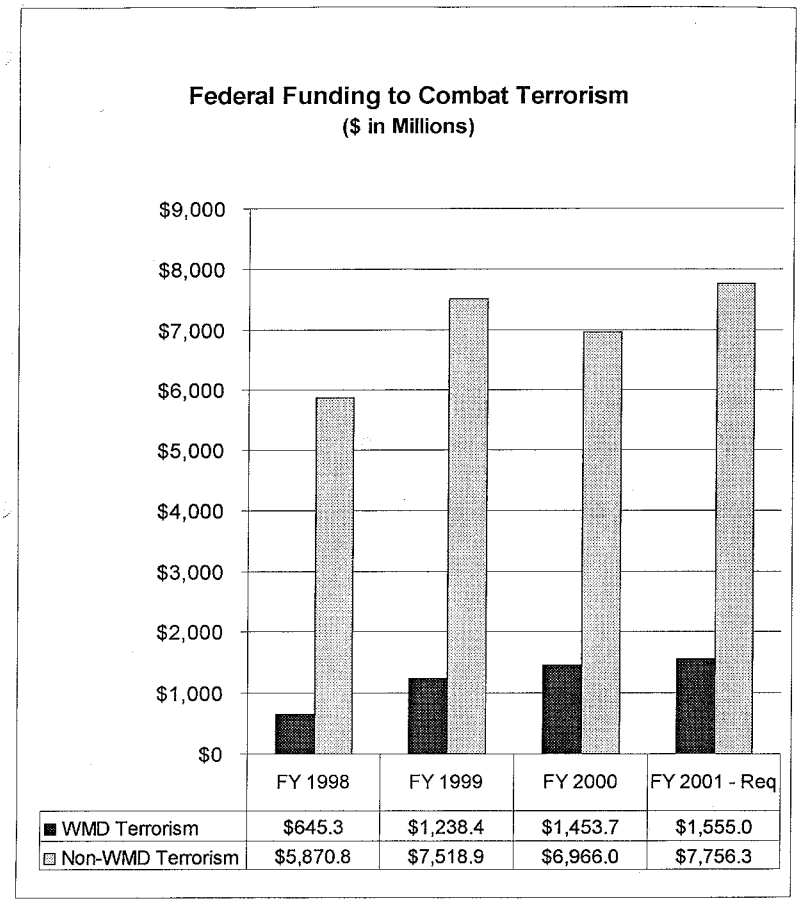
[24] Report of the Accountability Review Boards, "Bombings of the US Embassies in Nairobi, Kenya and Dar es Salaam, Tanzania," August 7, 1999 (http://www.state.gov/www/regions/africa/accountability_report.html) (October 18, 1999).

[25] The 2000 OMB Annual Report, p. 10.

[26] Matthew Purdy, "Public Health Meets Public Relations in Battle Against Mosquitoes, *New York Times*, p. 19.

[27] "Combating Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism," U.S. General Accounting Office (GAO/NSIAD-00-85) (April 2000).

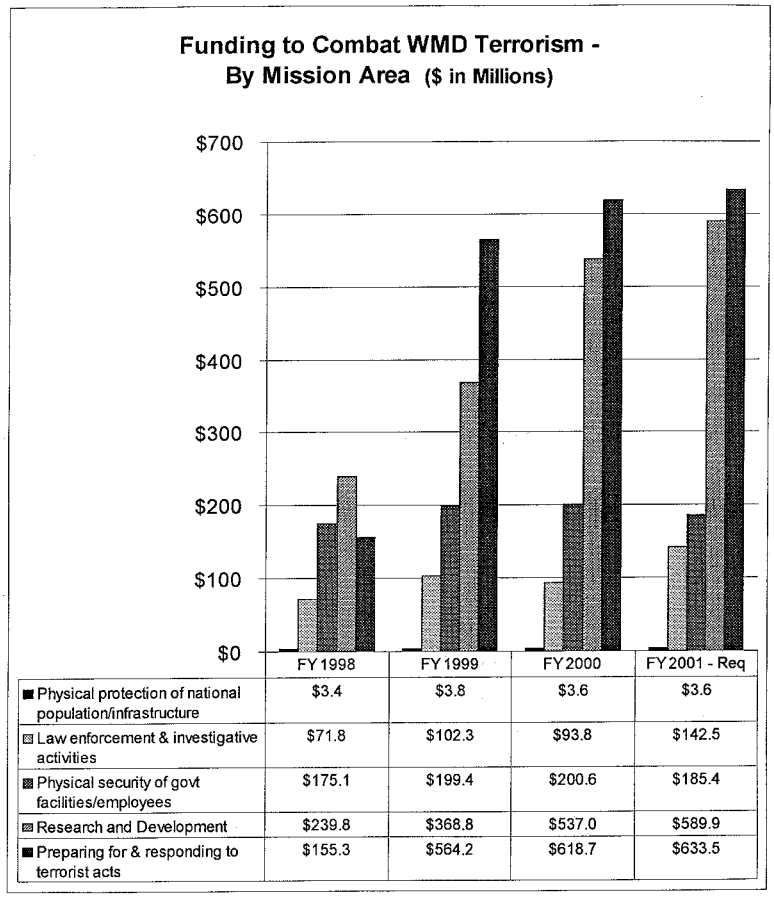
Figure 1:



	FY 1998	FY 1999	FY 2000	FY 2001 - Req
WMD Terrorism	$645.3	$1,238.4	$1,453.7	$1,555.0
Non-WMD Terrorism	$5,870.8	$7,518.9	$6,966.0	$7,756.3

All figures taken from Office of Management and Budget's *Annual Report to Congress on Combating Terrorism*, May 18, 2000.

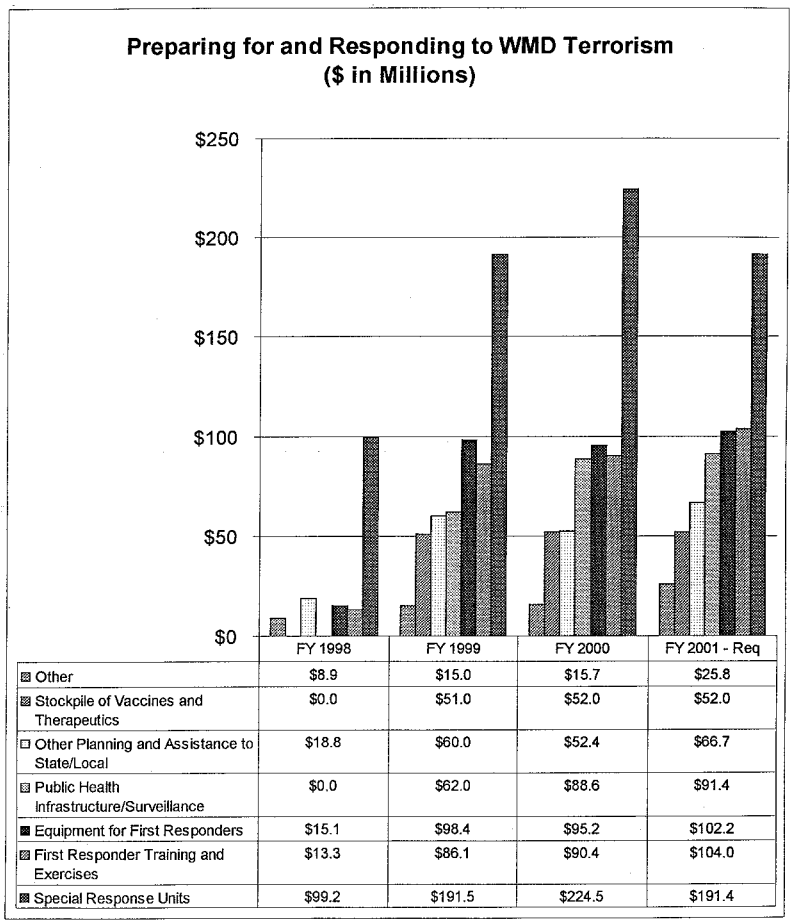
Figure 2:



	FY 1998	FY 1999	FY 2000	FY 2001 - Req
Physical protection of national population/infrastructure	$3.4	$3.8	$3.6	$3.6
Law enforcement & investigative activities	$71.8	$102.3	$93.8	$142.5
Physical security of govt facilities/employees	$175.1	$199.4	$200.6	$185.4
Research and Development	$239.8	$368.8	$537.0	$589.9
Preparing for & responding to terrorist acts	$155.3	$564.2	$618.7	$633.5

All figures taken from Office of Management and Budget's *Annual Report to Congress on Combating Terrorism*, May 18, 2000.

Figure 3:

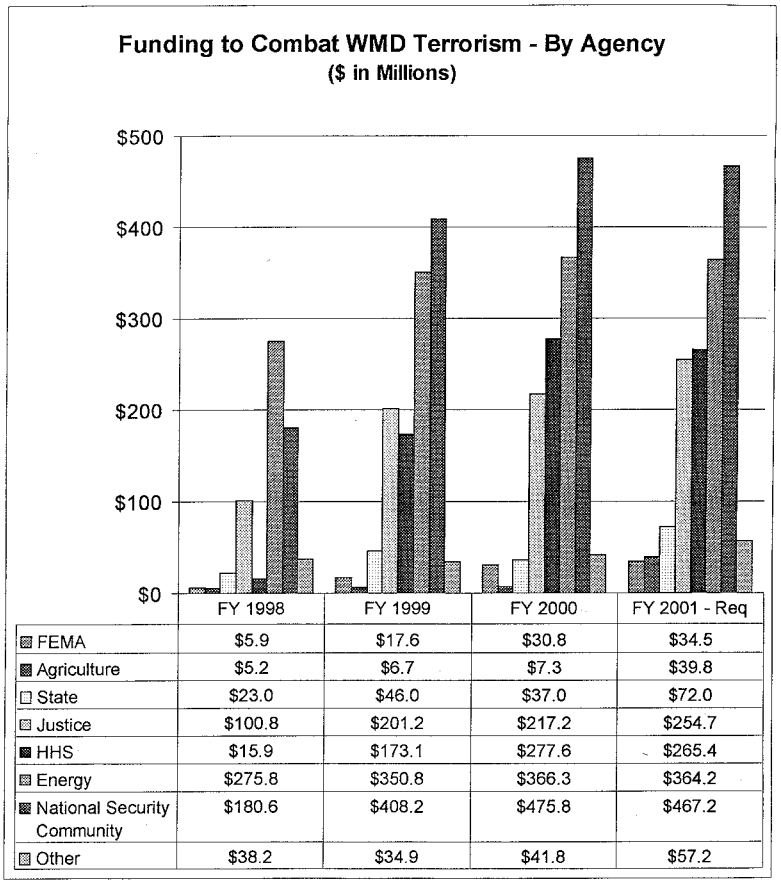


	FY 1998	FY 1999	FY 2000	FY 2001 - Req
Other	$8.9	$15.0	$15.7	$25.8
Stockpile of Vaccines and Therapeutics	$0.0	$51.0	$52.0	$52.0
Other Planning and Assistance to State/Local	$18.8	$60.0	$52.4	$66.7
Public Health Infrastructure/Surveillance	$0.0	$62.0	$88.6	$91.4
Equipment for First Responders	$15.1	$98.4	$95.2	$102.2
First Responder Training and Exercises	$13.3	$86.1	$90.4	$104.0
Special Response Units	$99.2	$191.5	$224.5	$191.4

"Other" consists of Federal Planning Exercises, Medical Responder Training and Exercises, & Other

All figures taken from Office of Management and Budget's *Annual Report to Congress on Combating Terrorism*, May 18, 2000.

Figure 4:

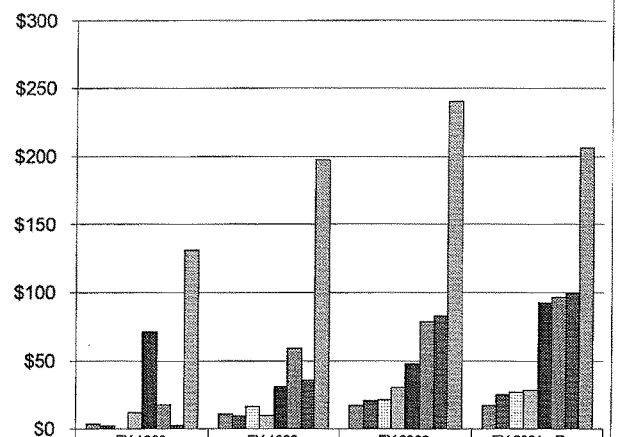


	FY 1998	FY 1999	FY 2000	FY 2001 - Req
FEMA	$5.9	$17.6	$30.8	$34.5
Agriculture	$5.2	$6.7	$7.3	$39.8
State	$23.0	$46.0	$37.0	$72.0
Justice	$100.8	$201.2	$217.2	$254.7
HHS	$15.9	$173.1	$277.6	$265.4
Energy	$275.8	$350.8	$366.3	$364.2
National Security Community	$180.6	$408.2	$475.8	$467.2
Other	$38.2	$34.9	$41.8	$57.2

"Other" consists of Commerce, EPA, Interior, NRC, Transportation, Treasury, and USAID

All figures taken from Office of Management and Budget's *Annual Report to Congress on Combating Terrorism*, May 18, 2000.

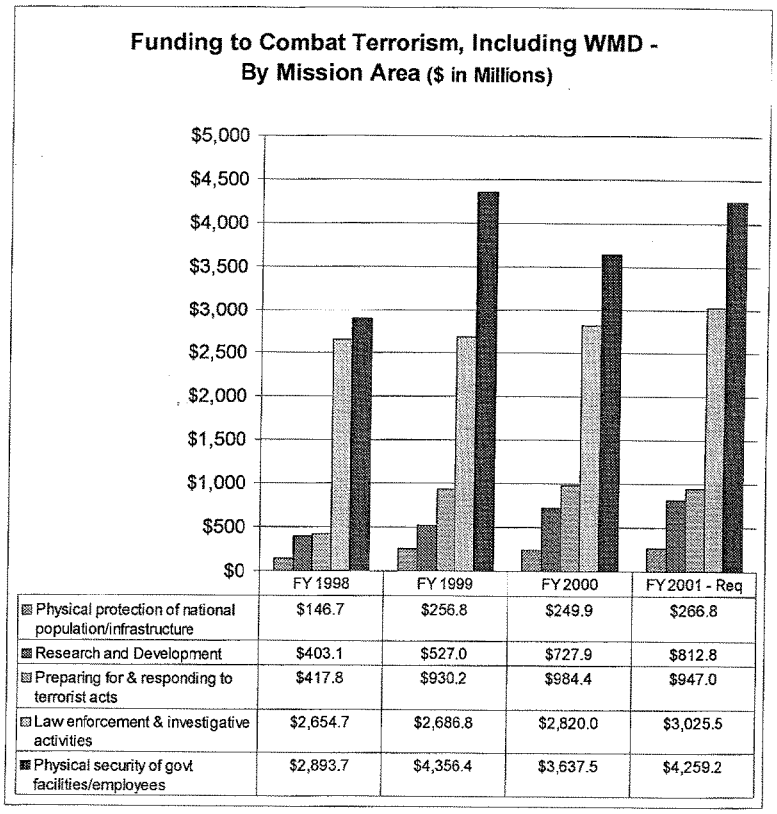
Figure 5:



	FY 1998	FY 1999	FY 2000	FY 2001 - Req
Modeling, Simulation, Systems Analyses	$3.6	$10.6	$16.7	$16.7
Personal/Environmental Decontamination	$1.8	$9.3	$20.3	$24.2
Therapeutics/Treatments	$0.0	$16.0	$20.9	$26.6
Personal/Collective Protection	$12.0	$10.0	$30.0	$28.2
Basic Research, incl. Gene Sequencing	$70.5	$31.0	$48.0	$92.3
Detection/Diagnostics	$17.8	$59.0	$78.3	$97.0
Vaccines	$2.9	$35.7	$82.6	$99.2
Other	$131.2	$197.2	$240.3	$205.8

All figures taken from Office of Management and Budget's *Annual Report to Congress on Combating Terrorism*, May 18, 2000.

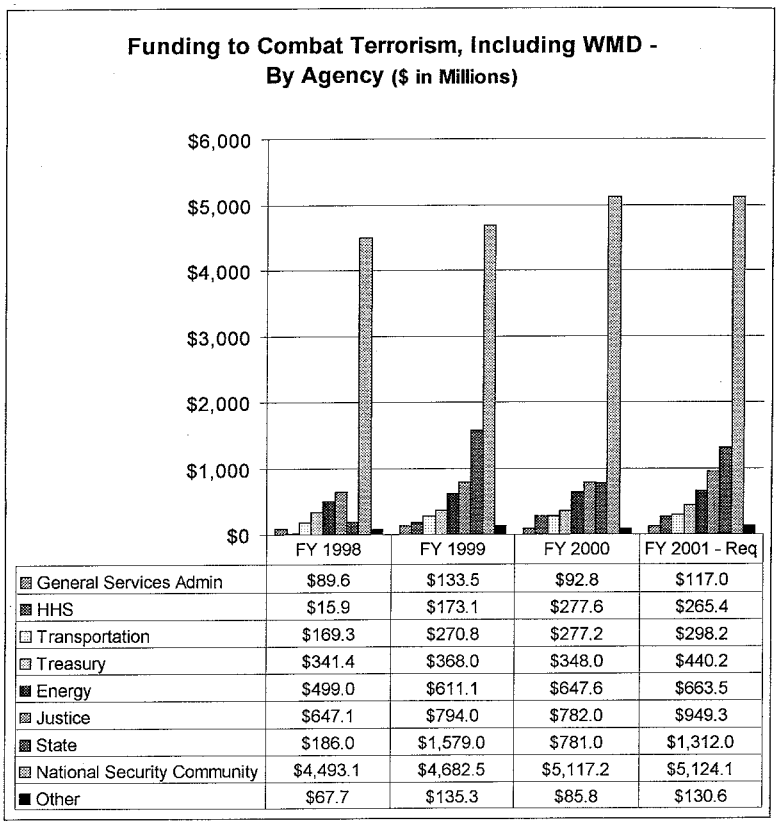
Figure 6:



	FY 1998	FY 1999	FY 2000	FY 2001 - Req
Physical protection of national population/infrastructure	$146.7	$256.8	$249.9	$266.8
Research and Development	$403.1	$527.0	$727.9	$812.8
Preparing for & responding to terrorist acts	$417.8	$930.2	$984.4	$947.0
Law enforcement & investigative activities	$2,654.7	$2,686.8	$2,820.0	$3,025.5
Physical security of govt facilities/employees	$2,893.7	$4,356.4	$3,637.5	$4,259.2

All figures taken from Office of Management and Budget's *Annual Report to Congress on Combating Terrorism*, May 18, 2000.

Figure 7:



	FY 1998	FY 1999	FY 2000	FY 2001 - Req
General Services Admin	$89.6	$133.5	$92.8	$117.0
HHS	$15.9	$173.1	$277.6	$265.4
Transportation	$169.3	$270.8	$277.2	$298.2
Treasury	$341.4	$368.0	$348.0	$440.2
Energy	$499.0	$611.1	$647.6	$663.5
Justice	$647.1	$794.0	$782.0	$949.3
State	$186.0	$1,579.0	$781.0	$1,312.0
National Security Community	$4,493.1	$4,682.5	$5,117.2	$5,124.1
Other	$67.7	$135.3	$85.8	$130.6

"Other" consists of Agriculture, EPA, Commerce, FEMA, Interior, NRC, USAID

All figures taken from Office of Management and Budget's *Annual Report to Congress on Combating Terrorism*, May 18, 2000.

Mr. SHAYS. Mr. Carus.

Mr. CARUS. Thank you.

Mr. SHAYS. Doctor, excuse me. I figure if you're a doctor, you deserve to be called that.

Mr. CARUS. Well, it's an honor to be asked to testify before your committee.

Mr. SHAYS. Thank you. It's an honor to have you here.

Mr. CARUS. My remarks today will concentrate on the threats and responses associated with potential terrorist use of chemical, biological, radiological and nuclear weapons, or, for convenience, CBRN weapons.

Let me emphasize that the remarks I'm going to make are my personal views and don't necessarily reflect the views of either the Department of Defense or the National Defense University where I work.

Let me extract three of the subjects that I discuss in more detail in my prepared testimony, first the threat from state use of CBRN weapons and how it should affect our view of response efforts; second, the potential for terrorist use of such weapons; and finally, how we should think about developing responses in this arena.

First I think it's important to keep in mind that the primary threat from CBRN weapons comes not from terrorists, but from hostile states. While there is considerable controversy about the prospects of terrorist use of such weapons, we know for certain that hostile states have acquired them, including several that the United States could face as military adversaries. For example, North Korea, Iran and Iraq are all assessed to have offensive biological and chemical weapons programs. Moreover the Department of Defense now believes that use of such weapons will be a likely condition of future warfare. So even if there were no terrorist threat, Defense would still need to make substantial investments in CBRN protection and mitigation capabilities.

There are numerous circumstances where it would make sense for a state to attack or threaten to attack targets within the territory of the United States. An adversary might attack air and sea ports of embarkation to prevent the United States from responding to attacks in distant theaters of operation.

Similarly a hostile state might believe that credible threats to employ such weapons especially against U.S. territory could deter the United States from intervening in their regions, making it safe for them to pursue aggression.

Because of the potential for asymmetric use of these weapons by state adversaries, threat assessments focused exclusively on terrorism provide a skewed view of the challenge and are of little value in determining the appropriate level of resources required for response. Needed CBRN response capabilities probably will not change depending on the character of the perpetrator. A terrorist use of the biological agent may look identical to a covert release engineered by the operatives of the state.

Let me now turn to a second issue, which is the threat posed by terrorist use of CBRN weapons. We must start with the assumption that our picture of the threat is incomplete and likely to remain so. The available evidence suggests it is extremely difficult to collect intelligence on some of these threats even when state pro-

grams are involved. As CIA Director George Tenet said earlier this year about chemical and biological weapons, there is a continued and growing risk of surprise. This reflects the difficult experience we have trying to uncover Iraq's programs despite highly intrusive inspections.

For this reason we must recognize that the absence of evidence is not proof of the absence of threat. Given the difficulties associated with collection in this arena, we must expect surprises. Hence the right answer is to develop policies that do not depend on the ability of the Intelligence Community to accurately assess what is probably a—what is almost certainly a low probability, but potentially very high consequence of that.

My views reflect some of the lessons of the research during the past few years on the illicit use of biological agents, and I'll make some specific comments about this. While the arguments apply to other so-called weapons of mass destruction, I'll admit they're primarily focused on the problem of bioterrorism. In terms of thinking about the threat, it's important to be clear that terrorist groups have shown limited interest in use of biological weapons, although there may be slightly more interest today than was true in the past. Thus, I've been able to identify fewer than 25 terrorist groups that are known to have shown any interest in biological agents. And only 751 people have ever been harmed in bioterrorism incidents.

Second, while most terrorists are not interested in causing mass indiscriminate casualties, there have been a few terrorists who did want to kill large numbers of people, and they were constrained not by moral or political imperatives, but lacked the technical capabilities to accomplish their objectives. Thus technical limitations have been the real barrier of past use of biological agents.

Contrary to views observe expressed that biological agents are trivial, easy to employ, it is still extremely difficult to develop an effective biological agent.

Finally, there is a prospect that some terrorist groups might acquire more robust capabilities in the future. The number of people with biological experience is growing, as is access to appropriate facilities. Moreover a dedicated, well-financed group might gain access to the needed technology from a state weapons program.

It is perhaps significant that every country on the list of state sponsors of terrorism has shown at least some interest in biological weapons, and some have large and active programs. These considerations suggest it will be difficult to precisely delineate the bounds of the threat. While a threat clearly exists, there's is no way to reliably estimate the probabilities of use.

Let me conclude by making a few comments about responses that are influenced by the preceding remarks. I strongly believe that policymakers, as I said, must be willing to make decisions regarding investments here, recognizing that they're not going to be able to have more than a general sense of what the threat is. As a result, there is a danger that we're going to spend too little and thus not have the required response capabilities, or spend too much and thus divert resources from other underfunded programs. For this reason I strongly believe that we should emphasize investments that will prove beneficial even in the absence of a CBRN attack.

A model for such a program is the Epidemic Intelligence Service, a component of the Centers for Disease Control and Prevention that investigates disease outbreaks in support of State and local governments. The EIS was created 50 years ago because of concerns that the United States might be subjected to a biological weapons attack. Since its creation it has never detected a biological warfare attack on the United States, yet the EIS more than justifies its existence by contributions to the Nation's health.

As it happens, much of the investment in CBRN response is being made in areas where it appears similar benefits will accrue. For example, CDC's Bioterrorism Preparedness and Response Program is devoting considerable resources to enhancing disease surveillance systems in public health laboratories. Strengthening these components of the public health infrastructure is certain to have a positive impact on the national capacity for responding to disease outbreaks. As a result many of the response investments will provide significant benefits even in the absence of the terrorism threat.

In conclusion, let me make two points. First, our response efforts must reflect the uncertainties that inevitably will accompany attempts to assess the threat. Second, we should ensure that our responses will have merit even in the absence of terrorist attacks, either because they have a positive impact on the health and well-being of the American people, or because they address other threats such as state use of CBRN weapons. We have more confidence in the quality of our threat assessments. Thank you for your time.

[The prepared statement of Mr. Carus follows:]

Testimony of W. Seth Carus

before the Subcommittee on

National Security, Veterans Affairs and International Relations

of the House Committee on Government Reform,

July 26, 2000

It is an honor to testify before this committee. The subject of this hearing, assessing the threat from terrorism and the appropriate responses to it, is an important one, and I am grateful for this opportunity to present my views. My remarks today will concentrate on the threats and responses associated with the potential terrorist use of chemical, biological, radiological, and nuclear weapons (or CBRN weapons).

Before continuing, let me note that my testimony reflects my personal views and does not necessarily reflect the views of the National Defense University or the Department of Defense.

In the next few minutes, I will address two main subjects. First, I will make a few observations about the nature of threat assessments and the relationship that they have to the consideration of responses. Second, I will discuss the nature of the appropriate responses to the challenges posed by CBRN weapons, including a few comments specifically aimed at the role of the Department of Defense.

Threat Assessments

Assessing the threat posed by terrorist use of CBRN weapons has proven to be a remarkably difficult process. During the past year, a contentious debate has developed over the likelihood and potential magnitude of the threat from terrorist use of CBRN weapons. Some analysts argue that there is no identifiable CBRN terrorist threat, while others contend

The views expressed in this testimony are those of the author and do not necessarily reflect the official policy or position of the Department of Defense or the U.S. Government.

that there is an imminent risk of catastrophic use of such weapons. This is not an academic debate, but, rather, one that has very concrete implications. How the policy community assesses the threat is likely to have profound consequences for calculating the appropriate level of resources needed to respond to CBRN use. For that reason, our answers must facilitate efforts to define the types and levels of resources need to be devoted to CBRN responses. Unfortunately, the debate has provided remarkably few insights to help the policy community in its efforts to determine the appropriate level of investment in preparing for CBRN responses.

Misconceptions about the Threat

Understanding of the threat from CBRN weapons continue to be undermined by the persistence of certain misconceptions about the nature of the threat. Specifically, many people appear to believe that the sole source of CBRN threats to the territory of the United States comes from terrorist groups. Thus, they seem to believe that we can determine the investments required for response capabilities simply by assessing the threat posed by terrorists. In addition, many people appear to believe that threat assessments are the same as intelligence analysis. While it is clear that intelligence forms an essential part of a threat assessment, it is not the only significant input and may not even be the most important.

Terrorists are not the main threat

Let me start by addressing the misconception that terrorists are the only relevant threat.

The primary threat from CBRN weapons comes not from terrorists but from hostile states. While there is considerable controversy about the prospects for terrorist use of CBRN weapons, we know for certain that hostile states have acquired these weapons to threaten and/or use against the U.S. military and the territory of the United States. The Soviet Union had a massive biological weapons program targeted at the United States, including pathogens aimed at both our people and our agriculture sector. Currently, there are at least a dozen countries with BW programs, including several that the United States could face as military adversaries. For example, North Korea, Iran, and Iraq are all assessed to have offensive biological weapons programs.

For the Department of Defense, the acquisition of chemical and biological weapons capabilities by hostile states in regions of vital interest to the United States has profound implications. Defense now believes that use of such weapons will be a likely condition of future warfare. Even if there were no terrorist threat, Defense would still need to make substantial investments in CBRN protection and mitigation capabilities. These include passive and active defenses, as well as counterforce capabilities designed to defeat the CBRN threat.

It is highly unlikely that hostile states will restrict their use of chemical and biological agents to targets outside the territory of the United States. There are numerous circumstances where it would make sense for a state to attack or threaten to attack targets within the United States. It is possible, for example, that an adversary might attack air and sea ports of embarkation to prevent the United States from responding to attacks in distant theaters of operation. Thus, the 1999 Pope-Bragg Study demonstrated that a chemical or biological agent attack on Fort Bragg and Pope Air Force Base would significantly delay the ability of U.S. power projection forces to deploy overseas. Similarly, a hostile state might believe that credible threats to employ CBRN weapons, especially against U.S. territory, could deter the United States from intervening in their regions— making it safe for them to pursue aggression. Moreover, North Korea might view threats to employ CBRN weapons as a regime survival mechanism in the event that it saw itself losing a war on the Korean peninsula.

Many argue that no adversary would dare target the United States, apparently believing that the leaders of hostile states would fear the potential U.S. response to such use. While it is true that the United States has military capabilities, including its nuclear deterrent, that will give pause to any aggressor, there is legitimate reason to worry that we may not be able to deter use of CBRN weapons. The conditions for deterrence are significantly different today than they were during the Cold War. The states of current concern, such as North Korea or Iraq, differ in significant ways from the Soviet Union. Their leaders may be more prone to risk taking than was the Soviet leadership. Certainly, an adversary who believed that we threatened the very survival of their regime is likely to have few qualms about threatening to attack U.S. territory. A hostile state also might calculate that it possessed escalation

options of its own, and thus come to believe that it could deter the United States from retaliation involving a full range of military responses.

Threat assessments focused exclusively on terrorism provide a skewed view of the challenge and are of little value in determining the appropriate level of resources required for resources. Many critics of current CBRN response efforts appear to believe that since they can identify no CBRN terrorism threat, responses must be a waste of money. This view is clearly misguided, and potentially dangerous. CBRN response capabilities do not change depending on the character of the perpetrator. A terrorist use of a biological agent may look identical to a covert release engineered by operatives of a state. Hence, steps taken to deal with the terrorist threat will also deal with the state challenge, just as efforts aimed primarily at state threats will have utility in dealing with terrorist actions.

Threat assessments are not just intelligence assessments

Let me now turn my attention to a second misconception about CBRN threat assessments, that the primary focus of threat assessments is intelligence analysis.

Clearly, we want to rely on accurate and detailed intelligence analyses to guide decision making. Unfortunately, the intelligence community cannot always provide that type of information. This problem becomes more evident in specific areas where the intelligence community may find it difficult to collect critical types of data. CIA Director George Tenet made some significant observations on this point in Congressional testimony earlier this year. He told the Senate Foreign Relations Committee, "Biological and chemical weapons pose, arguably, the most daunting challenge for intelligence collectors and analysts." For this reason, he added, "There are, and there will remain, significant gaps in our knowledge. As I have said before, there is continued and growing risk of surprise."

I cite these words because they provide some perspective on a key issue in this arena. Threat assessments consist of several components, reflecting both an understanding of adversary capabilities and intentions (which includes his understanding of his own capabilities) and an evaluation of the impact of those capabilities on friendly forces and intentions. Although the process necessarily includes intelligence collection and analysis, it encompasses additional elements, including analyses of response capabilities and an understanding of the potential impact of the adversary's activities. Finally, threat assessments

cannot reflect a linear extrapolation from past possibilities. This is especially true in an area as scientifically dynamic as biological warfare. There is little doubt that the challenges we will face in the coming decades will differ radically in important respects from the ones that we have had to deal with to this time.

Threat assessments always involve analyses that go beyond the data that the intelligence community is able to provide. When the intelligence information is insufficiently robust to prevent the possibility of surprise, those other inputs grow in importance. In terms of addressing the new kinds of threats that we expect to face in the future, we also need to incorporate three other kinds of assessment: scenarios, scientific bench-marking, and red teaming.

Scenarios are often used to help understand the potential impact of CBRN use. They permit exploration of alternative means of using such weapons, and help bound the problem, including by development of "worst plausible cases".

Scientific research can help establish a technical basis for evaluating the potential threat posed by particular capabilities developed by adversaries. This would include microbiological and medical research into the activities of particular organisms, as well as engineering research into the practicality of particular means for disseminating organisms. Scientific forecasting efforts would be needed to extrapolate the likely evolution of the threat out through the long-term planning horizons of DoD.

Finally, red teaming studies make it possible to assess the kinds of capabilities that groups may be able to obtain given certain constraints. Thus, by providing indications of what a terrorist group could credible accomplish with CBRN weapons under different circumstances, it is possible to provide an indication of what types of response capabilities may be needed.

Assessing CBRN Terrorist Threats

Let me now turn to the problem posed by terrorist use of CBRN weapons. This is an area rife with disagreements. Some analysts totally discount the threat, and argue that as a result the United States is grossly overspending on response efforts. Others contend that the challenge is far greater than often considered, and that insufficient resources are being devoted to the problem. The available evidence does not support either perspective.

The Absence of Evidence is not the Absence of Threat

Some experts have argued that there is no hard evidence to suggest that any terrorist is interested in CBRN weapons, and for this reason discount the whole threat. This argument is misguided. The absence of evidence is not proof of the absence of threat. The available evidence suggests that it is extremely difficult to collect intelligence on such matters. Even when state programs are involved, the intelligence community finds it extremely difficult to assess the scope of the threat that faces the United States. This is starkly evident from our experience with Iraq during the past decade. Especially in the biological weapons arena, but even in areas associated with chemical and nuclear weapons, it proved extraordinarily difficult to get an accurate picture of Iraqi activities. To this date, it is unclear that we know what capabilities Iraq possesses in the biological arena. The available evidence would tend to suggest that the difficulties are even greater when non-state actors are involved. The U.S. government only recognized Aum Shinrikyo's activities after the event. Indeed, even though it now appears that Aum targeted U.S. military installations in Japan, intelligence sources apparently provided no warning of the threat.

There is a real risk that we will expect too much from the intelligence community. Certainly, we would hope that they would discover reliable and complete information about terrorist involvement with CBRN. And it is clear that the U.S. government is doing a much better job of addressing this problem today than it did prior to the Aum Shinrikyo attack. Hence, there is a greater probability that activities like Aum's would now be detected. But given the difficulties associated with collection in this arena, we must expect surprises. Hence, the right answer is to develop policies that do not depend on the ability of the intelligence community to accurately assess what is almost certainly a low probability, but very high consequence event.

Lessons from the History of Bioterrorism

My views on this subject are largely molded by my research during the past three years into the illicit use of biological agents by terrorists and criminals. While the arguments apply in part to the other so-called weapons of mass destruction, they are primarily focused on the problem of bioterrorism.

First, it is clear that in the past there was limited interest by terrorist groups in use of biological weapons. Thus, fewer than 25 terrorist groups are known to have shown any interest in biological agents, no more than eight are known to have acquired biological weapons, and only five are believed to have employed them. There are only two instances in which groups caused harm. In total, only 751 people have been harmed in bioterrorism attacks; no one is known to have died. The simple reality is that most terrorists have never been interested in biological weapons.

Second, while most terrorists are not interested in causing mass, indiscriminate casualties, there have been a few terrorists who wanted to kill large numbers of people. These terrorists were not constrained by moral or political imperatives. Rather, they failed to achieve their goals because they lacked the necessary technical capabilities. In this sense, the mere existence of a group like the Aum Shinrikyo, which was responsible for the Tokyo sarin attack, demonstrates that groups can exist that will want to inflict mass casualties.

Third, technical limitations have been the real barrier to past use of biological agents. Contrary to views often expressed that biological agents are trivially easy to employ, it is still extremely difficult to develop an effective biological weapon. The technical information needed to produce an effective weapon is not widely available on the Internet, as often claimed. Clearly it is possible to create such capabilities, and the technology involved is not new: the United States had effective biological weapons capable of causing mass casualties in the 1960s. Yet, there is no reason to believe that such capabilities are currently available to non-state actors.

This experience appears to suggest that those attempting to generate threat assessments face particularly difficult challenges. Only a small percentage of terrorist groups are likely to develop an interest in CBRN weapons, and the groups that do may have unconventional characteristics that make it difficult to identify them.

There is also the possibility that state sponsors of terrorism could provide capabilities to terrorist organizations. Significantly, five of the seven countries on the State Department list of state sponsors of terrorism are known to have offensive biological weapons programs, and there are serious concerns about the other two. There is no evidence to suggest that any state has transferred CBRN capabilities to a terrorist group. Moreover, concerns about potential misuse of such weapons will tend to limit the willingness of most

states to provide such types of assistance. On the other hand, there are suggestions that some state sponsors of terrorism have been willing to provide terrorists with training on subjects related to CBRN weapons. And, it is possible to imagine certain circumstances in which a state might believe it to be in their interest to support terrorist capabilities against the West, especially if they believed it could be done without being traced back to the source. Syrian support for those responsible for attacking the Marine barracks in Lebanon certainly indicates that some countries are willing to support terrorist activities intended to inflict mass casualties on Americans.

How to Assess the Threat

What to make of these observations about the nature of the terrorism threat?

It is impossible to precisely delineate the bounds of the threat through traditional intelligence means. While a threat clearly exists, there is no way to reliably estimate the probabilities of use. For this reason, policy makers must be willing to make decisions regarding investments in responses without precise threat assessments. This leads to a danger that we will either spend too little, and thus not have the required response capabilities, or spend too much and thus divert resources from other under funded programs.

Responding to the Challenge

How should the United States as a nation respond to a threat of uncertain dimensions? There are two aspects to this problem: calculating the extent of the resources needed, and determining the character of the responses that ought to be developed. There are methods for thinking about the problem even in the absence of robust threat assessments.

Invest in dual use capabilities

As a starting point, we should emphasize investments that will prove beneficial even in the absence of a CBRN terrorist attack. The model for such a program is the Epidemic Intelligence Service (EIS), a component of the Centers for Disease Control and Prevention that investigates disease outbreaks in support of state and local governments. The EIS was

created fifty years ago because of concerns that the United States might be subjected to biological weapons attacks. Hence, it was thought that an ability to investigate unusual disease outbreaks was essential. Since its creation, the EIS has never detected a biological warfare attack on the United States, yet it has conducted thousands of investigations that have strengthened public health. While it remains an integral component of our national response to biological agent use, the EIS more than justifies its existence by its contributions to the nation's health.

As it happens, much of the investment in CBRN response is being made in areas where it appears similar benefits will accrue. The Domestic Preparedness Program, which was created to enhance the ability of cities to respond to chemical and biological threats, has enhanced the ability of those cities to address any incident that causes mass casualties. Moreover, it has enhanced the readiness of the cities to respond to hazardous materials incidents. Similarly, much of the spending by the Department of Health and Human Services will go to create capabilities that will benefit the country on a regular basis. Hence, CDC's Bioterrorism Preparedness and Response Program is devoting considerable resources to enhancing disease surveillance systems and public health laboratories. Strengthening these components of the public health infrastructure is certain to have a positive impact on the national capacity for responding to disease outbreaks. Similarly, the National Disaster Medical System has been strengthened by the investments in CBRN response, which means that it is better able to address other kinds of medical emergencies. These types of investments are not dependent on the specific character of the CBRN terrorism assessment, and many could be justified simply on the basis of the benefit that they will provide to the public on a routine basis.

In addition to activities that will have public benefit even in the absence of bioterrorism attacks, there are capabilities that are needed to respond to the potential use of CBRN weapons by state adversaries. A classic example is provided by the Department of Agriculture's bioterrorism response program. In the past, the United States virtually ignored this threat. Hence, it is ironic that during the Cold War the United States devoted virtually no resources to protecting agriculture from biological attacks, even though the we now know that the Soviet Union had a massive anti-agriculture program. Since other states are also

known to have worked on biological agents for use against agriculture, it could be argued that a response program is needed even without a terrorist justification.

In the final analysis, many of the investments being made to respond to CBRN threats are actually addressing fundamental deficiencies in the national infrastructure. Accordingly, many of the investments will provide significant benefits even in the absence of a terrorism threat.

Admittedly, there are some investments being discussed that cannot be justified on the basis of providing dual-use capabilities. The pharmaceutical stockpile program clearly falls into this category. Thus, it is difficult to find a rationale for resuming production of smallpox vaccine on the basis of dual-use requirements. The vaccine is needed if and only if someone releases smallpox back into human populations. Although there has been considerable attention given to the danger that terrorists might take such steps, it is clearly an extremely low probability event, but with extremely high consequences.

There is, however, a second way to look at the dual-use criteria. Capabilities that are needed to respond to known and likely state biological weapons capabilities also should fall into this category. The Soviet Union is known to have adopted smallpox as a biological agent, and there is every reason to believe that Russia also may retain it as a military weapon. In addition, others states are suspected of possessing smallpox and some are thought to have adopted it for use as a military weapon. Hence, there is a clear need to maintain response capabilities against smallpox that have nothing to do with the terrorist threat.

The Role of DoD

Let me conclude with a few observations concerning the Defense Department's CBRN response role.

During the past four years, Defense has become increasingly concerned about its ability to respond to use of CBRN weapons. Consequence management activities in support of civilian authorities have received growing attention. The Department has created the Office of the Assistant to the Secretary of Defense for Civil Support and has established a Joint Task Force for Civil Support. It also has organized Civil Support Teams within the National Guard. In addition, many Defense organizations possess specialized capabilities that would contribute to consequence management responses.

There is a real danger, however, that resources devoted to support for civil authorities may come at the cost of capabilities needed to execute Defense's core warfighting mission. Defense developed CBRN capabilities to support its warfighting activities and, in the view of at least some observers, has insufficient capabilities to address the challenges it may face from hostile military forces. Given that chemical and biological weapons are now seen to be likely conditions of future conflict, diversion of CBRN response assets to support the domestic consequence management responses could undermine the ability of the military to fight wars. In addition, it is important to recognize that while Defense can make significant contributions to civilian needs, the military also may need to call on civilian resources.

In particular, the focus of future Defense Department investments in consequence management should be installation preparedness. Many military bases are unprepared to respond to CBRN attacks, especially those located in the United States. Indeed, many are less well prepared than nearby communities. Should adversaries target certain key installations, the ability of the United States to support overseas operations could be severely degraded. It is critical that we address this deficiency with the same urgency assigned to the Domestic Preparedness Program that has enhanced the capabilities of the country's largest cities. Such a program would have ancillary benefits for the nearby civilian communities, because it would enhance the ability of Defense to execute consequence management responses in support of civil authorities.

Conclusion

In conclusion, let me reiterate four points.

First, the threat from CBRN weapons is not limited to terrorists. Thus, the development of responses should not be based solely on the assessment of the terrorist threat. From this perspective, those who argue that we are spending too much to enhance CBRN response capabilities are wrong. The United States must worry about the potential state use of CBRN weapons. For that reason, we have a clear need to develop robust CBRN response capabilities independent of the terrorism threat.

Second, it is difficult to precisely define the probability that terrorists may acquire and use CBRN weapons. We know that some terrorists have shown interest in such

weapons, and that some have unsuccessfully tried to use them in the past. It appears that technical constraints have been the key factor accounting for the failure of such groups to cause mass casualties. There is reason for concern that this will not remain the case. In addition, it is possible that terrorists might obtain CBRN capabilities from state sponsors of terrorism.

Third, many of the responses to use of CBRN weapons depend on the capabilities of federal, state, and local emergency management agencies and public health organizations. As a result, investments needed to address consequence management requirements usually reflect underlying weaknesses in government response capabilities. For this reason, much of the funding for consequence management activities, whether aimed at chemical or biological terrorism, will have benefits even if such attacks never occur. Moreover, consequence management capabilities to address CBRN terrorist incidents will also be available to tackle attacks mounted by hostile states.

Finally, the Department of Defense plays a critical role in supporting national efforts to respond to CBRN terrorism. It possesses unique capabilities for dealing with such threats. It is appropriate that such capabilities be viewed as part of a national system for confronting CBRN threats. At the same time, we must be careful that we do not undermine Defense's critical warfighting role. While there are many agencies at the federal, state, and local level that have capabilities to respond to CBRN events within the territory of the United States, only Defense is capable of fighting hostile military forces. At the same time, Defense needs the resources to enhance the preparedness of key military installations. Targeted investments in installation-based consequence management capabilities would enhance Defense's ability to support its wartime missions and provide support to civil authorities. Unless efforts are made to target Defense investments in such programs, there is a real danger that Defense assets essential to support the warfight might be diverted, unnecessarily, to domestic response missions. This is clearly not in our national interest.

Mr. BLAGOJEVICH [presiding]. Thank you very much, Doctor, and all of you, for coming to testify today. I'd like to begin by asking Dr. Carus a couple of questions.

Doctor, in our closed session earlier today with the FBI, they testified that they avoid all-encompassing national threat and risk assessments because they view them as inherently too broad-based to be of much practical value.

My question to you is do you believe it would be possible or of any use at all to attempt a single comprehensive threat and risk analysis that encompasses all risks to U.S. interests, whether they be military, international and domestic?

Mr. CARUS. I think there clearly is an ability to create threat assessments that are more encompassing. I do agree with some of the statements made earlier that that comment reflects a cultural perspective that comes out of the background of the Bureau, which is not used to making these sort of broad, all-encompassing assessments.

I would point out, however, that while in the national security arena we're much more comfortable with making those assessments, they're not necessarily silver bullets. I mean, as one looks at the track record of the Intelligence Community there assessing foreign threats, the estimates are often wrong in significant ways. So while they help bound the problem, they don't solve the difficulties of uncertainties about what really is happening. And so, you know, as I said, they're not a silver bullet, but they do at least help bound the problem in a useful way.

Mr. BLAGOJEVICH. OK. Mr. Parachini, Dr. Carus made a point. Would you like to give us a counterpoint on that?

Mr. PARACHINI. The one point that I would add is that the beauty of a communitywide intelligence assessment is that it forces all the different parts of the community to come to a common standard. There are some divisions within the community now on the magnitude of the CBRN threat, and one of the ways to get a consensus on that is to go through the process of forging a national threat assessment.

This is a different problem to conduct a national threat assessment on than it was the Soviet Union in the cold war or even North Korea's ballistic missile program now. There are not fixed things that you can look at with a variety of intelligence assets. It's a very fluid threat, so it's hard to get a sense about the nature of it. That doesn't mean that you don't try. That doesn't mean that you don't revisit it. That doesn't mean that you don't try and craft some standard of which evidence is to be evaluated.

Mr. BLAGOJEVICH. In your initial statement, Mr. Parachini, you suggest that increasing emphasis should be placed on the front end of the program through preemption of attacks and prevention of attacks; less emphasis should be placed on the back end of the problem with respect to the postattack consequences of management. How is it that you can make a proposal like that if the comprehensive threat assessment you recommend has not been done?

Mr. PARACHINI. Well, I think there are bits and pieces of a threat assessment out there. I think the Intelligence Community has that. We at the institute have been looking into all of the historically noted cases of chemical and biological weapons terrorism; inter-

viewing the terrorists, the law enforcement officials; reading the court record, everything the terrorists have written. And the magnitude of the threat we get from looking at the historical record looks different than that which we read about in the newspapers or hear from some public officials.

I'm not suggesting that we stop emergency preparedness. I think that's very important. I'm just suggesting that we try and have a few more tools such as diplomatic tools, law enforcement tools, and intelligence tools which cost less, and that we develop those a little more and not go overboard and spend so much money that we're having a little trouble keeping account of on the domestic preparedness side.

I think what Dr. Carus suggested about dual use investments on the preparedness side are very good, those things which help contribute to the Nation's public health, for example, but also give us the ability to address bioterrorism. Those are the examples of postevent investments that we should be making.

Mr. BLAGOJEVICH. Ambassador Bremer, I noticed the Congress and indeed even this committee did not escape the Commission's review. Your support—your report suggested that Congress should reform our system for reviewing and funding counterterrorism programs. And the point you have raised is a good one, which is that Congress ultimately has responsibility for doling out the money, so we should say how we want it spent and what we want it spent on. How can we organize ourselves here in the Congress to better execute the mandate you're suggesting?

Mr. BREMER. Well, we in our Commission made—we sort of wimped out actually, Congressman. We basically thought it was a bit presumptuous of us, even though we were a creature of Congress, to suggest how Congress organize itself. We suggested it, at least as a first step, that the appropriations committees in the two Houses of Congress ought to appoint senior staff members to do some work from both Houses and from both parties to do some sort of thinking through together about cross appropriations.

One could also suggest the relevant committees try to hold joint hearings, but that tends to not get very far up here, in my experience.

I think what we're really saying is this: The executive branch, in our view, is not ideally organized to fight terrorism. To some degree that is Congress's fault because you have these stovepipes in this town that run from various committees in Congress to various parts of the Federal—the executive branch, and those stovepipes tend to channel responsibility and budget authority particularly along very narrow lines, whereas if you're going to deal with terrorism as a national problem, whether it's on the basis of a national threat assessment or anything else, you're going to have to start cross-cutting at both ends of Pennsylvania Avenue.

Mr. BLAGOJEVICH. OK. I will ask Larry Halloran, the majority counsel, if he has any questions.

Mr. HALLORAN. Did you want to put this letter in first?

Mr. BLAGOJEVICH. Could I do that? Thank you very much, Larry.

What I would like to do is offer a letter and make this letter a part of the record. This is a letter that OMB has asked that we submit for the record to the subcommittee outlining their role and explaining their budgetary review process. So I'd like to offer this for the record.

Mr. HALLORAN. Nobody is going to object.

[The information referred to follows:]

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

July 26, 2000

The Honorable Christopher Shays
Chairman
Subcommittee on National Security, Veterans Affairs
and International Relations
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman,

I commend your committee for holding today's hearing on Combating Terrorism: Assessing Threats, Risk Management, and Establishing Priorities. I would like to take the opportunity to share our thoughts on this matter. We hope you will make them part of your record. As you know from our previous discussion, OMB has committed extensive time and effort to improving management and funding of programs to combat terrorism, and we would have liked to continue our engagement with you on this issue. We know that your own interest matches ours, and welcome any future opportunities to continue the discussion.

An Architecture for Combating Terrorism

In the spring of 1998, the Administration began the creation of an interagency process to enhance coordination of efforts to combat terrorism with the issuance of two Presidential Decision Directives (PDDs). PDDs 62 and 63 set out the roles and responsibilities of the many U.S. agencies involved in combating terrorism and the cyber threat and created a new and more systematic approach to fighting emerging threats. The PDDs established interagency working groups, as well as the position of the National Coordinator for Security, Infrastructure Protection and Counter-terrorism, to coordinate development and implementation of policies and programs. We have been working to implement and refine this architecture since then.

The interagency process, led by the National Coordinator, embraced a three-step approach to decisions for combating terrorism: first it analyzes the threat, relying on the combined judgment of both domestic and international intelligence agencies. Next, it develops suitable responses to that threat. Finally, it determines the appropriate agency and appropriate tools to carry out the response, with the associated resource decisions.

Threat Assessment

As noted above, the plan begins with analysis of the threat, relying on the judgments of both domestic and international intelligence agencies as to the assessment of the threat. This is an ongoing process, based in some cases on competing views of differing analysts, some of whom are witnesses before your committee today. We believe this approach is preferable to a formal, consensus assessment. Competing assessments of the terrorist threat are more likely to stimulate the creative thinking necessary to combat this unconventional national security challenge.

Establishing Government-Wide Priorities in the Budget Process

The Director of OMB recently submitted the "Annual Report to Congress on Combating Terrorism" which outlined the Administration's efforts to develop coherent strategies, manage interagency coordination, and create a comprehensive investment plan for combating terrorism. That document is the result of a recently established interagency budget review process (conducted by the PDD 62 and 63 working groups) developed to ensure that agencies structure their activities most effectively and efficiently to achieve a national program to combat emerging threats. This review process addresses many of the concerns expressed by Congress – and specifically by this Subcommittee – on the organization and management of terrorism programs.

The review process is intended to inform agency decision-making by providing agencies with a government-wide perspective on their own contributions to these efforts. The representatives from each relevant agency are subject matter experts, charged with reviewing the national effort to combat terrorism rather than simply their own agency efforts. In a constrained resource environment, the subject experts must prioritize programs across the government, not just within agencies, resulting in a comprehensive investment plan. The review process involves four phases:

Program Review: Interagency working groups, chaired by the National Security Council, review the crosscutting issues in a government-wide context. Strategic guidance is provided by Presidential Decision Directives 62 and 63. The Administration's "Five Year Interagency Counter-Terrorism Plan" provides more detailed guidance, setting goals and milestones for terrorism programs in each agency. The working groups--using intelligence assessments provided by the Intelligence Subgroup for each issue area--identify gaps and duplications in the national effort and develop detailed programmatic initiatives to increase our effectiveness in countering unconventional threats.

Budget Review: 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 the initiatives, but is instead an effort to provide realistic, well-justified cost estimates for them.

Agency Action on Recommendations: The working groups then prioritize the initiatives across the government and transmit them as funding recommendations to the agencies. Agencies address the recommendations in the context of other priorities and fiscal constraints in their fall budget submissions to OMB.

Review of Agency Action: OMB and NSC review agency action on the recommendations and make any necessary course corrections during the final decision-making by the President, based on information from the working groups, other agency priorities, and available resources. During implementation, OMB uses the apportionment process and execution reviews to ensure that Administration priorities--as set by the interagency review process--are followed.

Knowing the Subcommittee's interest in which office makes the final determination of how much money is given to an agency or program, the last two steps of the decision making process require some elaboration. In many cases, interagency support in the working group for an initiative is sufficient to convince agencies to adopt them and integrate them into their budgets. The reverse is also true: when it becomes apparent that a program is duplicated in another part of the government, agencies are usually more than willing to reallocate resources to other priorities. However, in some cases, the interagency advocates an initiative for which there is no clear "home" or recommends discontinuing an initiative supported by the host agency but which is lower in priority for the national program as a whole. In these cases, the debate is submitted for resolution in the standard OMB budget process and Director's Review and the initiative is added to the budget of an appropriate agency or funding is redirected.

Throughout the Administration hundreds of people have worked to develop and refine this process. We think it represents a substantial advance on previous policymaking. We hope for a continued dialogue between the Administration and Congress on how this process can be used to identify and fund the highest priorities for this critical issue.

Funding National Security Needs

In addition to its concerns about process, I hope your Subcommittee will also review the actual levels of funding for this effort.

Funding to combat terrorism continues to increase steadily. Over the past four years it has increased 40 percent to $9.1 billion. Funding for new missions such as WMD preparedness and critical infrastructure protection (CIP) has doubled in that time. The FY 2001 Budget proposes increases for each of these areas, which would bring WMD preparedness to $1.6 billion and CIP to over $2 billion. These funds willenhance ongoing efforts and launch new initiatives to strengthen our ability to deter and respond to attacks. We can also see the results of our enhanced coordination between agencies reflected in this budget request. The interagency budget review resulted in reallocation of resources--both within and between agencies--to fund critical shortfalls and eliminate duplication.

Regardless of any procedural suggestions the Subcommittee might make to improve management of terrorism programs, I urge you to underscore with your colleagues the need for increased funding for this critical issue. To date, a number of important initiatives have not been supported by the Congress in the appropriations process. Examples of such programs whose funding has been eliminated or dramatically reduced include:

- Department of State request of $30 million for a Center for Anti-Terrorism and Security Training and $239 million for embassy security construction in Kosovo and the Balkan region proposed in the emergency FY 2000 supplemental.
- Department of Justice request of $80 million for FBI counterterrorism and WMD initiatives which would improve State and local governments' ability to respond to potential terrorist acts.
- US Customs Service and US Secret Service request of $15.9M for air operations and interdiction teams to support their responsibility for providing air space protection program at high-profile, National Special Security Events.
- Immigration and Naturalization Service request of $39 million in the FY 2001 budget amendment for counterterrorism programs securing our borders.
- Federal Aviation Administration request of $49 million to improve information security at the FAA. Not only have the House and Senate denied the information security research projects, but the Senate reduced the funding level for FAA operations, which will reduce the Department's ability to counter information security threats for the second year in a row.
- Department of Agriculture request of $10 million to protect our agriculture against bioterrorism.
- In addition, the President proposed several new CIP initiatives to fund training and personnel improvements, improve intrusion detection capabilities and federal information systems readiness, identify computer security research and development shortfalls, improve agency vulnerability assessments and develop PKI programs. The funding for these, nearly $100 million in FY 2001 and $9 million in the FY 2000 supplemental, was not provided by the relevant House appropriations sub-committees.

If combating terrorism funding is considered in piecemeal fashion rather than as a comprehensive whole, we will have missed an opportunity to enhance the nation's security against this emerging -- and increasingly dangerous – threat. These programs, among others, received interagency support through the review process. We believe that the real value of that process is precisely to ensure that programs in one agency which have ramifications for programs in another agency are coordinated and funded -- to create a comprehensive, coordinated and effective national effort. The funding cuts threaten to undermine that effort.

Thank you for your continued interest in this issue. We hope for close cooperation between the Administration and the Congress to advance these critical national security interests we share.

Sincerely,

Joshua Gotbaum

Joshua Gotbaum
Executive Associate Director & Controller

Identical Letter sent to The Honorable Rod Blagojevich

Mr. BLAGOJEVICH. I got the gavel here. Nobody here to object. Oh, there he is. Perfect timing. I'm from Chicago. That's how we do things.

Mr. SHAYS [presiding]. Is a dead body going to ask a question?

Mr. BLAGOJEVICH. Not until after he votes. I already asked him to vote for me.

Mr. HALLORAN. Mr. Bremer, you said the Commission recommended—let me paraphrase—in effect that the FBI might need some sharing lessons. It has been noted in other forums as well. What—did the Commission come across any circumstances where the FBI really close-held information that might have been useful in the response scenario that you're aware of?

Mr. BREMER. We in the Commission did not come across those, but I've had the personal experience when I was in government of that happening. And I have to say I think in most cases the FBI is withholding the information for perfectly legitimate reasons, which is to protect the integrity of the evidence that they're collecting to make a case.

Mr. HALLORAN. That gets to my next point that you made and I think Mr. Wermuth made in his testimony as well is the difference between evidence and intelligence, and that the FBI as lead agency in domestic counterterrorism may not possess the skill sets necessary to perform the tasks they're being given. What other limitations besides a certain degree of justified paranoia does the FBI bring to the job that may hinder them in doing what they're being asked to do in this field?

Mr. BREMER. Some of the things are very mundane. For example, when an FBI in a field office in the United States interviews a terrorist suspect, he fills out a 301 interrogation form. The 301 form stays at the field office. It almost never comes to headquarters. There's simply no mechanism for it happening. One would imagine computers that would allow that to happen in these days and ages.

What we suggested was the FBI basically faces a comparable problem to the CIA. CIA collects intelligence abroad in which they must protect the sources and methods, but the intelligence has to be gotten around to the Intelligence Community and to decision-makers. CIA has resolved that problem across the years by developing a cadre of reports officers. These are specialized officers in the agency, stationed in the stations abroad and here at home, whose training and job it is to look over the intelligence and figure out how to disseminate it, how to make it clean enough to get out to the community.

FBI does not have a comparable reports officer function, and we suggest that such a function should be created with a special cadre in the field offices here, which would begin to break down the cultural barrier of seeing themselves only as investigators trying to make cases.

Mr. HALLORAN. Anyone else want to comment on that?

OK. In the letter from OMB that Mr. Blagojevich put in the record, with regard to threat assessments, OMB describes this as an ongoing process based on some cases of competing views of different analysts, some of whom are witnesses before your committee today. We believe this approach is preferable to a formal consensus assessment. Competing assessments of the terrorist threat are

more likely to stimulate the creative thinking necessary to combat this unconventional national security challenge.

Do you agree with that?

Mr. BREMER. Well, I actually do agree with the idea of having—I think you can have both again. I do not agree the objective of a national threat assessment should be consensus. There I disagree with Mr. Parachini. I do not think that should be the objective, because then I think you get pablum, which is what you basically get out of any group of people if you tell them they have to agree. But I don't see any reason why you can't have a national threat assessment where they have competing views where they are strongly felt.

Mr. HALLORAN. Anybody else?

Mr. PARACHINI. In this particular instance there on the threat, on the biological agents that the various intelligence portion of the Intelligence Community see as likely, there has been a division. And there has been—there have been two agencies that have held different views from other parts of the community. And so my question to OMB would be, well, when you see that, then how do you decide to make various spending decisions based on the split in the community on a key thing? You just go ahead? Which is what has been done in this instance. Or—and while I take Ambassador Bremer's point about the danger of consensus is that you get something that's not very meaningful, somehow on hard issues you do have to draw some conclusions. People have to bring their evidence forward, and there has to be some common agreement on hard problems, like agents in which we need to respond to in which we're going to invest billions of dollars in developing vaccines and antibiotics. Otherwise we're going to make huge investments on partial intelligence assessments that may or may not be correct in 10 years' time.

Mr. BREMER. I don't think that's the job of OMB. That is the job of somebody who's politically responsible to the Congress and the American people. He or she is going to have to sit down and look at those splits, and he or she is going to be held politically responsible to decide, OK, now agency A is right and agency B is wrong. But that's not the job of staff. That's not the job of somebody at the NSC who is not politically responsible. That is the job of somebody who has budget authority and political accountability up here.

Mr. CARUS. May I interject a common on this?

Mr. SHAYS. Lower your mic, Doctor. Just lower the mic. Thank you.

Mr. CARUS. Because I think an example that John Parachini mentioned merits a little bit of elaboration. If you think about whether or not we should invest money in certain kinds of vaccines, you would come up with a very different answer if you just looked at the terrorism issue as opposed to just looking at the broader biological warfare threat issue. If you were just concerned about terrorists, you probably would say that smallpox is probably not a very likely threat agent because of the difficulties of obtaining access to it. But if you shift the focus and say what is the overall national threat from states, you would discover that there certainly is at least one state and probably multiple states, including several that want to do us harm, that possess smallpox, and there-

fore, from that point of view, the fact that we have a deteriorating supply of smallpox vaccine should be of great concern.

I think if you go across the board, you would discover that if you broaden the focus from merely terrorism to the broader issue of potential use of some of these weapons against the United States either overseas or domestically, that you would come up with radically different answers about what's appropriate investment and responses.

Mr. HALLORAN. I'm not sure I took your point there. Who else would use them besides terrorists? State sponsors and individuals?

Mr. CARUS. A state might use them. The Soviet Union had, we were told, SS–18 ICBMs loaded with smallpox. We are told that other states that may want to prosecute wars against us, including places like North Korea, perhaps Iraq, perhaps Iran, may have smallpox. Clearly they have incentives that have nothing to do with terrorist modalities for using or threatening to use a weapon of this kind. As a result, clearly the United States, both in terms of national security and Department of Defense concerns, as well as the broader protection of the American people, have a legitimate concern about the potential use of this particular agent.

Mr. HALLORAN. Thank you.

Let me ask another point if I can start a little debate here in terms of the extent to which in this—attempt to kind of know the unknowable, the—that the past is prologue, that we can project from what has happened, how many people have been injured in terrorism in the last 10 years, for example, or how much—how many have ever been exposed to a biological agent or at least intentionally to do harm. To what extent should that inform threat assessments today? Or is it your perception that it could at least draw us back from worst-case scenarios to some degree?

Mr. WERMUTH. I don't think you'd want to rely exclusively on historical incidents in forming current threat assessments. You need to have that perspective because it's an indication of who has used agents in the past. Aum Shinrikyo, you want to know about those as a basis for forming some conclusions, but you wouldn't want to use that as the basis for the overall threat assessment, because too much is happening from the technological standpoint, from a biogenetic engineering standpoint. You can use the historical perspective to help form some basis for developing the way you conduct threat assessments perhaps, but you wouldn't want to use them necessarily, particularly the——

Mr. HALLORAN. It certainly could be a measure of the technical difficulty they face. I think we learned more about the difficulties of biological weapons from the Aum Shinrikyo, that is, from the potential lethality of a chemical weapons release in a subway system, did we not?

Mr. WERMUTH. No question about it.

Mr. SHAYS. Would you all comment on the concept of when you deal with states, deterrence usually has an impact. Does deterrence have an impact with terrorists?

Mr. BREMER. Mr. Chairman, we looked at this in the Commission in light of the changing threat because we believe that the threat is increasing from terrorist groups and less from direct states acting in terrorism. And I think you're right to say that in the last

20 years if there has been a decrease in overt state support for terrorism, it's really the result of a good comprehensive American leadership in fighting terrorism and in saying to states it can no longer be a justified way to conduct yourself in international relations to practice terrorism.

It's a little hard to find those same levers against these groups because you can't call back your Ambassador to Usama bin Ladin. We don't have an ambassador. You can't cutoff exports to him. We don't knowingly export to him. He's not very likely to be very moved by even the most eloquently phrased demarche from the United Nations.

So you really are pushed away from the classic sort of diplomatic and economic tools that we've used against terrorists for the last 20 years or so. And you therefore, in my view, have to pay more attention to intelligence, because the way you're going to be most effective against that guy is to know what his plans are, and the way to know what his plans are is to have a spy in his organization.

That's really the heart of the matter. If you want to save American lives, you have to get good intelligence on what the terrorist plans are. They are not likely to be, particularly the new kind of terrorist, very susceptible to the concept of punishment by the rule of law, because many of them are living for, as in Aum Shinrikyo, sort of an apocalyptic view of the world that is not very susceptible to our kind of reasoning. So I come back again and again to the need for good intelligence being the most effective way to fight these new terrorists.

Mr. WERMUTH. I would simply add I think there is some deterrent value in at least exhibiting an ability on behalf of ourselves as a Nation to respond if a terrorist incident does occur, that there is some deterrence value there. If it looks like we're well organized, if it looks like we have a good game plan, if it looks like we are prepared to react and to administer justice very swiftly and very surely, I think that can have a deterrent effect on terrorists even beyond what Ambassador Bremer has mentioned.

Mr. SHAYS. Any comments? Part of the reason I ask is that I find myself at these hearings thinking of a young man who ran against my predecessor years ago from Princeton who was able to go to the library and develop a feasible nuclear weapon that the experts looked at, and then they embargoed his—classified his basic term paper, but now we can get on the Internet and get information. And I just wonder if years to come we just—it won't be absolutely easy to make weapons of mass destruction. And then I just think of how you deal with the logic of that. Then I think of Beirut and the bombing of—the total destruction of the Marine barracks there. That individual was willing to drive the truck underneath and blow it up and himself with it.

So I just wonder, deterrence doesn't strike me as being particularly effective for someone that is willing to kill themselves. It may be with the people that are sponsoring them. So I think I'm getting—the bottom line is what I fear is actually true. We used to respond to terrorism by dealing with the state-sponsored organizations, and now we don't quite have that same leverage. Not a pretty thing. So your point is in dealing with intelligence. Then I think

that anyone who is willing to be a counter—a spy within an organization deserves the Medal of Honor, totally away from any resource dealing with crazy people, constantly in fear that he may be found or she may be found.

Mr. BREMER. Not even the Medal of Honor, but more importantly he deserves to get American money. The current arrangement, as you know, Mr. Chairman, as we discovered in our report, discourages the recruitment of terrorist spies. The current CIA guidelines discourage the recruitment of terrorist spies, which we think is a very serious flaw in the current counterterrorist strategy.

Mr. SHAYS. It's a bit off subject, but it's certainly something that's on subject in this committee. Maybe you could make the point in a little more depth.

Mr. BREMER. Until 1995, when the CIA wanted to recruit an asset, as they call it, in any field, they had a procedure to vet that asset involving both the station and, as appropriate, people in Washington. In 1995, new guidelines were promulgated——

Mr. SHAYS. By whom?

Mr. BREMER. By the DCI at that time—which had the effect of making it much more difficult to recruit any kind of an asset. We reviewed this rather carefully both in Washington and in the field with serving agents and with retired agents, with junior officers and station chiefs, and found that despite what the CIA says, the fact of the matter is these rules have the effect of discouraging the recruitment of terrorist spies. So we recommend that these guidelines be rescinded in respect to the recruitment of terrorist assets.

Mr. SHAYS. And?

Mr. BREMER. The CIA has publicly stated that they do not believe these guidelines have the effect of discouraging assets.

Now, I have profound respect for the Director of Central Intelligence, and I have told him what I would say to you to his face, which is I just think he honestly doesn't know what's happening out on point where these people are actually being recruited. The fact of the matter is young case officers are not encouraged to recruit terrorist spies, and I think that's a very serious problem.

Mr. SHAYS. I would agree.

What is the significance of overemphasis on a worst-case scenario? I mean, it's come up a few times. What are the distortions that result?

Mr. PARACHINI. Well, the most likely event that we're facing is some sort of tactical—actually the Intelligence Community has consistently said the most likely event is a high explosive. In the sort of unconventional weapons, the most likely event is a poisoning. And the consequences that occur are not in the thousand casualties or hundred casualties, they're in the tens.

I think one point the Gilmore Commission has made that is valuable on this, if you gear all of your preparation to this catastrophic attack, everything becomes a Federal event, and State and local resources are probably appropriate for most of the events that might occur. One.

Two, we might then start to focus too much of our attention in the first responder world to the agents that are those in the programs of nation states. That may be appropriate at some level. We want to take some hedge against that, smallpox and anthrax. But

the more likely thing to occur is for terrorists in our country or coming to our country to attack easy dual-use items, to get like tanks of chlorine or phostine or sodium cyanide, which are dual-use chemicals that are more readily available. So by doing these worst-case scenarios with these exotic nation state military program agents, we're focusing on the wrong thing.

Mr. SHAYS. OK.

Mr. PARACHINI. We have to do some focus on it because we have to take a hedge against it, but we need to shift the balance.

Mr. CARUS. May I add some comment, sir? I think it shows up in a great many areas if you're not careful about disaggregating the threat and not merely looking at worst-case scenarios. If you look at the issue of chemical threats, if the only focus is on the most lethal of military chemical agents, the nerve agents, what you lose track of is that the capabilities for responding to different kinds of chemical threats differs depending upon who you're looking at.

One of the reasons why I think people have overemphasized the Department of Defense responses is because they focused on this small category of military chemical agents, when, in, fact most Department of Defense units have little or in many cases no capability for dealing with the broader range of toxic industrial chemicals. If you focus more on the toxic industrial chemicals, you discover that the broader-based capabilities of civilian and hazardous material units, whether they're working for the Department of Defense or for a local fire department, become much more salient in terms of understanding the response.

Mr. SHAYS. Thank you.

I think one area, unless it leads to something else, and that is the statement was made maybe by you, Mr. Wermuth, that national strategy is essential, national threat assessment is part of that. Or maybe it was—I'm not sure which, but it was——

Mr. WERMUTH. I think it was John Parachini, but I certainly agree with that.

Mr. SHAYS. I just want to—this morning's hearing was not particularly satisfying, and I don't think any of you gentlemen were there, but the general sense was that I had—that's not something I can't disclose is there wasn't a buy-in into having a threat assessment, that that's kind of—it's an ongoing process, and we evaluate every day and so on.

I get the sense from that, and I want to get you to respond to that, that each agency in a sense thinks it has their threat assessment as it relates to them, but they don't get it all together and try to figure out how their threat assessment works with other agency threat assessments, and then a more universal threat assessment.

You all are looking at me like, what, is this guy crazy? You all were struggling to understand me, but I don't know if I made the point well.

Mr. WERMUTH. I think I understood, and I think there's a certain amount of validity to that observation. I believe that whether it's threat assessments or not or whether it's simply agencies assuming some scenarios and then using those scenarios to help inform the decisions about plans and resources, therein does lie the problem. If there is no comprehensive assessment that has been done that

is recognized to be the assessment of the Federal Government, then agencies are pretty much left on their own to do whether they call it threat assessments or simply scenario building for helping to establish programmatics and the application of resources.

That certainly is going on. I mean, HHS is an example of that on one hand; FEMA is another example, as you heard from GAO testimony before we came up here. So that's another good reason for the integrated threat assessment that has all of the players involved.

And I just, from my perspective, make one other comment. You know, there is an obligation, too, for the government, particularly the national government, the Federal Government, to inform the American people about what the levels of threats—and I always use that plural, because there's no single threat—what the threats are. And without that good comprehensive threat assessment—right now the American people are basically informed by the entertainment media and the news media, if you can tell them apart, with these catastrophic kinds of events. And if that's not the real situation, then we ought to do a better job of letting the American people know what the probabilities of threats are and how they might be expected to respond in the event that an incident does occur across an entire spectrum of potential threats.

Mr. SHAYS. OK.

Mr. PARACHINI. I might add that the discussion on national missile defense and the threats we face from the ballistic missile programs of Iran and North Korea are helpful here. There have been very different views at different stages in this debate on the threat we face with missiles. Eventually there have been a number of communitywide assessments. There were then special panels and commissions that reviewed those assessments. I think all of that created a basis that was helpful for forging a national consensus on what to do, and I think if indeed we believe this problem is of that magnitude of a national security threat, then we should go through a similar process, because I think it benefited our decisions on national missile defense considerably. Might also benefit our decisions here.

Mr. SHAYS. Thank you.

Ambassador, when I was thinking of your earlier work as Ambassador-at-large on terrorism——

Mr. BREMER. Counterterrorism.

Mr. SHAYS. Counterterrorism. Sorry. Sorry. Sorry. So we don't have such an office.

Mr. BREMER. The President used to make that mistake very often by introducing me as his expert on terrorism. I'm counterterrorism.

Mr. SHAYS. I'm in good company then. Did you quickly correct him, or were you a little more subtle?

Mr. BREMER. No, sir, I wasn't.

Mr. SHAYS. Did that just all of a sudden—was that an office that was created out of the State Department's sensing a need, or had it existed for a long period of time?

Mr. BREMER. No. It has a long and rather sorry story. There was an office created in the State Department in 1972 to deal with terrorism, which was buried down to the bureaucracy. When Vice

President Bush chaired a commission at the President's request in 1985 to examine how we were structured in the government to fight terrorism, one of the recommendations of that commission was that there should be a clear agency function for State overseas and for Justice in the United States—that's still with us—and that the State Department should upgrade the office to an ambassador-at-large position reporting to the Secretary of State, and that office was then created. I was honored to be the first and, in fact, only—the only incumbent, because after the Reagan administration the office has been progressively downgraded. But in any case, that's where it comes from.

Mr. SHAYS. Well, I don't have any other questions. I would invite you if you had a question that we should have asked or wish we had asked, I would invite——

Mr. BREMER. May I make one point? It seems to me there are a couple of things that——

Mr. SHAYS. Excuse me. You did not have any questions?

Mr. RAPALLO. Maybe just one.

Mr. SHAYS. Let me have you respond, then I'll go to David.

Mr. BREMER. There are a couple of things that, irrespective of whether there's a national threat assessment, Congress could do to deal with terrorism. One of them, which we recommended in our report, is to control biological pathogens better. The principle should be that biological pathogens in this country should be as tightly controlled as nuclear agents have been for the last 50 years. Currently that is not the case.

I don't know where the legislation stands. Maybe one of my colleagues does now. There is legislation floating around to make it, in effect, illegal to possess biological pathogens unless you've got a legitimate need to have them. That is not against the law right now.

Second we recommended—as many of my colleagues have said, it's not as easy to make a biological weapon as some people would lead you to believe. You need very specialized equipment, you need fancy fermenting equipment, you need aerosol inhalation chambers, you need cross-flow filtration equipment. That equipment is now controlled for export by the United States, but it is not controlled for domestic sale. We recommended in our report that Congress should look into controlling that.

It seems to me these are good things to do irrespective of whether you have a national threat assessment, whether you have three national threat assessments.

Finally, as Dr. Carus pointed out, it ought to be possible to look for things which are dual use, and we recommended one, which is perhaps of interest to you, Mr. Chairman, right now, which is the question of surveillance by the CDC. You have the West Nile fever back upon you again in Connecticut. The CDC has a national surveillance system. It is not modernized. It's not computerized. And there is virtually no such system overseas.

It seemed to us we would want to know if West Nile fever was here whether it's here because you got dead crows or because somebody put it there. We would want to know if there was an outbreak of ebola that might be coming our way or of anthrax somewhere else.

There is no international surveillance system. This is something we have recommended that the Secretary of State and HHS should look into. These are things which, it seems to me, are pretty easy to do. They don't cost a lot of money. They're dual use. They're not dependent on a precise definition of what the threat is, but they are good things to do. I would just commend them to your attention Mr. Chairman.

Mr. SHAYS. It raises the point what committees did you present your report to?

Mr. BREMER. We actually presented the report to the Speaker and the Majority Leader. I have testified before a number of committees in both Houses.

Mr. SHAYS. Just totally focused on that report? In other words, the purpose of the hearing was for that report?

Mr. BREMER. Yes, sir.

Mr. SHAYS. Did you feel it got the kind of dissemination that you expected? I mean, was it——

Mr. BREMER. It got quite a lot of attention. Some of it was misdirected by some of the early news reports, but we got a very good reception, I must say, on both sides of the aisle in the report in general on all the committees I've been before.

Mr. SHAYS. Thank you.

Any other comment or question that we—question we should have asked that you needed to respond to or something that you prepared for that would be eloquent if you shared it with us? Nothing. OK.

Let me say—and I'm going to recognize David Rapallo—this has really been an excellent panel. Hopefully we'll be able to utilize your contribution in the future as well. It's been very interesting, and your statements were interesting; if not interesting in every respect, very informative and important for us to have. I'm talking about the written one. Your verbal one was very interesting.

Mr. RAPALLO. Just one quick followup for Ambassador Bremer. On the 95 CIA regulations I want to make sure there's a complete explanation, it didn't just happen in a vacuum. Could you give just a little description of why they were adopted, the rationale behind them?

Mr. BREMER. The given rationale was concerns that some assets who had been engaged by CIA in a country in Central America had been involved in alleged serious crimes. And there was a view at that time that the head of the CIA and the DCI, that this put us at risk by having assets who might have committed crimes or might have committed human rights violations. And it was in response to those concerns, as I understand it, that these guidelines were issued.

Mr. SHAYS. But the bottom line is you believe it's much harder to recruit.

Mr. BREMER. The DCI at the time and the DCI today maintain that the intention of these was not to discourage the recruitment of hard assets. We say we understand that. We're not challenging what the intention was, but the effect has been to discourage it.

Mr. SHAYS. David asked the question, that's on the record, but important that you tell us your concern as well. Gentlemen, very,

very interesting. I appreciate your participation as I did the panel before yours. Thank you very much, and at this point this hearing is adjourned.

Thank you for your help as well, Recorder.

[Whereupon, at 3:20 p.m., the subcommittee was adjourned.]

○