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

20000731 084

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

G A O
Accountability * Integrity * Reliability

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 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

[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.

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.

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

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

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

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.

Terrorist Face Significant Challenges to Using Some CBRN Materials

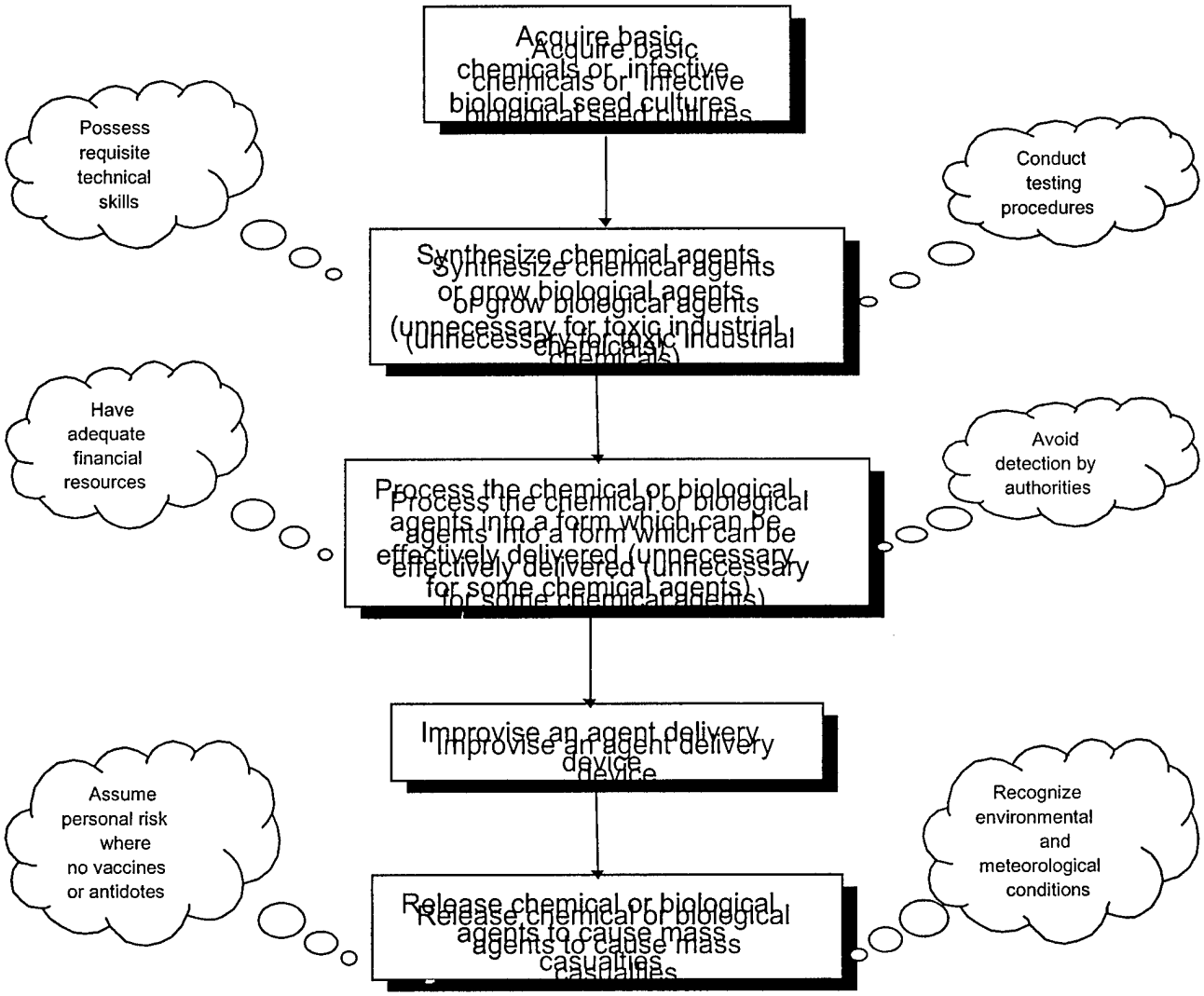
Some past public statements by intelligence agencies do not include the challenges that terrorists would face in using CBRN materials. Moreover, in open testimony and public documents, the CIA has indicated that it was relatively easy for terrorists to produce and use CBRN agents.[4] Our work—which examined 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

[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).

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.

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

[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).

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 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

[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.

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 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

[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).

[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).

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 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.

[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).

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 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

[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.

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).

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 Information

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 Programs

Contact one:

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

E-mail: fraudnet@gao.gov

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