United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Oversight, Investigations, and Emergency Management, Committee on Transportation and Infrastructure, House of Representatives

For Release on Delivery
Expected at 2:00 p.m.
Thursday,
April 6, 2000

COMBATING TERRORISM

Issues in Managing Counterterrorist Programs

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

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

20000407 084

GAO
Accountability * Integrity * Reliability

GAO/T-NSIAD-00-145

DTIC QUALITY INSPECTED 1

Madam Chairman and Members of the Subcommittee:

I am pleased to be here to discuss our prior work and observations on federal efforts to combat terrorism, especially those to prepare for and respond to terrorist attacks involving chemical, biological, radiological or nuclear (CBRN) materials.[1] This is an important issue because responding to a terrorist CBRN attack would require close coordination among federal agencies (the Departments of Justice, Defense, the Federal Emergency Management Agency and others), as well as with state and local agencies. In addition, the amount of federal spending for combating terrorism has risen significantly to $11 billion as requested in the President's fiscal year 2001 budget. With so many players and so many resources at stake, good management of these programs 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.

My testimony will first discuss the need to link threats to strategies and resources in federal efforts to combat terrorism. The second issue I will discuss is the need to improve federal and state inter-governmental coordination and program issues. Finally, at your request, I will comment on the Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction—better known as the Gilmore Panel because its chairman is James S. Gilmore, III, Governor of Virginia.

Summary

One of the major deficiencies in federal efforts to combat terrorism is the lack of linkage between the terrorist threat, a national strategy, and agency resources. Much of the federal efforts to combat terrorism have been based upon vulnerabilities rather than an analysis of credible threats. For example, agencies have used and are still using improbable "worst case scenarios" to plan and develop programs. While there has been a major effort to develop a national strategy, to date the strategy does not include a clear desired outcome to be achieved. Resources to combat terrorism have increased in terms of both budgets and programs. These increased resources have not been clearly linked to a threat analysis and we have found cases where some agency initiatives appear at odds with the judgments of the intelligence community. This situation also creates the

[1] For purposes of this testimony, I 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 only include chemical, biological, radiological and nuclear weapons, others define it to include large conventional explosives.

potential for agencies to develop their own programs without adequate coordination, leaving the potential for gaps and/or duplication. Efforts to track and coordinate federal spending across agencies have started, but they have only begun to tackle the important task of prioritizing programs. We have recommended, and the executive branch has agreed to, conducting threat and risk assessments to improve federal efforts to combat terrorism. Specifically, such assessments could be an important step to develop a national strategy and to target resources.

The federal government cannot prepare for CBRN incidents on its own. Several improvements are also warranted in intergovernmental relations between federal, state and local governments. For example, we found that federal agencies developed some of their assistance programs without coordinating them with existing state and local emergency management structures. In addition, the multitude of federal assistance programs has led to confusion on the part of state and local officials. One step to improve coordination and reduce confusion has been the creation of the National Domestic Preparedness Office within the Department of Justice to provide "one stop shopping" to state and local officials in need of assistance. This office has recently prepared a draft plan on how it will provide assistance. Another intergovernmental issue requiring resolution is the matter of command and control at the site of a terrorist incident. Roles of the federal government versus the state and local governments need to be further clarified to prevent confusion. The federal government is making some progress in addressing these command and control issues through exercises. Federal exercises, in contrast to earlier years, are now practicing crisis and consequence management simultaneously and including state and local participation.

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

Background

Two Presidential Decisions Directives—number 39 issued in June 1995 and number 62 issued in May 1998—define U.S. policy to combat terrorism. These presidential directives and implementing guidance divide the federal response to terrorist attacks into two categories—crisis management and consequence management. Crisis management includes efforts to stop a terrorist attack, arrest terrorists, and gather evidence for criminal prosecution. Consequence management includes efforts to

provide medical treatment and emergency services, evacuate people from dangerous areas, and restore government services. The presidential directives also organize federal efforts to combat terrorism along a lead agency concept. The Department of Justice, through the Federal Bureau of Investigation (FBI), is the lead federal agency for crisis management of domestic terrorist incidents. For managing the consequences of domestic terrorist incidents, state and local authorities are primarily responsible. The Federal Emergency Management Agency (FEMA) is the lead federal agency for consequence management if state or local authorities request federal assistance.

Congress, concerned about federal programs to combat terrorism, created the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, better known as the Gilmore Panel.[2] The Panel was chartered to examine federal, state, and local preparedness, response, and funding issues for responding to terrorist attacks involving CBRN materials.

Linking Threats to Strategies to Resources

A well-organized and efficient national counterterrorism program starts with a rigorous assessment of the terrorist threat the United States faces. Included in the analysis should be a clear examination on the qualifications to that threat. Adjusted threat scenarios would feed a risk analysis for use in developing a strategy. A strategy should have a desired outcome to attempt to achieve and to measure progress against. Resource decisions should be based on both a threat and risk assessment, and a strategy with a clear desired outcome.

Assessing the Terrorist Threat

Intelligence agencies continuously assess the foreign and domestic terrorist threats to the United States. The U.S. foreign intelligence community, which includes the Central Intelligence Agency and others, monitors the foreign-origin terrorist threat to the United States. In addition, the 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 FBI reports an increasing number of domestic cases involving U.S. persons attempting or threatening to use such materials. The intelligence community also reports an increased possibility that terrorists may use CBRN agents in the next decade.

[2] The Panel was established in the Strom Thurman National Defense Authorization Act for Fiscal Year 1999 (Public Law 105-261, Section 1405).

Understanding Qualifications to the Terrorist Threat

What is important about intelligence agency threat assessments is the very critical distinction between what is conceivable or possible and what is likely in terms of the threat of a terrorist attack. Some of the public statements made by intelligence community officials about the terrorist CBRN threat do not include important qualifications to the information they present. 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.

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. 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 or environmental conditions and personal safety risks.

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

Need for Threat and Risk Assessment

In a prior report, we have recommended that the federal government conduct sound threat and risk assessments to define and prioritize requirements and properly focus programs and investments in combating terrorism.[3] The critical first step in a sound threat and risk assessment process is the threat analysis. The analysis should identify and evaluate each threat in terms of capability and intent to attack an asset, the likelihood of a successful attack, and its consequences. The result of this analysis should be a list of potential terrorist attack scenarios. Next the

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

risk assessment should be a deliberate, analytical effort that results in a prioritized list of risks (i.e., threat-asset-vulnerability combinations) that can be used to select countermeasures to create a certain level of protection or preparedness.

Without the benefits that a threat and risk assessment provides, many agencies have been relying on worst case scenarios to generate countermeasures or establish their programs. Worst case scenarios are extreme situations and, as such, may be out of balance with the threat. In our view, by using worst case scenarios, the federal government is focusing on vulnerabilities (which are unlimited) rather than credible threats (which are limited). By targeting investments based on worst case scenarios, the government may be over funding some initiatives and programs and under funding the more likely threats the country will face. As an example, we have testified that the Department of Health and Human Services is establishing a national pharmaceutical and vaccine stockpile that does not match intelligence agencies' judgments of the more likely chemical and biological agents that terrorists might use.[4] In some of our current work at other federal agencies, we are continuing to find that worst case scenarios are being used in planning efforts to develop programs and capabilities.

As you know, we have recommended that the threat and risk assessments be conducted at the local level as a tool to target federal assistance programs. In addition, since we last testified before this Subcommittee, we also recommended that the FBI perform a national-level threat and risk assessment.[5] The FBI has agreed in principle with our recommendations and FBI officials recently updated us on their progress. Regarding local threat and risk assessments, the FBI and the Department of Justices' Office of Justice Programs are about to send out threat and risk assessment information for local governments to use. The local jurisdictions will then send their assessments to their respective state governments to compile and analyze. The state governments will use the findings to develop a state-wide domestic preparedness strategy. The FBI has agreed to lead a national level threat and risk assessment, but has noted certain limitations. For example, because of the restrictions it faces on the use of law enforcement intelligence information, its efforts will first concentrate on the threats posed by various CBRN agents, as opposed to

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

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

threats posed by specific terrorist groups. The FBI would then combine this with threat information in a classified assessment. The FBI officials did not have an estimate as to when they would formally begin their national assessment, but they estimated it would take about 6 months.

Developing a Strategy With a Desired Outcome

We also believe there needs to be a federal or national strategy on combating terrorism which 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 December 1998, classified 5-year interagency plan on counterterrorism and technology crime represents a substantial interagency effort to develop a federal government counterterrorism strategy. The plan includes goals, objectives, and performance indicators and recommends that specific actions be taken to resolve interagency problems and issues it identified and assigns relative priorities to the actions. However, the plan does not have a clear desired outcome that would be useful to establish requirements and priorities. The plan also does not link its recommended actions and priorities to budget resources, although it states that the agencies hope to improve the link between the plan and resources in subsequent updates. While we hoped to provide you with new information on this plan since our last testimony, the first update to the original plan had not been released at the time we prepared this statement.

Linking Resources to the Threat and Strategy

Once threat and risks have been assessed and a strategy has been developed, agencies can target programs and spending appropriately. The threat and risk assessment, and the development of a strategy are particularly important given the rapid increase in federal programs and spending. For example, we have reported on a proliferation of potentially duplicative programs and initiatives across several agencies to provide training and/or equipment related to CBRN terrorist attacks to first responders—the local police, fire, and emergency personnel that would first respond to the incident.[6] Similarly, multiple equipment programs were causing frustration and confusion at the local level and were resulting in further complaints that the federal government is unfocused and has no coordinated plan or desired outcome for domestic preparedness. Paralleling the growth in federal training and equipment programs, federal response elements have also expanded and increased. Individual agencies' initiatives include adding teams or capabilities that can (1) identify and

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

analyze CBRN agents; (2) contain or handle the weapon, device, or area of an incident; and (3) provide medical support or response for dealing with potential casualties of an incident.

In addition to reporting on the increase in the number of programs, we have testified twice on the rapid increase in federal funding to combat terrorism.[7] The Office of Management and Budget (OMB) reported 1998 actual spending at $7.658 billion consisting of $5.871 billion for combating terrorism, $.645 billion for combating weapons of mass destruction and $1.142 billion for critical infrastructure protection. The President's budget request for fiscal year 2001 totals $11.117 billion consisting of $7.538 billion for combating terrorism, $1.552 billion for combating weapons of mass destruction and $2.027 billion for critical infrastructure protection. As proposed in the President's budget request, total funding would increase about 45 percent from 1998 to 2001, with component increases of about 28 percent for combating terrorism, about 140 percent for combating weapons of mass destruction, and about 77 percent for critical infrastructure protection. As noted in our earlier work, funding has increased dramatically at the Departments of Health and Human Services, Justice, and at the FBI.

In those testimonies, we reported positively on OMB's efforts to track budgeting and spending by counterterrorist and CBRN programs. We believe that the OMB reports on governmentwide spending and budgeting to combat terrorism are a significant step toward improved management and coordination of the 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. The OMB reports to date, however, do not clearly or explicitly describe any established priorities or duplication of efforts as called for in legislation.[8] At the time we prepared this statement, OMB had not released its detailed spending report for fiscal year 2000. However, OMB officials told us that they are now collecting detailed programmatic data from each agency, which will be useful for comparing agencies and analyzing trends. We

[7] *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)

[8] The National Defense Authorization Act for fiscal year 1998 required that OMB establish a system for collecting and reporting information on executive agencies' spending and budgets for combating terrorism (Section 1051 of Public Law 105-85, November 18, 1997). The legislation also required OMB to submit an annual report to Congress detailing, among other things, any established priorities or duplication.

continue to be hopeful that OMB's efforts will provide useful information for prioritizing and targeting resources.

Addressing Intergovernmental Issues

Responders at all levels of potential terrorist attacks must continue to resolve intergovernmental issues. For example, the multiplicity of federal assistance programs requires focus and attention to minimize redundancy of efforts and eliminate confusion at the recipient level. Based on the concerns of local officials, a single federal office acts as a clearinghouse. However, command and control roles at incident sites are still unclear under the current operational environment. To some extent, these issues can be explored and resolved through exercises that simultaneously practice crisis and consequence management and that include state and local participants.

Focusing and Coordinating Federal Assistance Programs

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

A major federal initiative to provide better focus and to coordinate federal assistance programs is the National Domestic Preparedness Office. The Office, which was recently funded in the Consolidated Appropriations Act for Fiscal Year 2000, is just getting organized.[9] The Office will function as an interagency forum to coordinate federal policy and program assistance for state and local emergency responders. For instance, the Office will assess federal training programs to eliminate duplication and ensure that

[9] Public Law 106-113, November 29, 1999. The Conference Report on this legislation is House Report 106-479, Nov. 18, 1999.

the training adheres to minimum national standards. It is to coordinate and serve as an information clearinghouse for federal programs devoted to supporting state and local emergency responder communities in the area of CBRN-related domestic preparedness planning, training, exercises, and equipment research and development. However, the Office will not have veto power over any agency's programs, so its authorities to actually prevent or stop duplicate programs will be limited.

Since our last testimony before this Subcommittee, the National Domestic Preparedness Office has drafted an action plan. According to the plan, the Office will focus on (1) identifying existing needs assessment tools, (2) cataloging all federal domestic preparedness training, (3) verifying that federal domestic preparedness training initiatives meet the applicable standards, (4) identifying existing training delivery systems and coordinate among federal agencies, (5) coordinating the development of sustainment CBRN training for emergency responders, and (6) facilitating the incorporation of lessons learned into training curriculums. As requested by this subcommittee, we plan to obtain updated information on the National Domestic Preparedness Office and report back to you.

Clarifying Command and Control at Incidents

Another intergovernmental issue requiring attention is the issue of command and control between the federal and state and/or local governments for crisis management. Except in cases where a terrorist attack occurred on a federal property (e.g., a military base), local first responders would initially be in charge. For example, a CBRN incident involving chemical agents would look like a major hazardous materials emergency and the local fire chief would usually be the incident commander. Local officials have expressed concerns about potential problems if the federal government tries to take over a state and/or local response already in progress. For example, an Oklahoma City official testified before this Subcommittee last year that a well-coordinated response to the Oklahoma City bombing was in progress but that relationships strained when federal teams arrived from outside the area.[10] She stated that there needs to be a uniform command and control protocol. The emergence of more federal response elements and capabilities (as discussed earlier) will further increase the challenge for the federal government to provide a well-coordinated response in support of a state or local incident commander. For example, FBI officials have expressed concerns about a conflict between certain DOD teams and their

[10] Testimony of Ann Simank, Council Member, Oklahoma City, Oklahoma, on behalf of the National League of Cities Before the House Subcommittee on Oversight, Investigations, and Emergency Management, June 9, 1999.

own Hazardous Materials Response Unit or other federal assets, if all arrive with the same capabilities and try to give advice to the incident commander.

This ambiguity over command of an incident is exacerbated by the separation of crisis management and consequence management. For terrorist attacks on U.S. soil, two separate federal agencies lead these activities—the FBI leads crisis management and FEMA leads consequence management. While the FBI would likely be in command (i.e., leading state and/or local officials) for the crisis management, FEMA is always in support of the state and/or local officials for consequence management. When terrorist attacks occur without adequate threat warning, crisis response and consequence management will be concurrent activities. This complicates unity of command because half of the response (crisis management) will be led by the federal government, and half of the response (consequence management) will be led by the state and/or local government.

Exercises Helping to Clarify Command and Control Issues

We found that federal agencies are working to clarify command and control issues through exercises. Exercises test and validate policies and procedures, test the effectiveness of response capabilities, and increase the confidence and skill level of personnel. In addition, exercises identify strengths and weaknesses before they arise in an actual incident. In combating terrorism, where operations are inherently interagency and intergovernmental matters, exercises also allow the various agencies' personnel to become familiar with the others' missions and procedures and learn to coordinate and operate together.

We have observed progress in intergovernmental exercises. In our review of federal counterterrorist exercises from 1995-98, we found that 69 of 201 exercises (or 34 percent) were intergovernmental—they included state and local authorities such as police and fire departments.[11] However, we also found that domestic crisis response exercises led by federal law enforcement agencies did not include many of the state, and local authorities that would be needed to effectively respond, or the entire range of activities required to respond to a terrorist crisis. We did note some improvements as we issued that report in 1999. The FBI began taking steps to enhance its program and said they viewed participation by state and local agencies as a top priority as it continued to plan and

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

execute counterterrorist exercises. FBI officials noted that staffing and budget considerations or restrictive union contracts sometimes hinder state and local participation in federal exercises.

We have also observed increased efforts to conduct exercises that simulate crisis management and consequence management together. During our review of federal counterterrorist exercises, we found that domestic crisis management exercises always ended in the successful tactical resolution of the incidents and did not include more likely scenarios where terrorist attacks were successful or occurred without adequate threat warning. Thus, the full gamut of interagency response activities was not tested. For example, in the 3 years following Presidential Decision Directive 39, the FBI did not conduct or participate in a field exercise that simulated the concurrence of crisis and consequence management to deal with a major terrorist incident. However, other agencies did lead exercises that focused on both crisis and consequence management. While there were none in the first year after PDD-39, there were 2 exercises in the second year and 33 exercises in the third year that included both crisis management and consequence management.

Comments on the Gilmore Panel Report

The Gilmore Panel issued its first report late last year and it focused primarily on assessing the threat of CBRN terrorism.[12] There are two aspects of the Panel that we view as very positive. First, by having a 3-year mandate, the Panel can delve into the issues more deeply and reassess its work as well as monitor federal programs as they develop. Secondly, the Panel includes several members from state and local governments, which will provide an important perspective to federal decisionmakers. As discussed below, there are many areas where the Panel's conclusions are very similar to our findings. In addition, Panel raised some other important points that Congress might want to study further.

GAO and Gilmore Panel Find Many Similar Deficiencies

Our work over the last 3 years—much of it summarized earlier in this statement—has identified a number of areas requiring improvements to federal programs to combat terrorism. The Gilmore Panel, through its own analysis, found many of the same deficiencies. Specific examples of the Panel's findings with which we have identified similar problems are as follow:

[12] *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, I. Assessing the Threat*, December 15, 1999.

- Federal programs addressing terrorism appear, in many cases, to be fragmented, overlapping, lacking focus, and uncoordinated.
- A terrorist group would face many difficulties in acquiring or developing and delivering a device with the capability to cause mass casualties.
- The United States should reconsider the "worst case scenario" assessments that have dominated domestic preparedness planning for CBRN terrorism.
- There should be a comprehensive and articulate assessment of potential credible terrorist threats as part of a risk and vulnerability assessment.
- It is not always clear "who is in charge" at the federal and state or local level when an incident occurs.
- There should be agreed-upon templates for local to federal handoffs of command and control, and these should be exercised in advance.
- A national strategy—beyond the existing Attorney General's Five Year Plan --is needed to address domestic preparedness and CBRN terrorism.

Other Issues Raised in the Gilmore Panel Report

The Gilmore Panel also raises some points that this Subcommittee and Congress as a whole may want to study further. We have not taken specific positions on these issues in our past reports, but believe they are worth mentioning in our testimony.

- The Panel concluded that there is ambiguity and lack of consensus on definitions for terrorism, weapons of mass destruction, mass casualties, and other terms that federal programs are being built around. Therefore, some common terms of reference would enhance communication and coordination among the federal agencies.
- The Panel concluded that the most likely terrorist attacks will involve large explosives. Therefore, more attention to these types of incidents would enhance overall preparedness to respond to terrorist attacks.
- The Panel concluded that congressional decisions for authority and funding to address the issue appear to be uncoordinated. They suggested that Congress consider forming an ad hoc Joint Special or Select Committee to provide more efficiency and effectiveness in Federal efforts.

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

GAO Contacts and Staff Acknowledgments

For additional questions 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 and George M. Delgado.

Related GAO Products

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).

Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations (GAO/T-AIMD-00-7, Oct. 6,1999).

Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences (GAO/AIMD-00-1, Oct. 1, 1999).

Information Security: The Proposed Computer Security Enhancement Act of 1999 (GAO/T-AIMD-99-302, Sept. 30, 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: 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: 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: Federal Agencies' Efforts to Implement National Policy and Strategy (GAO/NSIAD-97-254, Sept. 26, 1997).

(702060)

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)