THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

HTTP://WWW.BLACKVAULT.COM

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

United States General Accounting Office

GAO

Report to Congressional Committees

September 2001

COMBATING TERRORISM

Selected Challenges and Related Recommendations

DISTRIBUTION STATEMENT A:
Approved for Public Release -
Distribution Unlimited

20010924 027

G A O

Accountability * Integrity * Reliability

GAO-01-822

Contents

Tables

Figures

Abbreviations

AAR	after-action report
ATF	Bureau of Alcohol, Tobacco, and Firearms
CBIRF	Chemical-Biological Incident Response Force
CERT	Computer Emergency Response Team
CIAO	Critical Infrastructure Assurance Office
CIP	critical infrastructure protection
CONPLAN	Concept of Operations Plan
DOD	Department of Defense
DOE	Department of Energy
DTRA	Defense Threat Reduction Agency
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FedCIRC	Federal Computer Incident Response Center
FEMA	Federal Emergency Management Agency
GAO	General Accounting Office
HHS	Department of Health and Human Services
ISAC	Information Sharing and Analysis Center
NDPO	National Domestic Preparedness Office
NIPC	National Infrastructure Protection Center
NSC	National Security Council
NSF	National Science Foundation
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OEP	Office of Emergency Preparedness
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PCIE/ECIE	President's Council on Integrity and Efficiency and Executive Council on Integrity and Efficiency
PDD	Presidential Decision Directive
SWAT	Special Weapons and Tactics
TOPOFF	Top Officials
TSWG	Technical Support Working Group
USDA	U.S. Department of Agriculture
WMD	weapons of mass destruction
VA	Department of Veterans Affairs

GAO
Accountability * Integrity * Reliability
United States General Accounting Office
Washington, DC 20548

Comptroller General
of the United States

September 20, 2001

The Honorable Carl Levin
Chairman
The Honorable John Warner
Ranking Minority Member
Committee on Armed Services
United States Senate

The Honorable Bob Stump
Chairman
The Honorable Ike Skelton
Ranking Democratic Member
Committee on Armed Services
House of Representatives

We at the U.S. General Accounting Office, as all Americans, were shocked by the coordinated terrorist attacks on New York City and Washington, D.C., on September 11, 2001. This report, which already was scheduled for release this month before the events of September 11, summarizes federal efforts to combat terrorism prior to these events. Given the tragic events of September 11, it is clear that combating terrorism efforts are now at the top of the national agenda. This report does not include recent efforts made in light of these recent attacks. While this report is a dispassionate and analytical discussion of the progress made and challenges faced by the federal government and the nation, we recognize the terrible cost of terrorism in human terms. The events of September 11 remind us that the victims of terrorism are real people—men, women, and children—and are our families, colleagues, friends, and neighbors. Our hearts go out to the victims, including the heroic first responders who were lost, and their families. We hope that this report promotes a reasoned discussion and additional actions designed to better prepare the nation to combat terrorism.

Concerned that terrorists might use weapons of mass destruction—a chemical, biological, radiological, or nuclear agent or weapon—against civilian targets within the United States, or attack critical infrastructure through computer systems, the Congress and various federal agencies have undertaken numerous initiatives over the past few years designed to improve the nation's ability to combat terrorism. As mandated in section 1035 of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (P.L. 106-398, Oct. 30, 2000), we reviewed the strategy, policies,

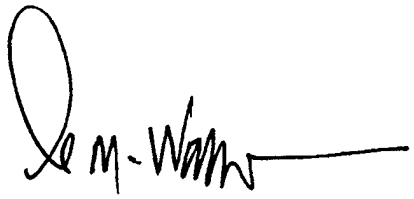
and programs to combat domestic terrorism, particularly domestic terrorism involving weapons of mass destruction. We briefed your staffs previously on the preliminary results of our work. This report contains the final results of our review.

In response to the mandate and, as agreed with your offices, this report assesses (1) the current framework for leadership and coordination of federal agencies' efforts to combat terrorism on U.S. soil, and proposals for change, (2) progress the federal government has made in developing and implementing a national strategy to combat terrorism domestically, (3) the federal government's capabilities to respond to a domestic terrorist incident, (4) progress the federal government has made in helping state and local emergency responders prepare for a terrorist incident, and (5) progress made in developing and implementing a federal strategy for combating cyber-based attacks. This capping report updates and summarizes our extensive evaluations conducted in recent years of federal programs to combat domestic terrorism and protect critical infrastructure. We include a series of Recommendations for Executive Action, including three recommendations to the President, to improve overall leadership and coordination of federal efforts to combat terrorism as well as other improvements. Agency comments on a draft of this report were based on their efforts prior to the September 11, 2001, terrorist attacks.

We are sending copies of this report to other interested congressional committees. We also are sending copies to the President; the Vice President; the Secretaries of Agriculture, Commerce, Defense, Energy, Health and Human Services, State, Transportation, the Treasury, and Veterans Affairs; and the Attorney General. In addition, we are sending copies to the Director, Bureau of Alcohol, Tobacco, and Firearms; the Director, Centers for Disease Control and Prevention; the Director of Central Intelligence; the Administrator, Environmental Protection Agency; the Director, Federal Emergency Management Agency; the Director, Federal Bureau of Investigation; the Administrator, General Services Administration; the Assistant to the President for National Security Affairs; the Assistant to the President for Science and Technology; the Director, Office of Management and Budget; the Commandant of the U.S. Coast Guard; and the Director, U.S. Secret Service. We will make copies available to other interested parties upon request. This report also will be available on GAO's web site at www.gao.gov.

If you or your offices have any questions about matters discussed in this report, please contact me at (202) 512-5500; Henry L. Hinton, Jr., Managing Director, Defense Capabilities and Management, at (202) 512-4300; or

Raymond J. Decker, Director, at (202) 512-6020. They also can be reached by e-mail at hintonh@gao.gov and deckerrj@gao.gov, respectively. Contacts and key contributors are listed in appendix XVII.



David M. Walker
Comptroller General
of the United States

Executive Summary

Purpose

With the coordinated terrorist attacks against the World Trade Center in New York City and the Pentagon in Washington, D.C., on September 11, 2001, the threat of terrorism rose to the top of the country's national security and law enforcement agendas. Even before these catastrophic events, terrorism was a growing national security and law enforcement concern. Current federal efforts to combat terrorism are inherently difficult to lead and manage because the policies, strategies, programs, budgets, and activities are spread across more than 40 different federal agencies. For fiscal year 2002, the federal government's proposed budget for these programs is over $12 billion. In addition, the Congress recently approved the President's request for $20 billion in emergency assistance and provided an additional $20 billion to supplement existing contingency funds.

Concerned about the preparedness of the federal government and state and local emergency responders to cope with a large-scale terrorist attack involving the use of weapons of mass destruction, the Congress in section 1035 of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (P.L. 106-398) mandated that GAO report on the strategies, policies, and programs for combating domestic terrorism involving weapons of mass destruction.[1] As agreed with your offices, this report assesses

- the current framework for leadership and coordination of federal agencies' efforts to combat terrorism on U.S. soil, and proposals for change;
- progress the federal government has made in developing and implementing a national strategy to combat terrorism domestically;
- the federal government's capabilities to respond to a domestic terrorist incident;
- progress the federal government has made in helping state and local emergency responders prepare for a terrorist incident; and
- progress made in developing and implementing a federal strategy for combating cyber-based attacks.

[1]Throughout this report, we use the term weapons of mass destruction to refer to chemical, biological, radiological, or nuclear agents or weapons. Some agencies define it to include large conventional explosives as well. As clearly demonstrated by the September 11, 2001, incidents, a terrorist attack would not have to fit this definition of weapons of mass destruction to result in mass casualties, destruction of critical infrastructures, economic losses, and disruption of daily life nationwide.

Background

The threat of terrorism is a high-priority U.S. national security and law enforcement concern. U.S. policy on combating terrorism has been evolving for about 30 years. A series of presidential decision directives along with implementing guidance, executive orders, interagency agreements, and legislation provide the basis for counterterrorism programs and activities in more than 40 federal agencies, bureaus, and offices. In addition to reducing vulnerabilities and preventing and deterring terrorist acts before they occur, the U.S. strategy for combating terrorism consists of crisis management and consequence management. Crisis management involves efforts to prevent and deter a terrorist attack, protect public health and safety, 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.

Since 1982, the Department of Justice, through the Federal Bureau of Investigation, has been responsible for crisis management. Presidential Decision Directive 39, issued in June 1995 in the aftermath of the bombing of the federal building in Oklahoma City, Oklahoma, reaffirmed the Department of Justice, through the Federal Bureau of Investigation, as the lead agency responsible for crisis management of domestic terrorist incidents. Although state and local governments have the primary responsibility for managing the consequences of a domestic terrorist incident, the 1995 directive designated the Federal Emergency Management Agency as the lead agency responsible for coordinating federal agencies' responses and activities when state and local authorities request assistance.

In May 1998, the President issued Presidential Decision Directive 62, which reaffirmed the earlier directive and established within the National Security Council in the Executive Office of the President a National Coordinator for Security, Infrastructure Protection and Counterterrorism to provide a focal point for federal efforts to combat terrorism. In May 2001, the President tasked the Vice President with overseeing the development of a coordinated effort to improve national preparedness (see app. VII). Also, the President established, within the Federal Emergency Management Agency, a new Office of National Preparedness, which will coordinate all federal domestic preparedness and consequence management programs and activities for terrorist-related weapons of mass destruction incidents or other threats.

The United States also is developing and implementing a strategy for combating the threat of cyber, or computer-based, attacks. This strategy is

articulated in Presidential Decision Directive 63, which was issued in May 1998 concurrently with Presidential Decision Directive 62. Protection against computer-based attacks requires vigilance against a broader array of threats, to include not only terrorists, but nation states, criminals, and others. Attacks could severely disrupt computer-supported operations and infrastructures, such as telecommunications, power distribution, financial services, national defense, and critical government operations. The risk to these infrastructures has increased in recent years due to their growing dependence on computers and the greater interconnectivity among computers.

The proposed federal budget for these programs for fiscal year 2002 is over $12.8 billion, of which about $8.6 billion is to combat terrorism, about $1.8 billion is to combat weapons of mass destruction, and about $2.6 billion is for critical infrastructure protection. This proposed budget represents about a 78-percent increase in total funding to combat terrorism compared with the fiscal year 1998 funding level of about $7.2 billion. In addition, the Congress recently approved the President's request for $20 billion in emergency assistance and provided an additional $20 billion to supplement existing contingency funds. The Office of Management and Budget tracks federal funds to combat terrorism and has provided this information to the Congress on an annual basis since fiscal year 1998.

This capping report updates GAO's extensive evaluations in recent years of federal programs to combat domestic terrorism and protect critical infrastructure.

Results in Brief

Greater attention has been placed on combating terrorism as concerns have grown. Assignment of Executive Branch responsibilities and authorities also has received additional emphasis, including the appointment of a national coordinator in 1998 in the National Security Council to serve as a focal point for overall leadership and coordination. The growing threat of terrorism, combined with the significant increase in funding and growth in the number of programs to combat terrorism over the past several years, presents evolving challenges to the existing framework for leadership and coordination. GAO's analysis indicates that a need now exists to clarify and expand the responsibilities of the Executive Branch focal point. While the National Coordinator serves as a focal point for some interagency functions, other key overall leadership and coordination functions, such as guiding the development of a national strategy, are not clearly assigned to the focal point. In GAO's view, the

functions and responsibilities of the focal point should include overseeing a threat and risk assessment and the development of a national strategy, coordinating governmentwide budgets, and monitoring overall agency implementation. A clear assignment of these responsibilities and the authority to discharge them are needed to provide assurance that (1) federal programs are based upon a coherent strategy and the programs are well coordinated and (2) gaps and duplication in capabilities are avoided as threats are likely to grow more complex and diffuse.

The Congress and the President both have recognized the need to review and clarify the structure for overall leadership and coordination. At the request of the President in May 2001, the Vice President will oversee the development of a coordinated national effort to improve national preparedness, including efforts to combat terrorism. GAO believes it is important that the President, in conjunction with the Vice President's efforts, focus on the functions, responsibilities, and authorities of the focal point. GAO makes a recommendation to the President that he assign a single focal point within the Executive Office of the President, with the time, responsibility, authority, and resources for overall leadership and coordination of federal programs to combat terrorism.

Federal efforts to develop a national strategy to combat terrorism and related guidance have progressed, but key challenges remain. The initial step toward developing a national strategy is to conduct a national threat and risk assessment. The Department of Justice and the Federal Bureau of Investigation have collaborated on taking steps to conduct such an assessment. They have developed an assessment tool at the state and local level that will provide important information for federal resource decisions. However, at the national level, they have not completed assessments of the most likely weapon-of-mass-destruction agents and other terrorist threats. With regard to drafting a national strategy to combat terrorism, the Attorney General, working with several other agencies, published a Five-Year Interagency Counterterrorism and Technology Crime Plan. The Five-Year Plan, which was an interagency effort, identifies goals and objectives, sets priorities, and tracks agencies' progress; but it lacks two critical elements. First, while citing goals and objectives, the plan does not include measurable outcomes. Second, it does not identify state and local government roles in combating terrorism. The Five-Year Plan is not linked to resources, but the Office of Management and Budget has made progress in tracking and reporting on terrorism-related budgets and spending. However, the National Security Council and the Office of Management and Budget in the annual report to the Congress on combating terrorism have not identified priorities or

reported on duplication of efforts. GAO makes two related recommendations: one to complete a threat assessment and one to revise the Five-Year Plan to better serve as a national strategy.

Beyond a national strategy, substantial progress has been made in completing operational guidance and related plans to coordinate agencies' responses at the site of a terrorist incident. A number of previous GAO recommendations that the federal government complete interagency operational guidance have been implemented. Progress also has been made by some individual agencies that have completed or are developing internal plans and guidance.

Under current policy, the federal government also has improved its capabilities to prevent, deter, and respond to a domestic terrorist incident. The Federal Bureau of Investigation and the Federal Emergency Management Agency are tasked with leading federal efforts in their respective roles for managing a terrorist crisis and the consequences of an incident. These two agencies would be supported by a number of other federal agencies with response capabilities. The Federal Bureau of Investigation and the U.S. Secret Service have better coordinated their response capabilities during special events, such as the presidential inauguration, political conventions, and preparation for the 2002 Olympic Winter Games.

Also, federal agencies have conducted a variety of exercises to test their response capabilities. These exercises have improved considerably in recent years and now regularly include interagency and intergovernmental command and control. Field exercises actually tested deployments with scenarios that practiced crisis and consequence management simultaneously. Improvements still are needed in consequence management exercises and in evaluating interagency aspects of federal exercises. Activities to develop future capabilities—through research and development and applying technology—are coordinated by interagency working groups. However, limits to the scope of these working groups' activities, in conjunction with the large number of projects and funding, provide the potential for duplication of efforts. GAO makes one recommendation to the President to direct the focal point to capture and evaluate interagency lessons learned from federal counterterrorism exercises and three other recommendations to improve readiness in consequence management, increase agencies' benefits from exercises, and complete a strategy to coordinate counterterrorism research and development.

Federal assistance to state and local governments to prepare for terrorist incidents has resulted in training for thousands of first responders—those state and local officials who would first respond at the scene of an incident. Some of these programs initially were developed without recognizing existing state and regional coordinating mechanisms for emergency preparedness. Moreover, these assistance programs overlapped because several federal agencies had similar efforts that were not well coordinated with each other. Since our earlier work, some programs have been consolidated; and there have been increased efforts to coordinate programs across agencies.

To further improve this coordination, state and local officials have called for a single federal liaison for state and local preparedness programs. In response, the Attorney General established the National Domestic Preparedness Office within the Federal Bureau of Investigation to coordinate federal agencies' efforts to train first responders. However, this Office has not been effective due to funding, personnel, and organizational problems. Recently, the President directed that the Federal Emergency Management Agency establish an Office of National Preparedness to coordinate all federal consequence management programs dealing with weapons of mass destruction. This development creates an opportunity to consolidate within the Federal Emergency Management Agency the federal consequence management assistance programs to state and local governments that are at the Department of Justice and Federal Bureau of Investigation. GAO recommends that this be done.

Finally, the federal government has provided some states with specialized National Guard teams, but these teams continue to experience problems that undermine their usefulness. GAO makes a recommendation to place a temporary moratorium on adding new, specialized National Guard response teams until their roles and missions are fully coordinated.

Regarding risks to computer systems and, more importantly, to the critical operations and infrastructures they support, an array of efforts has been undertaken to implement a national strategy outlined in Presidential Decision Directive 63. However, progress in certain key areas has been slow. Specifically, federal agencies have taken initial steps to develop critical infrastructure protection plans; but independent audits continue to identify persistent, significant information security weaknesses that place federal operations at high risk of tampering and disruption. In addition, outreach efforts by numerous federal entities to establish cooperative relationships with and among private and other non-federal entities have raised awareness and prompted information sharing, and the federal

government and the private sector have initiated a variety of critical infrastructure protection-related research and development efforts. However, substantive analysis of sector-wide and cross-sector interdependencies and related vulnerabilities has been limited. An underlying deficiency impeding progress is the lack of a national plan that fully defines the roles and responsibilities of key participants and establishes interim objectives. The administration currently is reviewing and considering adjustments to the government's critical infrastructure protection strategy that may address this deficiency. GAO recommends developing a more detailed strategy for combating computer-based attacks, which should be linked to a national strategy to combat terrorism.

Principal Findings

Overall Leadership and Coordination Need to Be Addressed

The management structure for leading and coordinating federal efforts to combat terrorism has evolved since June 1995 when Presidential Decision Directive 39 assigned the Department of Justice, through the Federal Bureau of Investigation, responsibility as the lead federal agency for crisis management and the Federal Emergency Management Agency responsibility as the lead federal agency for consequence management of domestic terrorist incidents. In May 1998, Presidential Decision Directive 62 established the position of National Coordinator within the National Security Council; however, its functions were never detailed in either an executive order or through legislation. Many of the overall leadership and coordination functions GAO has identified as critical were not given to the National Coordinator. In fact, several other agencies, such as the Department of Justice, Federal Bureau of Investigation, Federal Emergency Management Agency, and the Office of Management and Budget, currently perform these functions. Some of the functions currently located in different agencies include overseeing a threat and risk assessment, developing a national strategy, and coordinating program implementation across agencies. The interagency roles of these various agencies are not always clear and sometimes overlap, which leads to a fragmented approach. For example, the Department of Justice, the National Security Council, the Federal Bureau of Investigation, and the Federal Emergency Management Agency have developed—or plan to develop—aspects of national strategies to combat terrorism. National efforts to combat illegal drugs offer potential lessons in addressing the overall leadership and coordination of interagency efforts to combat terrorism. Importantly, the Office of National Drug Control Policy, through legislation, has the legitimacy and authority to carry out its functions.

Both the Congress and the President have expressed concern about the overall national leadership and coordination of programs to combat terrorism. The Congress has held hearings, appointed commissions, and proposed legislation on these issues. The President asked the Vice President in May 2001 to oversee the development of a coordinated effort to improve national preparedness (see app. VII). While it is not yet clear what the Vice President specifically will be responsible for, agencies involved do not anticipate that his position will be one of permanent, overall leadership and coordination. The President also established an Office of National Preparedness within the Federal Emergency Management Agency to coordinate all federal consequence management programs dealing with weapons of mass destruction. Several proposals have been advanced to improve the overall leadership and coordination of programs to combat terrorism. These approaches generally create a single focal point located in either the Executive Office of the President or a lead executive agency. Each location has its advantages and disadvantages.

Based upon numerous evaluations, the identification of recurring problems in the overall leadership and coordination of programs, and an analysis of various proposals, GAO believes a single focal point, with all critical functions and responsibilities, should be assigned to lead and coordinate these programs. This focal point, for example, could be an individual, an executive office, or a council. Furthermore, this focal point should be in the Executive Office of the President and be independent of any existing federal agency. A focal point within the Executive Office of the President would be independent, above the interests of any of the several individual agencies involved. The focal point needs to have the time, responsibility, authority, and resources for coordinating both crisis management and consequence management activities. Current proposals to create a new agency to combine functions currently in several agencies still would not contain all the government agencies and functions needed to combat terrorism. While not endorsing any specific organizational structure for the single focal point, GAO has identified basic functions that any focal point should perform.

Limited Progress Made in Developing a National Strategy and Related Guidance and Plans

An important initial step in developing a national strategy is to conduct threat and risk assessments to define and prioritize requirements. The Department of Justice and the Federal Bureau of Investigation have made limited progress in implementing GAO's recommendations that such assessments be performed at both the local and national level. For example, the Department of Justice and the Bureau have worked together to provide a threat and risk assessment tool to state and local

governments. These state and local assessments may complement national-level threat and risk assessments and related policy-making. Regarding GAO's recommendation for national-level authoritative threat assessments, the Bureau agreed to lead such assessments in July 1999. The Bureau is collaborating with other agencies to complete two assessments of terrorist threats, including those involving weapons of mass destruction.

The Department of Justice has made progress toward developing a national strategy through its publication of the Attorney General's Five-Year Interagency Counterterrorism and Technology Crime Plan. The plan represents a substantial interagency effort and is the one current document that could serve as a basis for the development of a national strategy. However, GAO believes the plan should be improved to better serve as a national strategy. First, the plan needs to have measurable outcomes consistent with the Government Performance and Results Act of 1993. Although the plan has objectives and performance indicators, it focuses on agency activities, which represent outputs as opposed to results-oriented outcomes. Second, the plan needs to better define the roles of state and local governments. Although the Department of Justice obtained state and local input in preparing the Five-Year Plan and identifies specific ways to enhance state and local responder capabilities, the plan does not identify state and local government roles in responding to a terrorist incident. To the extent that the plan should better address the roles of state and local authorities, and be developed with them, GAO believes it can become more of a national strategy than a federal plan.

The Office of Management and Budget has made progress tracking budgets and expenditures for programs to combat terrorism and has issued four annual reports to the Congress. Through these reports, the executive branch and the Congress now have strategic oversight of the magnitude and direction of federal funding to combat terrorism. Each annual report progressively has contained more details about agency budgets and spending by various categories. In 1999, the National Security Council and the Office of Management and Budget initiated a new process by which interagency working groups reviewed the agencies' proposals and developed recommendations on whether they should be funded. The Office has stated that this new process resulted in the reallocation of resources to fund critical shortfalls and eliminate duplication. However, its annual reports have not identified priorities or reported on duplication of efforts.

Federal agencies also have made progress in completing guidance and plans related to terrorism. The Federal Bureau of Investigation and Federal Emergency Management Agency now have completed interagency guidance to combat terrorism domestically, thereby clarifying many command and control issues. Similarly, agencies have completed or are developing internal guidance and concepts of operations to respond to terrorist incidents.

Federal Response Capabilities Have Improved but Further Action Could Be Taken

Federal capabilities to respond to terrorist incidents have improved. Such capabilities include a broad array of teams and related assets, such as mobile laboratories for initial on-site analysis of a weapon of mass destruction. The Federal Bureau of Investigation leads a variety of potential federal teams for crisis management, while the Federal Emergency Management Agency leads a variety of potential federal teams for consequence management. These capabilities have been improved in several ways. First, these capabilities have been enhanced through agency participation in special events. These events provide federal agencies with valuable experience working together to develop and practice plans to combat terrorism. The Federal Bureau of Investigation and the U.S. Secret Service have improved their cooperation for such events. For example, they now have a written agreement on command and control issues and jointly conduct some planning and exercises. Second, federal agencies also have improved their capabilities by conducting exercises. The Federal Bureau of Investigation has made progress in regularly practicing its interagency and intergovernmental leadership role in crisis management. However, the Federal Emergency Management Agency still is not using exercises to fully practice its leadership role over consequence management. Third, federal capabilities have been improved when agencies learn lessons from exercises and operations, such as special events. As in its earlier reviews, GAO found that some federal agencies have relatively good processes in place to capture and share lessons learned while others have less rigorous processes. Some federal agencies work to capture and share interagency lessons learned; however, as yet, there is no regular process in place to capture and share these types of evaluations that cross agency lines.

Federal capabilities also have been enhanced through research and development projects. Examples of recently developed and fielded technologies include products to detect and identify weapons of mass destruction, transport contaminated materials, and validate protection equipment life spans. Federal agencies and an interagency working group presently are developing technologies, including vehicle explosives

screening and barrier technologies, as well as decontamination products for use in urban facilities, such as subways and airports. Because of the high risk, long development time, and high cost, federal government involvement probably will be required for research and development projects related to weapons of mass destruction. Federal research and development programs are coordinated in a variety of ways, but primarily through an interagency working group. However, coordination is limited by a number of factors, raising the potential for duplication of efforts among different federal agencies.

Federal Assistance to State and Local Governments Can Be Consolidated

Recent developments may allow the consolidation of federal programs that provide assistance to state and local governments. These programs have improved domestic preparedness by training and equipping over 273,000 first responders since fiscal year 1998. These programs also have included exercises to allow first responders to interact with each other and with federal responders during realistic field conditions. However, some of these programs initially were implemented without leveraging existing regional and state structures for emergency management. For example, the Department of Defense provided training to localities without taking advantage of the existing state emergency management structures, mutual aid agreements among local jurisdictions, or other collaborative arrangements for emergency response. In addition, the number of programs led by three different federal agencies—the Departments of Defense and Justice and the Federal Emergency Management Agency—created an overlapping approach with potential duplication. More recently, some programs have been consolidated, such as the Department of Defense's domestic preparedness programs, which were transferred to the Department of Justice. In addition, efforts have increased to better coordinate assistance programs across agencies.

The number of federal agencies involved in the programs led to confusion on the part of state and local officials. These officials asked the federal government to establish a single federal liaison for state and local governments. In 1998, the Attorney General established the National Domestic Preparedness Office under the management of the Federal Bureau of Investigation to serve as a single point of contact for state and local authorities. However, the Office has not been effective in carrying out its tasks due to insufficient funding, lack of key functional expertise, potential organizational duplication, and a perceived lack of independence due to its location within the Bureau.

In May 2001, the President asked the Director of the Federal Emergency Management Agency to establish an Office of National Preparedness that

will serve as the focal point within the federal government for the oversight, coordination, integration, and implementation of preparedness and consequence management programs and activities for weapons of mass destruction and related threats. This new Office provides an opportunity to consolidate federal programs to assist state and local governments, including some assistance programs currently under the Department of Justice and Federal Bureau of Investigation. However, the Department of Justice and the Federal Bureau of Investigation would retain their lead federal agency responsibilities for crisis management and their law enforcement and investigative roles and responsibilities.

Federal assistance also has been provided in the form of special National Guard teams that are trained and equipped to provide states with capabilities to detect and analyze weapons of mass destruction and provide technical advice. These teams continue to experience problems with readiness, doctrine and roles, and deployment that undermine their usefulness in an actual terrorist incident. Until the Department of Defense has completed its coordination of the teams' roles and missions with the Federal Bureau of Investigation—the lead federal agency for crisis management—the establishment of any additional teams would be premature. The Department of Defense agrees with GAO's assessment.

Limited Progress in Implementing a Strategy to Counter Computer-Based Threats

To protect critical federal systems from computer-based attacks, federal entities, such as the Chief Information Officers Council and the Critical Infrastructure Assurance Office, have developed model policies and tools for measuring the effectiveness of agency information security programs and taken steps to identify critical assets and better coordinate the federal response to computer incidents. In addition, individual executive agencies have taken significant actions to correct identified computer security weaknesses associated with their systems and improve their information security programs. However, audits have continued to identify significant information security weaknesses in virtually every major federal agency and, since 1996, GAO has reported that poor security program management is an underlying cause that has diminished agencies' abilities to ensure that controls are appropriate and effective. In addition, a March 2001 report by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency identified significant deficiencies in agencies' implementation of Presidential Decision Directive 63 and questioned the federal government's ability to achieve the directive's goal to protect the nation's critical infrastructures from intentional destructive acts by May 2003. Factors cited as impediments to

federal efforts include uncertainty regarding Presidential Decision Directive 63's applicability and resource constraints.

Beyond efforts to protect their own computer-dependent operations, lead agencies also have taken steps to foster cooperative relationships with the eight infrastructure sectors identified in Presidential Decision Directive 63, which include telecommunications, banking and finance, transportation, energy, and emergency services. For most of the infrastructure sectors, representatives had been selected to coordinate and lead efforts, and education and outreach efforts had been undertaken to promote understanding of the risk and encourage cooperation. In addition, five industry specific centers had been established to gather and share information about vulnerabilities and computer-based attacks. However, substantive, comprehensive analysis of infrastructure sector vulnerabilities and development of related remedial plans had been limited because relationships were still being established, critical assets and entities had not been identified completely, and appropriate methodologies still were being identified and developed. Factors that had impeded progress in gaining private sector involvement included lack of senior executives' awareness about the importance of their assets to national and economic security and concerns about antitrust violations and release of sensitive information. Further, in April 2001, GAO reported significant deficiencies in progress made by the Federal Bureau of Investigation's National Infrastructure Protection Center, which was established to serve as a national analysis and warning center for cyber threats and attacks. In that report, GAO identified several impediments to progress, including staffing shortfalls and inconsistent interpretations of the Center's role and responsibilities among other entities involved in critical infrastructure protection.

Other federal efforts include activities to expand international cooperation regarding critical infrastructure protection. The Departments of State, Justice, and Commerce have organized and participated in meetings with representatives of other countries to discuss infrastructure protection, developed a United Nations Resolution on cyber-crime, and were in the process of negotiating a Council of Europe treaty on cyber-crime. In addition, GAO identified a variety of research and development efforts that were either being planned or performed.

A recurring finding resulting from work done by GAO and by agency inspectors general is that a fundamental deficiency in the implementation of Presidential Decision Directive 63 has been the lack of an adequate national plan that delineates interim objectives and the specific roles and

responsibilities of federal and non-federal entities involved in critical infrastructure protection. In addition, several agency officials said that funding and staffing constraints contributed to their delays in implementing Presidential Decision Directive 63 requirements. The administration currently is reviewing the federal critical infrastructure protection strategy and, according to a May 2001 White House press statement, is developing recommendations on how to structure an integrated approach to cyber-security and critical infrastructure protection.

The federal government's cyber-security strategy should be linked to a national strategy to combat terrorism as discussed earlier. However, the two areas are different in that the threats to computer-based infrastructures are broader than terrorism and programs to protect them are more closely associated with traditional information security activities.

Recommendations for Executive Action

GAO is making multiple recommendations, which are summarized below. Chief among these are three recommendations to the President in chapters 2, 4, and 5. They are the following:

- Designate a single focal point with responsibility and authority for all critical functions necessary to provide overall leadership and coordination of federal programs to combat terrorism (see ch. 2).
- Direct the focal point to develop a formal process to evaluate interagency lessons learned from major federal exercises to combat terrorism (see ch. 4).
- Consolidate selected Department of Justice and Federal Bureau of Investigation assistance programs to state and local governments into the Federal Emergency Management Agency (see ch. 5).

GAO also is making a number of additional recommendations for executive action to improve federal efforts to combat terrorism. They entail taking the following actions:

- Complete a threat assessment on likely weapons of mass destruction and other weapons that might be used by terrorists (see ch. 3).
- Revise the Attorney General's Five-Year Interagency Counterterrorism and Technology Crime Plan to better serve as a national strategy (see ch. 3).
- Expand the Federal Emergency Management Agency's role in managing federal exercises (see ch. 4).
- Prepare agencies' after-action reports or similar evaluations of exercises and operations (see ch. 4).

- Complete a strategy to coordinate research and development to improve federal capabilities and to avoid duplication of effort (see ch. 4).
- Place a temporary moratorium on new National Guard teams until their roles and missions are fully coordinated in writing with the lead federal agency for crisis management (see ch. 5).
- Develop a strategy for combating computer-based attacks that more clearly defines specific roles and responsibilities of organizations involved, interim objectives and milestones for achieving goals, and related performance measures (see ch. 6).

Agency Comments and Our Evaluation

GAO provided a draft of this report to appropriate federal agencies for their review and comment in August 2001. Agency comments were based on their efforts prior to the September 11, 2001, terrorist attacks on New York City and Washington, D.C. The Office of Management and Budget provided consolidated written comments from the National Security Council, Office of Management and Budget, and Office of Science and Technology Policy on a draft of this report. The Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Justice, the Treasury, and Veterans Affairs and the Federal Emergency Management Agency also provided written comments on a draft of this report. These comments are reprinted, along with GAO's comments, in appendixes VII to XVI. The Departments of State and Transportation, the Environmental Protection Agency, and the General Services Administration provided GAO with oral comments on a draft of this report. Written and oral comments from all of these agencies, as well as their technical comments, have been incorporated in the report, as appropriate.

Several agencies generally concurred with GAO's report and/or its recommendations, including the Departments of Commerce, Defense, Energy, Transportation, and Veterans Affairs; the Federal Emergency Management Agency; and the Environmental Protection Agency. The Department of Health and Human Services stated that the report's observations and comments will be useful for the Vice President's pending comprehensive review on national preparedness. The Department of Transportation noted that, overall, the report provides a useful, comprehensive "capping" effort identifying the efforts undertaken by multiple federal agencies to combat terrorism. The Department of Energy said the report accurately describes both the recent accomplishments and the lack of progress within the interagency community in this area. In contrast, the Department of Justice had "serious reservations" about some of the discussion and recommendations in the report that the President designate a single focal point and that its assistance programs to state and

local governments be consolidated under the Federal Emergency Management Agency.

Two agencies—the Departments of Energy and Transportation—supported GAO's most important recommendation to the President—that he work with the Congress to establish a single focal point for overall leadership and coordination for programs to combat terrorism. The Department of Energy stated that a single responsible and accountable focal point for combating terrorism should be established, independent of any existing federal agency. The Department of Transportation said the report makes a reasonable case for a single point of focus for terrorism issues in the Executive Branch. In contrast, the Department of Justice said, in light of the Vice President's pending review, this recommendation is premature. The Department also said that, in its view, there is no need at this time to change or expand the role of the current NSC National Coordinator. Other federal agencies—including the Executive Office of the President—did not comment on this recommendation. The Office of Management and Budget referred us to the President's May 8, 2001, statement (see app. VII) in which the President tasked the Vice President with overseeing the development of a coordinated effort to improve national preparedness. Officials from several other agencies indicated that it would be premature for them to comment on this recommendation until the Vice President has completed his review of national preparedness. GAO disagrees that its recommendation on this matter is premature. Notwithstanding the Vice President's review, GAO's recommendation is based upon its own reviews over a 5-year period. Those reviews consistently showed problems related to overall leadership and coordination, as discussed in this report.

Agency comments on GAO's other recommendations, along with GAO's evaluation, are presented at the end of chapters 2, 3, 4, 5, and 6. In some cases, agencies did not directly comment on recommendations that GAO made to them.

GAO also provided a draft of this report to state officials in Colorado and Utah for their review and comment. Officials representing Colorado's Office of Emergency Management and Utah's Olympic Public Safety Command concurred with those sections of GAO's report they reviewed regarding the Top Officials 2000 and Wasatch Rings exercises, respectively. The official from Utah strongly supported our recommendation that the President designate a single focal point. The official stated that it is critical that the focal point have adequate authority to carry out its responsibilities.

Chapter 1: Introduction

With the coordinated terrorist attacks against the World Trade Center in New York City and the Pentagon in Washington, D.C., on September 11, 2001, the threat of terrorism rose to the top of the country's national security and law enforcement agendas. Even before these catastrophic incidents, the threat of attacks against people, property, and infrastructures had increased concerns about terrorism. The terrorist bombings in 1993 of the World Trade Center in New York City and in 1995 of the Alfred P. Murrah Federal Building in Oklahoma City (see fig. 1), which killed 168 people and wounded hundreds of others, prompted increased emphasis on the need to strengthen and coordinate the federal government's ability to effectively combat terrorism domestically. Also, the 1995 Aum Shinrikyo sarin nerve agent attack in the Tokyo subway system raised new concerns about U.S. preparedness to combat terrorist incidents involving weapons of mass destruction (WMD)—a chemical, biological, radiological, or nuclear agent or weapon.[1]

[1]Throughout this report, we use the term weapons of mass destruction to refer to chemical, biological, radiological, or nuclear agents or weapons. Some agencies define it to include large conventional explosives as well. As clearly demonstrated by the September 11, 2001, incidents, a terrorist attack would not have to fit this definition of weapons of mass destruction to result in mass casualties, destruction of critical infrastructures, economic losses, and disruption of daily life nationwide.

Figure 1: Aftermath of the April 1995 Terrorist Bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma

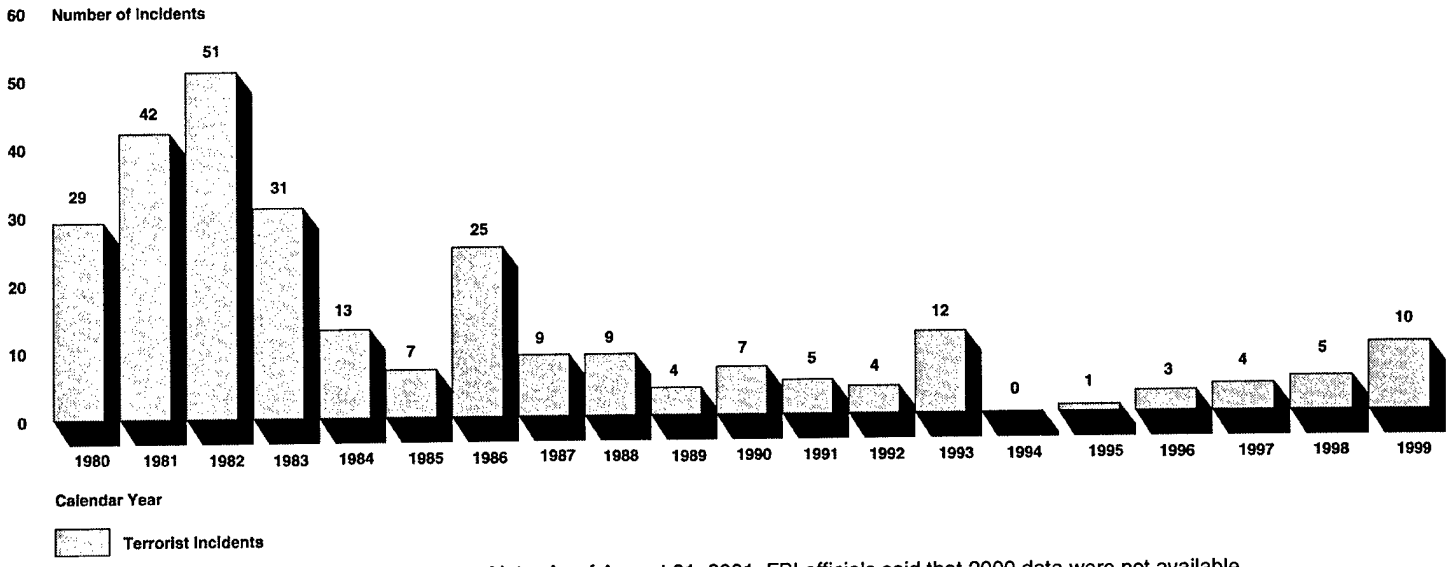
Source: Federal Emergency Management Agency.

U.S. intelligence and law enforcement communities continuously assess both foreign and domestic terrorist threats to the United States. The U.S. foreign intelligence community—the Central Intelligence Agency, the Defense Intelligence Agency, the Federal Bureau of Investigation (FBI), and the Department of State's Bureau of Research and Intelligence—monitors the foreign-origin terrorist threat to the United States. In addition, the FBI gathers intelligence and assesses the threat posed by domestic sources. According to the U.S. intelligence community, conventional explosives and firearms continue to be the terrorists' weapons of choice. Terrorists are less likely to use weapons of mass destruction, although the possibility that terrorists will use these weapons may increase over the next decade.

According to the FBI, during the 1990s, there were, on average, about five terrorist incidents in the United States each year.[2] In contrast, during the 1980s, there were, on average, 22 terrorist incidents in the United States each year. Figure 2 provides FBI statistics on the number of terrorist incidents in the United States between 1980 and 1999, five of which the FBI categorized as WMD incidents.

[2]The FBI broadly defines terrorism as "the unlawful use of violence, committed by a group of two or more individuals against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." The FBI includes in its annual reports on terrorism in the United States acts such as bombings, arson, kidnapping, assaults, and hijackings committed by persons who may be suspected of associating with militia groups, animal rights groups, and others.

Figure 2: Terrorist Incidents in the United States, 1980 to 1999



Note: As of August 31, 2001, FBI officials said that 2000 data were not available.

Source: FBI.

The Federal Government's Role in Combating Domestic Terrorism

U.S. policy and strategy for dealing with terrorism, along with the nature and perception of the terrorist threat, has been evolving over the past 30 years. A complex framework of programs and activities across more than 40 federal agencies, bureaus, and offices are in place to combat terrorism. The evolution of these programs came from a variety of presidential decision directives, implementing guidance, executive orders, interagency agreements, and legislation.[3] Formal interagency coordination intended to combat terrorism is managed by the National Security Council (NSC), which also sponsors a number of interagency working groups on terrorism issues.

The United States regards terrorist attacks against its territory, citizens, or facilities as a national security threat and criminal act, wherever the attack may occur. U.S. policy is to react rapidly and decisively to terrorism

[3]See app. I, which summarizes presidential decision directives, executive orders, and other guidance. Also see app. II, Selected Laws Related to Terrorism, in *Combating Terrorism: Federal Agencies' Efforts to Implement National Policy and Strategy* (GAO/NSIAD-97-254, Sept. 26, 1997), p. 73.

directed at the United States, whether it occurs domestically or internationally and whether it involves the use of conventional weapons or WMD devices. U.S. policy on combating terrorism for terrorist incidents overseas was formalized in 1986 under National Security Decision Directive 207. The Department of State was reaffirmed as the lead agency for international terrorism policy, procedures, and programs; and the FBI, through the Department of Justice, was reaffirmed as the lead agency for handling domestic terrorist threats. Following the April 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, the President issued Presidential Decision Directive (PDD) 39, which enumerated responsibilities for federal agencies in combating terrorism, including domestic incidents. In May 1998, the President reaffirmed PDD 39 with the issuance of PDD 62, which further articulated responsibilities for specific agencies. PDD 62 also established a National Coordinator for Security, Infrastructure Protection and Counterterrorism within the NSC, to coordinate agencies' programs. Both presidential decision directives and implementing guidance divide the federal response to terrorist attacks into two categories—crisis management and consequence management. Throughout the management of a terrorist incident, crisis and consequence management components operate concurrently. The concept of operations for a federal response to a terrorist threat or incident provides for an overall lead federal agency to ensure multi-agency coordination and a tailored, time-phased deployment of specialized federal assets. It is critical that all participating federal, state, and local agencies interact in a seamless manner.

Prior to an event involving a weapon of mass destruction or the release of biological, chemical, or nuclear/radiological material, crisis management activities and the achievement of law enforcement goals and objectives generally will have priority. However, consequence management planning to address the effects of a terrorist incident also will occur. When an incident results in the use of a weapon of mass destruction or the release of material, the execution of consequence management activities generally will have priority, with crisis management activities continuing until law enforcement goals and objectives have been met. Therefore, crisis and consequence management activities may overlap and/or run concurrently during the emergency response and are dependent upon the threat and/or strategies for responding to the incident.

The Department of State is the lead federal agency for crisis and consequence management of international terrorist incidents. Although the Department has a number of contingency arrangements and plans already in place to respond to a terrorist attack on U.S. interests abroad,

support for international crisis and consequence management comes from domestic assets. For example, Department of Defense (DOD); FBI; Bureau of Alcohol, Tobacco, and Firearms (ATF); Department of Health and Human Services (HHS); Environmental Protection Agency (EPA); or Department of Energy (DOE) teams could support overseas operations involving a WMD incident. Finally, a domestic terrorist incident may have significant international implications. For example, a domestic incident may involve a foreign terrorist organization or a biological terrorist incident could involve spreading the biological agent to virtually any city that has an international airport.

The Department of Justice, through the FBI, is the lead agency for crisis management of domestic terrorist incidents. The Department of Justice and the FBI manage and resolve a crisis resulting from a terrorist incident. They also conduct criminal investigations and pursue, arrest, and prosecute terrorists. When threats are communicated, particularly involving the use of weapons of mass destruction, the FBI initiates threat credibility assessments in close coordination with experts from other federal departments and agencies, such as DOD, DOE, HHS, EPA, and the Federal Emergency Management Agency (FEMA), to assess the threat from technical, operational, and behavioral perspectives. All federal agencies and departments, as needed, support the overall lead federal agency and the FBI on-scene commander.

Based on the preliminary threat assessment, the FBI Director, through the Attorney General, may authorize the deployment of a Domestic Emergency Support Team, which is comprised of those agencies that can advise or provide assistance to the FBI in managing the crisis on site. Upon the Attorney General's approval of the FBI's request, each agency's representatives are expected to be ready to deploy quickly.

In the event the President declares a national emergency, FEMA becomes the lead agency in charge of consequence management, which includes efforts to provide medical treatment and emergency services, evacuate people from dangerous areas, and restore government services. Unlike crisis management, the federal government does not have primary responsibility for consequence management; state and local authorities do. FEMA, using the Federal Response Plan, coordinates federal agencies' response and activities when the state and local authorities request

assistance.[4] Although state and local authorities will be the first to respond to a terrorist attack, any mass casualty-producing event would prompt a rapid, vigorous federal response, not just monitoring activity. The plan outlines the roles of other federal agencies, such as the Departments of Agriculture (USDA), Defense, Energy, Health and Human Services, Transportation, and Veterans Affairs (VA), and EPA, in consequence management covering a wide variety of contingencies, involving both conventional or WMD terrorists attacks.

The transition from crisis management to consequence management can occur in a variety of ways, although in general, both activities occur concurrently. If a terrorist incident becomes imminent or actually occurs, state and local authorities would initiate consequence management actions, while FEMA would monitor the situation. In the event state and local authorities become overwhelmed, the President could direct FEMA, with support of other federal agencies, to assist the state, in coordination with the FBI. Upon determination that applicable law enforcement goals and objectives have been met, no further immediate threat(s) exist(s), and federal crisis management actions are no longer required, the Attorney General, in consultation with the FBI Director and FEMA Director, will transfer the overall lead federal agency role to FEMA.

For fiscal year 2002, the federal government's proposed budget for these programs is over $12.8 billion, of which about $8.6 billion is to combat terrorism, about $1.8 billion is to combat weapons of mass destruction, and about $2.6 billion is for critical infrastructure protection (CIP).[5] Compared with the fiscal year 1998 funding level of about $7.2 billion, this proposed budget represents about a 78-percent increase in total funding to combat terrorism. In addition, the Congress recently approved the President's request for $20 billion in emergency assistance and provided an additional $20 billion to supplement existing contingency funds.

[4]The Federal Response Plan implements the authorities of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.) to respond to incidents or situations requiring federal emergency disaster assistance.

[5]The actual figures are $8.567 billion to combat terrorism, $1.766 billion for defense against weapons of mass destruction, and $2.595 billion for critical infrastructure protection. The total amount of $12.821 billion is the sum of these three categories less funding that overlaps categories.

Risks of Cyber-Attacks and Related Government Strategy

During the 1990s, concerns surfaced regarding computer-based attacks because of the nation's growing reliance on interconnected computer systems. Attacks could severely disrupt computer-supported operations, compromise the confidentiality of sensitive information, and diminish the integrity of critical data. A significant concern is that terrorists or hostile foreign states could severely damage or disrupt critical operations, resulting in harm to the public welfare.

In response to concerns about the potentially devastating implications of computer-based attacks, the President issued PDD 63 in May 1998, which described a range of activities to improve the nation's ability to detect and respond to serious physical and computer-based attacks. The directive called on the federal government to serve as a model of how infrastructure assurance is best achieved and designated "lead agencies" to work with private-sector and government entities in each of eight infrastructure sectors and five special function areas. In addition, PDD 63 established entities to provide central coordination and support and encourage private-sector cooperation. Chapter 6 contains a more detailed description of the directive's requirements and the organizations established to address critical infrastructure protection.

Objectives, Scope, and Methodology

Section 1035 of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (P.L. 106-398) mandated that we submit to the Senate and House Committees on Armed Services a report on the strategy, policies, and programs of the United States for combating domestic terrorism, particularly domestic terrorism involving weapons of mass destruction.

Based upon the act and, as agreed with your offices, our objectives were to evaluate (1) the current framework for leadership and coordination of federal agencies' efforts to combat terrorism on U.S. soil, and proposals for change, (2) progress the federal government has made in developing and implementing a national strategy to combat terrorism domestically, (3) the federal government's capabilities to respond to a domestic terrorist incident, (4) progress the federal government has made in helping state and local emergency responders prepare for a terrorist incident, and (5) progress made in developing and implementing a federal strategy for combating cyber-based attacks. This capping report updates and summarizes our extensive evaluations conducted in recent years of federal programs to combat domestic terrorism and protect critical infrastructures. A comprehensive list of GAO reports and testimonies related to terrorism appears at the end of this report.

The scope of this effort was governmentwide, including selected state and local emergency response agencies. A complete listing of organizations visited and contacted and locations visited are found in appendix VI.

The scope was limited to terrorist incidents on U.S. soil, whether foreign or domestic in origin. Our review did not include terrorist incidents outside of the United States or federal agencies' efforts to combat terrorism overseas. While we recognize that the role of intelligence and counter-intelligence for both operational and cyber issues is a key component of U.S. policies to combat terrorism, the scope did not include efforts by the U.S. intelligence community to gather and coordinate intelligence and counter-intelligence on terrorists, detect terrorist plans overseas, or respond to a terrorist incident. The scope also did not include efforts by the Immigration and Naturalization Service, U.S. Border Patrol, or U.S. Customs Service to prevent terrorists' entry into the United States. In addition, the report's discussion of DOD's terrorist response capabilities and assets is limited, since much of this information is classified.

For each objective, we interviewed agency officials, reviewed supporting documentation, compared current programs with our previous findings to review progress that has been made, reviewed about 30 of our prior counterterrorism reports, and followed up on findings and recommendations made in our previous reports (see app. V for the status of relevant prior GAO recommendations).

To evaluate the current framework for leadership and coordination of federal agencies' efforts to combat terrorism on U.S. soil, we conducted an analysis of interagency leadership and coordination functions and the roles and responsibilities of lead federal agencies and various interagency working groups. In addition, we reviewed a variety of proposals to change overall leadership and coordination, including various bills introduced in the U.S. House of Representatives and U.S. Senate, proposals contained in congressional committee reports, and related commissions. Also, we met with officials who helped prepare various commission reports that proposed changes to the leadership and coordination of federal counterterrorism efforts. Finally, we attended congressional briefings and hearings on terrorism issues and a national conference on WMD terrorism preparedness and response.

To evaluate what progress the federal government has made in developing a national strategy to combat terrorism domestically, we conducted an analysis of the process to develop and track budgets to combat terrorism, the Attorney General's Five-Year Interagency Counterterrorism and

Technology Crime Plan to determine whether it serves as a national counterterrorism strategy, agency response and concept of operation plans and their adequacy, interagency guidance, and agency threat and risk assessments.

To evaluate the federal government's capabilities to respond to a terrorist incident, we conducted an analysis of federal response teams and their missions, other support assets and specialized capabilities, how response teams and support assets are coordinated, the effectiveness of federal interagency exercise programs, and the status of research and development efforts and how they are coordinated.

To evaluate what progress the federal government has made in helping state and local emergency responders prepare for a terrorist incident, we conducted an analysis of how well federal agencies coordinate assistance to state and local emergency response agencies; how requirements are determined for training, equipment, and exercises; how well training and equipment are provided to and exercises conducted with state and local responders; whether training is provided efficiently and effectively; and whether exercises have tested the command and control system of federal, state, and local emergency responders. Also, we observed "Wasatch Rings," a multi-agency WMD field training exercise cosponsored by the FBI and the Utah Olympic Public Safety Command in preparation for the 2002 Olympic Winter Games in Salt Lake City, Utah. Regarding National Guard teams, we reviewed recent audit reports by GAO and the DOD Inspector General, reviewed testimony from related congressional hearings, and held discussions with state and local officials.

To evaluate federal efforts to combat computer-based attacks, we conducted an analysis of progress made in implementing PDD 63 to protect critical federal systems and ensure protection of private and other non-federal critical systems. We also surveyed related research and development. To accomplish this, we reviewed reports related to PDD 63, including the

- President's Council on Integrity and Efficiency/Executive Council on Integrity and Efficiency (PCIE/ECIE) report on federal implementation of PDD 63, March 2001;
- Report of the President of the United States on the Status of Critical Infrastructure Protection Activities, January 2001;
- Individual agency inspector general reports; and

- Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to Dialogue, The White House, January 2000.

We also reviewed CIP plans and other relevant documents and interviewed key officials from the Departments of Commerce, Defense, Energy, Health and Human Services, Justice, State, Transportation, and the Treasury and the EPA, FEMA, and General Services Administration. In addition, we interviewed officials from the NSC, Office of Science and Technology Policy (OSTP), and Critical Infrastructure Assurance Office (CIAO), as well as representatives from the banking and finance and emergency law enforcement infrastructure sectors.

We performed our review from December 2000 through August 2001 in accordance with generally accepted government auditing standards.

Chapter 2: Overall Leadership and Coordination Responsibilities Need to Be Centralized and Clarified

Because of the interagency and intergovernmental nature of programs to combat terrorism, certain leadership and coordination functions are needed above the level of individual agencies. These include, among others, overseeing a threat and risk assessment, developing a national strategy, monitoring governmentwide budgets, and coordinating agency implementation. The President established, within the NSC, a national coordinator for terrorism, with general responsibilities to coordinate federal activities. However, the coordinator was not specifically given responsibilities for all the requisite leadership and coordination functions. Further, these functions are fragmented across different organizations and some individual agencies are performing functions that would be more appropriately coordinated above that level. The Congress and the President also have expressed concerns about the overall leadership and coordination of programs to combat terrorism. The Congress and various commissions have proposed several changes to create a single focal point for overall leadership and coordination and to centralize key functions within it. These proposals vary in their scope of coverage and their location for the focal point. The proposals generally place their focal point in either the Executive Office of the President or in a lead executive agency. Each location has its advantages and disadvantages. These proposals also vary in the interagency functions they centralize within the focal point. Because overall leadership and coordination must encompass both crisis and consequence management programs, we believe that the single focal point for overall leadership and coordination would be most effective in the Executive Office of the President rather than in any executive agency. While we do not endorse any specific model for the single focal point, we have identified basic characteristics and functions for such a focal point.

Some Leadership and Coordination Functions Transcend Individual Agencies

The challenge to provide overall leadership and coordination of federal programs to combat terrorism is significantly affected by several factors. First, there are numerous federal agencies—more than 40—which have some role in combating terrorism. Second, these federal agencies represent different types of organizations, including those involved in intelligence, law enforcement, military matters, health services, environmental protection, emergency management, and diplomacy.[1]

[1]Activities involving diplomacy, carried out by the Department of State, are relevant to the extent that some domestic terrorist incidents could have a foreign origin and/or international implications.

Agencies' missions often include both domestic and international components. In addition, these agencies undertake a wide variety of activities to combat terrorism, including prevention, detection, crisis response, criminal prosecution, and consequence management, which require effective interagency coordination. Further, because terrorist incidents could potentially occur anywhere in the United States, federal efforts to combat terrorism must be intergovernmental to include state and local governments. As a result of these factors, no individual agency is in charge of all relevant capabilities needed to combat terrorism. These factors make it important that certain overall leadership and coordination functions are performed above the level of individual agencies. Examples of such functions that we have identified in the course of our previous work are as follows:[2]

- Act as the top official accountable to the President and the Congress.
- Oversee a national threat and risk assessment.
- Lead the development of a national strategy.
- Set priorities within the national strategy.
- Coordinate and monitor international programs.
- Provide liaison and assistance to state and local governments.
- Monitor governmentwide budgets across federal agencies.
- Develop and monitor overall performance measures.
- Coordinate overall research and development.

National Coordinator Established, but Some Responsibilities Are Fragmented Across Agencies

In May 1998, the President issued PDD 62, which established the position of a National Coordinator for Security, Infrastructure Protection and Counterterrorism at the NSC within the Executive Office of the President to provide a focal point for federal efforts to combat terrorism. Part of the rationale for creating this National Coordinator was to improve leadership and coordination among the various federal agencies. The directive enumerated responsibilities for the coordinator that included general coordination of federal efforts, chairing certain meetings, sponsoring interagency working groups, and providing budget advice. Many efforts of the Office of the National Coordinator have been positive and are discussed later in this report. Specific examples include tracking budgeting and spending and the activities of some of the working groups.

[2]See *Combating Terrorism: Comments on Bill H.R. 4210 to Manage Selected Counterterrorist Programs* (GAO/T-NSIAD-00-85, May 4, 2000) and *Combating Terrorism: Observations on Options to Improve the Federal Response* (GAO-01-660T, Apr. 24, 2001).

However, other than the general responsibilities identified in PDD 62, the functions of the National Coordinator were never detailed in either an executive order or legislation. Many of the overall leadership and coordination functions we have identified as critical were not given to the National Coordinator. In fact, several other agencies have these leadership and coordination functions, such as the Department of Justice, the FBI, FEMA, and the Office of Management and Budget (OMB). Some of the functions currently resident in different agencies include completing a threat and risk assessment, developing a national strategy, providing liaison to state and local governments, and developing and monitoring performance measures. Officials from a number of agencies that combat terrorism have indicated to us that the interagency roles of these various agencies are not always clear and sometimes overlap, leading to a fragmented approach. Table 1 below shows that several of the key leadership and coordination functions are spread across different or multiple agencies.

Table 1: Organizations Currently Responsible for Key Interagency Leadership and Coordination Functions for Programs to Combat Terrorism

Key interagency leadership and coordination function	Current organization responsible for the function
Act as the top official accountable to the President	NSC (National Coordinator for Security, Infrastructure Protection and Counterterrorism), as appointed by the President in PDD 62.
Act as the top official accountable to the Congress	Numerous officials (including the Attorney General, Director of the FBI, Secretary of State, and Secretary of Defense) who testify before the Congress on these matters.
Oversee a national threat and risk assessment	FBI. See ch. 3 for more information on this function.
Lead the development of a national strategy	Attorney General (other offices also have discussed doing this). See ch. 3 for more information on this function.
Set priorities within a national strategy	OMB, on behalf of the President, is required to identify priorities in its annual reports; to date, it has not done so. See ch. 3 for more information on this function.
Coordinate and monitor international programs	Secretary of State (via Coordinator for Counterterrorism).
Provide liaison and assistance to state and local governments	Department of Justice (the Office for State and Local Domestic Preparedness Support and the National Domestic Preparedness Office) and FEMA. See ch. 5 for more information on this function.
Monitor budgets across federal agencies	NSC and OMB. See ch. 3 for more information on this function.
Develop and monitor overall performance measures	No agency assigned to do this overall task. See ch. 3 for more information on this function.
Coordinate overall research and development	NSC (via the Preparedness Against Weapons of Mass Destruction Research and Development Subgroup). See ch. 4 for more information on this function.

Source: GAO analysis of interagency functions to combat terrorism.

The current fragmented placement of these functions limits accountability and hinders unity of effort. To the extent that a single focal point—such as the current National Coordinator or other proposed focal points as discussed later in this chapter—is assigned these functions and held accountable for them, more progress might be made in developing and advancing federal efforts to combat terrorism. Our analysis indicates that the following deficiencies discussed in this report are due, in part, to the current fragmented structure for overall leadership and coordination.

- Overall Accountability. In some cases, the President and the Congress have held different officials accountable for interagency functions. For

example, while the President appointed a national coordinator, the Congress directed a different official, the Attorney General, to develop an interagency strategy (see ch. 3).

- Threat and risk assessment. There has been only limited progress in the 3 years since the FBI agreed to perform an assessment; meanwhile, agencies may continue to expend resources for less likely threats and worst case chemical, biological, radiological, or nuclear scenarios (see ch. 3).
- National strategy. A strategy was developed by the Department of Justice, but it does not have measurable outcomes and should include the roles of state and local governments to truly become a national strategy. Also, other agencies may be developing competing "national" strategies (see ch. 3).
- Monitoring budgets. OMB, working with the National Coordinator, has made progress in tracking and analyzing agency funding to combat terrorism. However, these offices have not identified priorities or duplication (see ch. 3). Also, there is no clear linkage between these budgets and the implementation of a national strategy (see ch. 3).
- Tracking and Implementing Lessons Learned. An interagency working group is responsible for planning exercises that combine federal efforts and practice coordination with state and local governments. While this group has made some attempts to develop a system for tracking lessons learned from these exercises, the process is not standardized and varies from exercise to exercise (see ch. 4).
- Coordinating agency implementation. Different agencies developed programs to provide assistance to state and local governments that are similar and potentially duplicative. These multiple programs have created confusion and frustration among state and local officials (see ch. 5).

National efforts to combat illegal drugs offer potential lessons in addressing the overall leadership and coordination of interagency efforts to combat terrorism. There are similarities between combating illegal drugs and combating terrorism in terms of the number of agencies, disciplines, and activities, and the intergovernmental nature of the effort. The Congress created the Office of National Drug Control Policy in 1988 because fragmentation had hampered federal efforts to share information and coordinate programs. The Congress wanted strong, centralized leadership so the Office was located within the Executive Office of the President where it could rise above the particular interests of any one federal agency. The duties of the Office are to (1) develop a national drug control strategy containing both long- and short-term objectives, which is revised annually; (2) develop an annual consolidated drug control budget providing funding estimates for implementing the strategy; and (3) oversee and coordinate implementation of the strategy by the various federal

agencies. The Office, however, is not responsible for implementing the strategy—that is the role of individual agencies. Despite continuing difficulties in combating illegal drugs, the Office has set up a useful framework for leadership and coordination, and we supported its reauthorization in 1998. Most of the interagency leadership and coordination functions that we believe are needed for combating terrorism are resident in the Office of National Drug Control Policy structure. Moreover, through legislation, the Office has the legitimacy and authority to carry out these functions.

The Congress and the President Also Are Concerned About Leadership and Coordination

Both the Congress and the President have expressed concerns about the overall leadership and coordination of programs to combat terrorism. The Congress has demonstrated its concerns by holding hearings, appointing commissions, and introducing various bills. The President has demonstrated concern by recently appointing the Vice President to oversee domestic preparedness efforts and by establishing an Office of National Preparedness within FEMA to coordinate all federal programs dealing with WMD consequence management programs.

The Congress Shows Concern Through Hearings, Commissions, and Legislation

The Congress has expressed concerns about the overall leadership and coordination of programs to combat terrorism. Congressional committees have demonstrated this concern through a variety of hearings, committee reports, proposed legislation, and congressionally chartered commissions to examine programs related to terrorism. Examples of these are as follows:

- Multiple hearings have been held in the last several years that addressed problems in coordinating programs related to terrorism. These include hearings by the House Committee on Government Reform, House Committee on Armed Services, House Committee on Transportation and Infrastructure, Senate Committee on Governmental Affairs, Senate Committee on Appropriations, Senate Committee on Armed Services, Senate Select Committee on Intelligence, or their related subcommittees.
- Several legislative bills have been introduced in the last few years to resolve problems in coordinating programs related to terrorism. These bills included H.R. 4210, the Terrorism Preparedness Act of 2000; H.R. 525, the Preparedness Against Domestic Terrorism Act of 2001; H.R. 1158, the National Homeland Security Act; and H.R. 1292 the Homeland Security Strategy Act of 2001. In addition, laws have been passed that addressed improvements in programs related to terrorism.
- The Congress established three separate commissions to examine, among other things, problems coordinating programs related to terrorism. These

include the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (also known as the Gilmore Panel because it was chaired by Governor James Gilmore III of Virginia); the United States Commission on National Security in the 21st Century (also known as the Hart-Rudman Commission because it was chaired by former Senators Gary Hart and Warren Rudman); and the National Commission on Terrorism (also known as the Bremer Commission because its Chairman was former Ambassador Paul Bremer).[3] More details on these legislative proposals and commission recommendations appear below and in table 2.

President Appointed Vice President to Oversee National Effort

The President also has expressed concerns that efforts to protect the United States against a WMD weapon must have maximum effectiveness and be seamlessly integrated, harmonious, and comprehensive. In May 2001, the President asked the Vice President to oversee the development of a coordinated national effort on these matters. According to the Office of the Vice President, as of August 31, 2001, details on the Vice President's efforts had not yet been determined. While it is not yet clear what specific areas the Vice President will be responsible for, agencies involved do not anticipate that this position will be permanent or provide overall leadership and coordination of federal efforts to combat terrorism. The President also asked the Director of FEMA to create a new Office of National Preparedness to assist the Vice President in implementing a national strategy on consequence management. This new Office, which was established in July 2001, was created to coordinate all federal programs dealing with WMD consequence management.

Different Proposals on Leadership and Coordination Have Their Pros and Cons

Several proposals have been advanced to improve the overall leadership and coordination of programs to combat terrorism. These approaches generally create a single focal point located in either the Executive Office of the President or a lead executive agency. Each location has its advantages and disadvantages.

[3]The Bremer commission was focused on international terrorism. As noted earlier, international matters are relevant to the extent that some domestic terrorist incidents could have a foreign origin.

Several New Proposals on Leadership and Coordination

Several new proposals have been advanced—through proposed legislation, committee reports, or various commissions—to change the overall leadership and coordination of programs to combat terrorism. All of these proposals provide for a focal point for the overall leadership and coordination of programs to combat terrorism. The proposals provide the focal point with different, but often similar, functions to centralize the interagency leadership and coordination of federal programs. However, the various proposals differ in the scope of their coverage. Some limit the scope to domestic preparedness, others to all programs to combat terrorism, and still others to the larger issue of homeland security that encompasses threats other than terrorism, such as military attacks. The proposals also vary as to the location of the focal point. They generally place the focal point in either the Executive Office of the President or in a lead executive agency. Table 2 shows various proposals regarding the focal point for overall leadership, the scope of the focal point's activities, and its location.

Table 2: Proposals to Create a Focal Point for Overall Leadership and Coordination of Programs to Combat Terrorism

Source of proposal	Focal point for overall leadership	Scope of responsibilities	Location of focal point
H.R. 4210 (original version)	Office of Terrorism Preparedness	Domestic terrorism incidents involving weapons of mass destruction	Executive Office of the President
H.R. 525	President's Council on Domestic Terrorism Preparedness	Domestic terrorism preparedness (consequence management only)	Executive Office of the President
H.R. 1158	Cabinet-level head of proposed National Homeland Security Agency	Homeland security (including domestic terrorism, maritime and border security, disaster relief, and critical infrastructure activities)	Lead executive agency (National Homeland Security Agency)
H.R. 1292	Single official to be designated by the President	Homeland security (including antiterrorism and protection of territory and critical infrastructures from unconventional and conventional threats by military or other means)	To be determined based upon the President's designation
Senate Report 106-404	Deputy Attorney General for Combating Counterterrorism	Domestic terrorism preparedness (crisis and consequence management)	Lead executive agency (Department of Justice)
Gilmore Panel	National Office for Combating Terrorism	Domestic and international terrorism (crisis and consequence management)	Executive Office of the President
Hart-Rudman Commission	Cabinet-level head of proposed National Homeland Security Agency	Homeland security (including domestic terrorism, maritime and border security, disaster relief, and critical infrastructure activities)	Lead executive agency (National Homeland Security Agency)
Center for Strategic and International Studies	Assistant to the President or Vice President for Combating Terrorism	Homeland Defense (including domestic terrorism and critical infrastructure protection)	Executive Office of the President

Source: GAO analysis of various proposals.

Various Locations for Focal Point Have Pros and Cons

The two locations for the focal point have their pros and cons. Table 3 summarizes the advantages and disadvantages of placing the single focal point within the Executive Office of the President versus within a lead executive agency.

Table 3: Advantages and Disadvantages of Various Leadership Approaches

Location	Advantages	Disadvantages
Focal point within the Executive Office of the President	• Would be positioned outside the particular interests of any one federal agency • Would be located close to the President to resolve cross agency disagreement • Could increase coordination and accountability while leveraging expertise located in different agencies	• Could potentially interfere with operations conducted by the respective executive agencies • Could hinder direct communications between the President and the cabinet officer in charge of the respective executive agencies
Focal point within a lead executive agency	• Would provide a clear and streamlined chain of command within agency in matters of policy and coordination • Could have better access to President than a mid-level focal point within the Executive Office of the President	• Would lack autonomy • Would have other major missions and duties that might distract the focal point from combating terrorism • Could be viewed by other agencies as parochial rather than working in the collective best interest

Source: GAO analysis.

In contrast to these proposals, the current system is a hybrid approach because it combines leadership and coordination responsibilities in both the Executive Office of the President and specific lead executive agencies. As shown previously in table 1, many of the key interagency leadership and coordination functions are fragmented because they are spread across different organizations. Two of the proposals (the original H.R. 4210 and the Gilmore Panel) model their focal point after the Office of National Drug Control Policy because of its centralized approach to overall leadership and coordination.

Focal Point Should Be Located in the Executive Office of the President

Based upon years of evaluations, the fragmentation of leadership and coordination (as discussed above and throughout this report), and our assessment of the various proposals, our analysis indicates there needs to be a single focal point with responsibility for all critical functions to lead and coordinate these programs.[4] Furthermore, the focal point should be in the Executive Office of the President and be independent of any existing

[4]A list of our reports and testimonies related to terrorism appears at the end of this report.

federal agency. Such a position would allow the focal point to be outside the interests of any individual agency. Proposals to create a focal point within a lead agency—whether the Department of Justice or FEMA—would not allow the focal point to have the governmentwide perspective needed. Specifically, the focal point needs to be above both crisis and consequence management. In addition, creating a new agency to combine functions currently in several agencies—such as the proposed National Homeland Security Agency—still would not contain all the government agencies and functions needed to combat terrorism.[5]

Notwithstanding our belief that the focal point should be in the Executive Office of the President, the exact structure for the focal point could vary. The various proposals potentially make this focal point a new office (e.g., the proposed National Office for Combating Terrorism) or a council (e.g., the proposed President's Council on Domestic Terrorism Preparedness) or a person (e.g., the proposed Assistant to the President for Combating Terrorism). The current National Coordinator within the NSC also could potentially serve as the focal point if it were clearly responsible for the key functions we have identified.

Conclusions

Key interagency functions are resident in several different organizations, resulting in fragmented leadership and coordination. These circumstances hinder unity of effort and limit accountability. However, the current attention being focused on this issue provides an opportunity to improve the overall leadership and coordination of programs to combat terrorism. The Congress has introduced various bills to create a focal point for terrorism-related efforts. Several commissions and research organizations, some of which were chartered by the Congress, also have recommended major changes to the manner in which terrorism-related programs are led and coordinated. The President has expressed concerns over current efforts and recently has tasked the Vice President to review these activities across the government. While there are many proposals to create a focal point, there is no clear consensus on where the focal point should be located or what responsibilities it should have. Given the consensus

[5]The Hart-Rudman Commission, and subsequently H.R. 1158, called for the creation of a National Homeland Security Agency, which would combine several existing agencies from different departments, including FEMA (its regional offices), the Department of the Treasury (U.S. Customs Service), the Department of Justice (U.S. Border Patrol), the Department of Transportation (U.S. Coast Guard), and several elements from other departments.

that there is a need to address the overall leadership and coordination issues, and the uncertainty about the location of the focal point for these matters, we are making our recommendations to the President of the United States. In our view, the President and the Congress need to work together to implement a governmentwide solution on overall leadership and coordination to combat terrorism. We believe the President, in conjunction with the Vice President's overall assessment, should clearly determine the responsibilities and functions of this critical focal point and place the authority for them within the focal point.

Recommendations for Executive Action

We recommend that the President, in conjunction with the Vice President's efforts, appoint a single focal point that has the responsibility and authority for all critical leadership and coordination functions to combat terrorism. The focal point should have the following characteristics and responsibilities.

- The focal point should be in the Executive Office of the President, outside individual agencies, and encompass activities to include prevention, crisis management, and consequence management.
- The focal point should oversee a national-level authoritative threat and risk assessment on the potential use of weapons of mass destruction by terrorists on U.S. soil. Such assessments should be updated regularly.
- The focal point also should lead the development of a national strategy for combating terrorism. The current Attorney General's Five-Year Plan could serve as an initial point of departure with revisions to include measurable outcomes and the roles and participation of state and local governments. In addition, the national strategy should include research and development priorities and needs in order to facilitate interagency coordination, decrease duplication, and leverage monetary resources.
- The focal point should coordinate implementation of the national strategy among the various federal agencies. This would entail reviewing agency and interagency programs to ensure that they are being implemented in accordance with the national strategy and do not constitute duplication of effort.
- The focal point should analyze and prioritize governmentwide budgets and spending to combat terrorism to eliminate gaps and duplication of effort. The focal point's role will be to provide advice or to certify that the budgets are consistent with the national strategy, not to make final budget decisions.
- The focal point should coordinate the nation's strategy for combating terrorism with efforts to prevent, detect, and respond to computer-based attacks on critical infrastructures. We do not see the focal point for

combating terrorism with responsibility for also protecting computer-based infrastructures because the threats are broader than terrorism and such programs are more closely associated with traditional information security activities. Nonetheless, there should be close coordination between the two areas.

- The focal point should be established by legislation to provide it with legitimacy and authority and its head should be appointed by the President with the advice and consent of the U.S. Senate. This would provide accountability to both the President and the Congress. Also, it would provide continuity across administrations.
- The focal point should be adequately staffed to carry out its duties for planning and oversight across the federal government.

While some of the details of these interagency functions could be delegated to other agencies, the focal point should retain overall responsibility and be held accountable for their implementation.

Agency Comments and Our Evaluation

Agency comments on a draft of this report were based on their efforts prior to the September 11, 2001, terrorist attacks. The Departments of Energy and Transportation agreed with our recommendation that the President appoint a single focal point for all critical leadership and coordination functions to combat terrorism. DOE agreed that a single responsible and accountable "focal point" for combating terrorism should be established, independent of any existing federal agency. DOE said that regardless of where this entity is placed, it should be given the authority to cut across agency lines with a clear set of obtainable goals and milestones. The key to its success will be strong leadership, an organization with a sense of purpose, and access to the tools necessary to do the job. Similarly, Department of Transportation officials believe the report makes a reasonable case for a single point of focus for terrorism issues in the Executive Branch.

The Department of Justice disagreed with our recommendation to create a single focal point with specific functions. The Department said that the National Coordinator at the NSC was working in a "manner that recognizes the unique roles and contributions of each agency to the overall effort." In its view, there is no need to change or expand that role at this time. Moreover, the Department stated that our recommendation was premature in light of the Vice President's pending review. We agree that the National Coordinator at the NSC has made some important contributions. However, this position's responsibilities are not clearly defined and it lacks responsibilities for some overall leadership and

coordination functions that it should have. With respect to the Vice President's pending review, our recommendation states that the President should make the appointment working with the Congress and in conjunction with the Vice President's efforts.

The Executive Office of the President did not comment on this recommendation. OMB referred us to the President's May 8, 2001, statement (see app. VII) in which he tasked the Vice President with overseeing the development of a coordinated national effort to improve national preparedness. Most agencies did not comment directly on our recommendation that the President create a single focal point. Officials from these other agencies indicated that it would be premature for them to comment on the recommendation in deference to the Vice President's review of national preparedness. We disagree that our recommendation for a single focal point is premature. Notwithstanding the Vice President's pending review, our recommendation is based upon our own reviews over a 5-year period. Our reviews consistently showed problems related to overall leadership and coordination, as discussed in this report.

Chapter 3: Progress Made in Developing a National Strategy to Combat Domestic Terrorism

The federal government has made progress in recent years in developing a national strategy to combat terrorism, but several key components still are not complete or are missing. In the past, we have recommended that the federal government conduct a terrorist threat and risk assessment to establish requirements and prioritize program investments. The Department of Justice and the FBI have made some progress in implementing our recommendations. The Attorney General's Five-Year Plan represents a substantial interagency effort and is the one document that could serve as the basis for a national strategy. However, it lacks two critical elements: measurable outcomes and identification of state and local government roles. In the past, the amount of funds being spent to combat terrorism was unknown and difficult to determine. Now, OMB is tracking counterterrorism budgets and expenditures and issuing annual reports to the Congress—a significant step toward improving the management and coordination of these programs and activities. Nonetheless, the NSC and OMB have not identified priorities or reported on duplication of efforts. Finally, consistent with our prior recommendations, agencies now have completed interagency guidance to combat domestic terrorism, clarified command and control issues, and completed or are developing internal guidance and concepts of operations to manage terrorist incidents.

Threat Assessments Are Being Completed

An important step in developing sound programs to combat terrorism is to develop a thorough assessment of the terrorist threat. 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 also have the intention and capability to launch attacks.[1]

The intelligence community (both foreign and domestic agencies) reports an increased possibility that terrorists may use weapons of mass destruction in the next decade. However, there are several qualifications to this threat. For example, 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

[1]Other factors to consider in analyzing threats include a terrorist group's history, its targeting, and the security environment in which it operates.

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. 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 WMD materials.

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.[2] 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, many agencies have been relying on worst case chemical, biological, radiological, or nuclear scenarios to generate countermeasures or establish their programs. By using these worst case scenarios, the federal government is focusing on vulnerabilities (which are unlimited) rather than credible threats (which are limited).

The Department of Justice and the FBI have made some progress in implementing our recommendations that threat and risk assessments be done at both the local and national level.

Progress Made in Completing State and Local Assessments

Regarding local threat and risk assessments, the Department of Justice's 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.[3] This tool includes a step-by-step methodology for

[2]*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 Attack* (GAO/NSIAD-99-163, Sept. 7, 1999).

[3]*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.

assessing threats, risks, and requirements. It also includes information on how to prioritize programs and project spending amounts. Department of Justice officials told us that, as of August 31, 2001, four states had completed these assessments. The information from the risk and needs assessment will be used to develop statewide domestic preparedness strategic plans. The statewide assessment process includes an initial risk assessment and identification of the most likely scenarios. This risk assessment is the culmination of three other assessments: threat, vulnerability, and public health assessments. This design feature enables the preparedness programs to focus resources on preparing for the "most likely" scenarios. The Department plans to use the results of these assessments to drive the allocation of its equipment, training, and exercise program resources, which is consistent with previous GAO recommendations. Department of Justice officials stated that the systematic collection of these data is an unprecedented undertaking to remedy the federal government's current reliance on anecdotal information. They view the state assessments as being profoundly useful in presenting a national picture of preparedness and priorities. Thus, these officials believe that the compilation of all the state assessments and plans can be a foundation for a national domestic preparedness strategy.

National-Level Threat Assessments Are Underway

Regarding our 1999 recommendations for national-level authoritative threat and risk assessments, the FBI agreed to lead two assessments. However, the FBI noted some limitations to its methodology for producing such assessments in the domestic context. For example, the FBI stated that its law enforcement role placed limitations on its collection and use of intelligence data. FBI officials also said that they had little intelligence on specific domestic terrorist groups. They said the largest domestic threat is the "lone wolf" terrorist—an individual who operates alone and thus is difficult to identify or collect intelligence on. When the FBI has credible intelligence on a specific terrorist, it would make an arrest first and analyze the intelligence afterwards. FBI officials also noted that these would be threat assessments—not risk assessments.

The first threat assessment that the FBI is doing is a report on those chemical and biological agents that may be more likely to be used in the United States by a terrorist group that was not state sponsored (e.g., terrorist groups without access to foreign government chemical or biological stockpiles, production capabilities, or funding). Because of the limitations on intelligence discussed above, the FBI decided to focus on such WMD agents. While not identifying specific terrorist groups, this assessment would still be useful in determining requirements for programs

to combat terrorism. Once FBI officials became aware of a similar assessment being conducted jointly by the Department of Justice's National Institute of Justice and the Technical Support Working Group (TSWG), the FBI became a co-sponsor.[4] This report will be provided to state and local governments to help them conduct their own threat and risk assessments and reduce their vulnerabilities. The Department of Justice anticipated that a draft of the assessment would be available for interagency review and comment in September 2001 and the final assessment would be published in December 2001.

The second threat assessment is a national-level threat assessment of the terrorist threat in the United States. According to the Department of Justice, the FBI is in the process of conducting such an assessment. It will be a comprehensive assessment that encompasses domestic terrorism, international terrorism, WMD terrorism, cyber-terrorism, and proliferation. The report will assess the current threat, the projected threat, emerging threats, and related FBI initiatives. The Department stated that this assessment is being finalized and anticipated that the classified report would be published in October 2001.

While not fully responsive to our recommendation that threat *and risk* assessments be done, we are hopeful that these threat assessments by the FBI, once completed, will set priorities and help guide federal programs to combat terrorism. In our draft report, we raised concerns that the FBI was not going to coordinate these threat assessments with other intelligence agencies. The Department of Justice indicated that these assessments will be fully coordinated before publication.

[4]TSWG conducts the national interagency research and development program for combating terrorism. TSWG and its coordination role are discussed in more detail in chapter 4.

Attorney General's Five-Year Plan Represents a Substantial Effort, but Key Elements Still Are Lacking for a National Strategy

As we have noted in our prior work, a national strategy on combating terrorism is needed that has a clear outcome or goal against which performance can be measured.[5] The Attorney General's Five-Year Interagency Counterterrorism and Technology Crime Plan, issued in December 1998, represents a substantial interagency effort and is the one document that could serve as a basis for a national strategy. However, we believe it lacks two critical elements: (1) measurable outcomes and (2) identification of state and local government roles in responding to a terrorist incident.

Five-Year Plan Serves as a Baseline for a National Strategy to Combat Terrorism

A national strategy should provide a clear statement as to what the nation hopes to achieve through its programs to combat terrorism. A national strategy should not only define the roles and missions of federal, state, and local governments, but also establish objectives, priorities, outcome-related goals with milestones, and performance measures. A national strategy should incorporate the principles of the Government Performance and Results Act of 1993, which requires federal agencies to set strategic goals, measure performance, and report on the degree to which goals are met.[6] Further, the Department of State emphasized that a national strategy also has to be comprehensive, that is, it must include the international component.

The Congress directed the Attorney General to develop the Five-Year Plan to serve as a baseline strategy for coordination of national policy and operational capabilities to combat terrorism in the United States and against American interests overseas.[7] Department of Justice officials believe that this plan, in combination with several related presidential decision directives, represents a comprehensive national strategy. The classified plan identifies several high-level goals aimed at preventing and deterring terrorism, maximizing international cooperation to combat terrorism, improving domestic crisis and consequence planning and management, improving state and local capabilities, safeguarding

[5]See *Combating Terrorism: Linking Threats to Strategies and Resources* (GAO/T-NSIAD-00-218, July 26, 2000), p. 7.

[6]P.L. 103-62 (Aug. 3, 1993).

[7]See the Conference Committee Report (House Report 105-405, Nov. 13, 1997) accompanying the Fiscal Year 1998 Appropriations Act for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies (P.L. 105-119, Nov. 26, 1997).

information infrastructure, and leading research and development efforts to enhance counterterrorism capabilities. It sets forth current and projected efforts by the Attorney General in partnership with other federal agencies and state and local entities to improve readiness to address the terrorist threat.

In September 1999, the Attorney General released an unclassified edition of the Five-Year Plan, which was distributed to state and local governments. In addition, the Attorney General issues an annual update to the Five-Year Plan, which tracks agencies' progress. The annual updates do not revise the basic Five-Year Plan.

Five-Year Plan Focuses on Outputs, Not Outcomes

A national strategy on combating terrorism needs a clear outcome or goal against which performance can be measured. Although the Attorney General's Five-Year Plan links performance to objectives, it focuses on agency activities representing outputs rather than results-oriented outcomes.

In 1993, the Congress enacted the Government Performance and Results Act (commonly referred to as the Results Act). The legislation was designed to have agencies focus on the performance and results of their programs rather than on program resources and activities, as they had done in the past. Thus, the Results Act became the primary legislative framework through which agencies are required to set strategic goals, measure performance, and report on the degree to which goals are met. The outcome-oriented principles of the Results Act include (1) establishing general goals and quantifiable, measurable, outcome-oriented performance goals and related measures; (2) developing strategies for achieving the goals, including strategies for overcoming or mitigating major impediments; (3) ensuring that goals at lower organizational levels align with and support general goals; and (4) identifying the resources that will be required to achieve the goals. Moreover, in its guidance on implementing the Results Act, the Chief Financial Officers Council advised agencies that to comply with the spirit and intent of the act, the goals and measures used at lower organizational levels should be linked with the agency's strategic goals.

According to the Department of Justice, the Fiscal Year 1999 Update to the Five-Year Plan reports outcomes that can be used to gauge progress. For example, the FBI, FEMA, and the U.S. Secret Service are working together to coordinate the planning of special events (see a more detailed discussion of this cooperation in ch. 4). The FBI determined that bomb

squads need radiological monitors and personal protective equipment and it is providing that equipment to every accredited bomb squad in the United States. OSTP established an annual process to develop and coordinate broad national technical goals and priorities to combat terrorism. The Fiscal Year 2000 Update to the Five-Year Plan also cited completed measurable outcomes. For example, the Department of Justice drafted proposed Sentencing Guidelines for the Biological Weapons Anti-Terrorism Act of 1989.[8] HHS designed and developed a national pharmaceutical stockpile and delivery system. The Department of Justice began detailing Assistant U.S. Attorneys to the Criminal Division to develop prosecutive expertise in computer crime investigations.

While the Department of Justice considers these outcomes, we consider them outputs, since they represent agency activities rather than the results that agency activities would achieve. While these Department of Justice examples of measurable outputs are important, the plan does not have a defined outcome of where the nation should be in terms of domestic preparedness and capabilities within a specified period of time. Such an outcome would be useful in establishing requirements and priorities. While the plan lays out goals for preparedness, it does not attempt to (1) define the level(s) of preparedness necessary to handle a weapon of mass destruction incident, (2) determine how much preparedness is enough given the terrorist threat, or (3) identify what level of risk is desirable—or attainable.

If the Department of Justice applied the Results Act principles to the Five-Year Plan—and ultimately to a national strategy to combat terrorism—then we believe all performance indicators could be measured and a defined outcome of where the nation should be in terms of domestic preparedness and capabilities within a certain time frame could help establish counterterrorism program requirements and priorities. The result would be a more rational and efficient counterterrorism effort governmentwide.

Five-Year Plan Does Not Identify Roles for State and Local Governments

Although the Department of Justice obtained state and local input in preparing the Five-Year Plan and identifies specific ways to enhance state and local responder capabilities, the plan does not identify state and local government roles in responding to a terrorist incident. According to the

[8]P.L. 101-298 (May 22, 1990).

Department of Justice, state and local input was obtained through (1) a Stakeholders Forum held in 1998 for state and local jurisdictions concerning response incidents of domestic terrorism, (2) a questionnaire distributed by national associations representing the state and local emergency preparedness community to a cross-section of their constituencies, (3) the Inventory of State and Local Law Enforcement Technology Needs to Combat Terrorism, (4) a 1998 study funded by the National Institute of Justice, and (5) the State and Local Experts Forum convened by the Attorney General in 1999 for 25 leading state and local law enforcement, fire, medical/public health, and emergency management professionals. One of the six goals in the Five-Year Plan (Safeguard Public Safety by Improving State and Local Capabilities) focuses exclusively on state and local concerns.

However, state and local first responder organizations—those entities that represent state and local officials who would respond first to the scene of an incident—continue to criticize the plan. For example, according to the International Association of Fire Chiefs, the current national preparedness effort, though useful, has overlooked goal setting. The lack of clearly defined preparedness goals should be addressed through the development of performance capability objectives that, once met through the rational deployment of local, state, and federal assets, define the end-game, or goal: adequate preparedness. The Association also noted that until a national strategy is put in place, it would be exceedingly difficult to quantify the level of preparedness reached by the collective national response mechanism. Several other organizations have taken the same or similar positions.[9]

Although combating terrorism is primarily a federal responsibility, state and local emergency responders (police, fire, and emergency medical personnel) are almost certain to be the first to respond to the use of a weapon of mass destruction. We believe the Five-Year Plan should specifically address the role of state and local emergency responders, since their initial actions in handling a conventional explosive or incendiary device, or an unconventional weapon containing WMD matter will be critical to the success of the overall response and, thus, to public health and safety. To the extent the plan can better address the roles of

[9]These include, for example, the National Governors Association, the National Emergency Management Association, and the National League of Cities.

state and local authorities, and be developed with them, it can become more of a national strategy than a federal plan.

Other Agencies May Produce Competing Strategies

Efforts to develop a national strategy also may be hindered by other agencies developing competing national strategies. It also demonstrates that the President and the Congress sometimes have provided different messages on overall leadership and coordination. Notwithstanding the creation of the position of National Coordinator, the Congress directed the Attorney General to develop a national strategy.[10] In addition to the resultant Attorney General's Five-Year Interagency Counterterrorism and Technology Crime Plan, both the NSC and the National Domestic Preparedness Office (NDPO) (discussed in ch. 5) also have planned to develop national strategies. More recently, FEMA's new Office of National Preparedness (also discussed in ch. 5) will develop a national strategy. This potential proliferation of "national" strategies written by different entities clearly demonstrates the current fragmentation of overall leadership and coordination.

Progress Made in Tracking Spending to Combat Terrorism

The NSC and OMB both have roles in overseeing governmentwide programs to combat terrorism. The NSC has the responsibility to coordinate policies and operations and OMB has the responsibility to track funding for terrorism-related programs. At the time of our initial report, we found that the amount of funds being spent to combat terrorism was unknown and difficult to determine.[11] Despite their oversight roles, the NSC and OMB were not regularly collecting, aggregating, and reviewing funding and spending data relative to combating terrorism on a crosscutting, governmentwide basis. Further, funding priorities for terrorism-related programs were not established. As a result, there was no assurance that (1) agencies' requests were funded through a coordinated and focused approach, (2) the highest priority requirements were being met, (3) terrorism-related activities and capabilities were not unnecessarily duplicative, and (4) funding gaps or misallocation had not

[10]This plan was directed in the Conference Committee Report (House Report 105-405, Nov. 13, 1997) accompanying the Fiscal Year 1998 Appropriations Act for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies (P.L. 105-119, Nov. 26, 1997).

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

occurred. Based upon our findings, the Congress required OMB to establish a reporting system on the budgeting and expenditure of funds to combat terrorism.[12] Further, the Congress mandated an annual report containing agency budget and expenditure information that would identify any priorities and any duplication of efforts to combat terrorism.

Subsequent to this requirement being established, OMB has tracked budgets and expenditures for programs to combat terrorism and has issued four annual reports to the Congress. These OMB reports are a significant step toward improving the management and coordination of these programs and activities. The reports capture governmentwide information in a uniform fashion, highlight budget initiatives, and provide increasingly detailed information about individual agencies' spending. The last two reports have an annex with several years of budget data on programs to combat terrorism and critical infrastructure protection presented by agency, category, and categories within agencies.[13] The most recent report also has a detailed discussion of the different agencies' roles, missions, and activities. Through these reports, the executive branch and the Congress have strategic oversight of the magnitude and direction of federal funding for this priority national security and law enforcement concern.

In 1999, the NSC and OMB began a new process to identify priorities and duplication—as required by law. Interagency working groups reviewed the agencies' proposals and developed recommendations on whether they should be funded. The agencies integrated the working groups' funding recommendations into their fiscal year 2001 President's Budget submissions. According to OMB, the NSC and OMB then reviewed agencies' actions on the recommendations and made necessary course corrections during the final decision-making by the President, based on information from the working groups, other agency priorities, and available resources. The new process may represent progress because, before it was implemented, agencies would make budget recommendations related to terrorism through the annual OMB budget submission. At that time, decisions were made on an agency-by-agency basis rather than in a governmentwide context. OMB has stated that this interagency budget review resulted in reallocation of resources—within and between agencies—to fund critical shortfalls and to eliminate

[12]Section 1051 of the National Defense Authorization Act for Fiscal Year 1998 (P.L. 105-85).

[13]See OMB's *Annual Report to Congress on Combating Terrorism*, July 2001.

duplication. However, to date, OMB's annual reports have not identified priorities or reported on duplication of efforts.

Although OMB notes that the Attorney General's Five-Year Plan sets priorities, the plan does not link recommended actions to budget resources—a key step in developing a national strategy. While the original plan indicated that the annual updates would address this matter, they also have not linked actions with required resources. In the absence of a national strategy with measurable outcomes (as discussed earlier in this chapter), we are concerned that this new process 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.

Agencies Complete Interagency Operational Guidance, Enhancing Unified and Coordinated Response Capability

Federal agencies have completed interagency guidance to combat terrorism domestically and clarified many command and control issues. Completed interagency guidance should positively impact federal response operations leading to a more organized, unified, and coordinated national terrorism response capability. This is significant progress since 1999 when we reported that federal agencies had neither completed interagency guidance as directed by PDD 39 nor coordinated all proposed guidance with all federal agencies with domestic counterterrorism roles.[14] As a result, federal response operations potentially were not as well-coordinated and highly integrated as intended, sometimes resulting in conflict or confusion over roles and responsibilities as well as the transfer of tactical authority. Table 4 summarizes recently completed interagency plans and guidance.[15]

[14]*Combating Terrorism: Issues to Be Resolved to Improve Counterterrorism Operations* (GAO/NSIAD-99-135, May 13, 1999).

[15]A more complete listing of interagency plans and guidance for combating terrorism appears in app. I.

Table 4: Interagency Plans and Guidance for Combating Terrorism

Interagency plan or guidance	Description
Attorney General's Five-Year Interagency Counterterrorism and Technology Crime Plan	Drafted by the Department of Justice in conjunction with other agencies, this plan and its annual updates serve as a baseline strategy for the coordination of national policy and operational capabilities to combat domestic terrorism. The classified plan was issued in December 1998.
Federal Response Plan and Terrorism Incident Annex	Drafted by FEMA and coordinated with 26 other federal departments and agencies and the American Red Cross, the plan outlines the way the federal government responds to domestic incidents in which the President has declared an emergency requiring federal emergency disaster assistance. The plan was issued in April 1992 and revised in April 1999. The Terrorism Incident Annex, issued in February 1997, provides a concept of operations outlining how the federal government would assist state and local authorities in managing the consequences of a terrorist attack in the United States.
CONPLAN (United States Government Interagency Domestic Terrorism Concept of Operations Plan)	Drafted by the FBI and coordinated with FEMA, DOD, DOE, HHS, and EPA, the CONPLAN was issued in January 2001. It provides overall guidance to federal, state, and local agencies concerning how the federal government would respond to a potential or actual terrorist threat or incident in the United States, particularly one involving weapons of mass destruction. It is intended to integrate the plans and procedures of individual agencies and departments with responsibilities to respond to a WMD incident and to establish a conceptual framework for integrating federal crisis and consequence WMD response.
Domestic Guidelines (Guidelines for the Mobilization, Deployment, and Employment of U.S. Government Agencies in Response to a Domestic Terrorist Threat or Incidents in Accordance with Presidential Decision Directive 39)	Drafted by the FBI, the classified document provides guidance for deploying federal capabilities in response to a terrorist threat or incident. The Domestic Guidelines were issued in November 2000.
International Guidelines (Coordinating Subgroup Guidelines for the Mobilization, Deployment, and Employment of U.S. Government Elements in Response to an Overseas Terrorist Incident)	Drafted by the Department of State, the classified International Guidelines outline procedures for deploying the Foreign Emergency Support Team and for coordinating federal operations overseas. The International Guidelines were issued in January 2001.

Source: GAO analysis.

Federal agencies also are updating and revising interagency guidance to meet responders' needs and new developments. For example, FEMA is clarifying the Federal Response Plan to include an explanation of its relationship to other federal emergency plans, such as the Federal Emergency Response Plan, National Oil and Hazardous Substances Pollution Contingency Plan (National Contingency Plan), and Federal Radiological Emergency Response Plan. A change to the Federal Response Plan will be issued to expand and clarify individual agency roles and responsibilities as well as funding arrangements. Also, HHS is developing an annex to the Federal Response Plan for biological terrorism. (See app. I for a compendium of related federal policy and planning documents.)

Individual Agencies Complete or Develop Plans and Guidance

Agencies have completed or are developing internal guidance and concepts of operations to deal with terrorist incidents, including those involving a weapon of mass destruction. For example, DOD developed a detailed contingency plan to guide its actions in deploying and responding to a terrorist incident (including domestic incidents) and HHS developed a concept of operations plan to deal with the health and medical consequences of terrorist attacks and augment and support state and local governments. HHS is completing additional plans that coordinate efforts among state health departments and agencies and the federal government, and has developed medical and health responses for smallpox. The Centers for Disease Control and Prevention and the Office of Emergency Preparedness developed plans that support HHS' strategic objectives and goals for preventing bioterrorism, conducting epidemiological surveillance, providing medical and public health readiness for mass casualty events, ensuring a national pharmaceutical stockpile, and securing information technology infrastructures.

Another example of the progress made is FEMA's completion of the final draft of a terrorism supplement (Attachment G) to the State and Local Guide 101 for All-Hazard Emergency Operations Plan. FEMA issued the attachment in April 2001. The attachment will aid state and local emergency planners in developing and maintaining a Terrorist Incident Appendix to their Emergency Operations Plans for terrorist incidents involving weapons of mass destruction.

Appendix II describes individual agency plans and guidance for combating terrorism.

Conclusions

The federal government has made progress in recent years in developing a national strategy to combat terrorism, but several key components still are incomplete or are missing. Although the Department of Justice and the FBI agreed to implement our 1999 recommendations to conduct multidisciplinary and analytically sound threat and risk assessments, these still are not complete more than 2 years after the FBI agreed to do them. The Attorney General should ensure that national-level threat assessments regarding terrorist use of weapons of mass destruction are completed expeditiously.

While the Attorney General's Five-Year Plan is a substantial interagency effort and could serve as the basis for a national strategy, we believe it lacks two critical elements: measurable outcomes and identification of state and local government roles. By including measurable outcomes, the

Five-Year Plan would incorporate the principal tenets of the Government Performance and Results Act of 1993, which holds federal agencies accountable for achieving program results and requires them to clarify their missions, set program goals, and measure performance toward achieving these goals.

Recommendations for Executive Action

To help support a national strategy, we recommend that the Attorney General direct the Director of the FBI to work with appropriate agencies across government to complete ongoing national-level threat assessments regarding terrorist use of weapons of mass destruction. If a single focal point is established in the Executive Office of the President to lead and coordinate federal programs to combat terrorism, then this focal point should maintain oversight to ensure the assessments are coordinated fully with key federal agencies that combat terrorism (see Recommendations for Executive Action in ch. 2).

To guide federal efforts in combating domestic terrorism, we recommend that the Attorney General use the Five-Year Interagency Counterterrorism and Technology Crime Plan and similar plans of other agencies as a basis for developing a national strategy by including (1) desired outcomes that can be measured and that are consistent with the Results Act and (2) state and local government input to better define their roles in combating terrorism. If a single focal point is established in the Executive Office of the President to lead and coordinate federal programs to combat terrorism, then the focal point should take over this role from the Department of Justice to ensure that the national strategy is seen as an interagency document (see Recommendations for Executive Action in ch. 2).

Agency Comments and Our Evaluation

Agency comments on a draft of this report were based on their efforts prior to the September 11, 2001, terrorist attacks. The Department of Energy agreed with our recommendation to complete a national-level threat assessment. DOE said that the first step toward developing a national strategy is to conduct a thorough threat and risk assessment to define and prioritize requirements. The Department of Justice did not comment on our recommendation that the Attorney General direct the Director of the FBI to complete a national-level threat assessment regarding terrorist use of weapons of mass destruction. However, Department of Justice officials provided us with an update on their progress and we revised the report, as appropriate. While the Department of Justice and the FBI appear to be working to produce threat

assessments, we believe our recommendation still is valid until such assessments are complete.

The Department of Justice disagreed with our recommendation that the Attorney General's Five-Year Plan be revised to include measurable outcomes. According to the Department, each agency must have the flexibility to link the goals and objectives of the Five-Year Plan to its own strategic goals and measures. We disagree with the Department of Justice and still believe that the Five-Year Plan focuses more on agency outputs than outcomes that are results oriented. We believe that having overall results-oriented outcomes would not limit the flexibility of individual agency strategic goals and measures. We believe it would improve the strategic planning process across agencies.

Chapter 4: Federal Response Capabilities Are Improving

Federal capabilities to respond to terrorist incidents are improving. Federal agencies have a broad array of capabilities to respond to terrorist incidents. The FBI and FEMA could lead a variety of potential federal teams and related assets for crisis and consequence management. These federal capabilities are enhanced through agency participation in special events, such as political conventions, sporting events, and international meetings. Since our last review, the FBI and the U.S. Secret Service have improved their cooperation for such events. Federal agencies also exercise their capabilities to respond to a terrorist incident through exercises. The FBI has made progress in exercising its interagency and intergovernmental leadership role in crisis management. FEMA is not using exercises to practice fully its leadership role over consequence management. Evaluations from such exercises, as well as from actual operations, allow agencies to learn lessons from their successes and mistakes. Based upon our earlier work, we found that some individual federal agencies have improved their processes to capture and share lessons learned. However, as yet, there is no regular process in place to capture and share lessons learned at the interagency level. Federal capabilities also are enhanced through research and development projects. While federal research and development programs are coordinated in a variety of ways, coordination is limited, raising the potential for duplication of efforts among different federal agencies.

The Federal Government Has a Broad Array of Response Capabilities

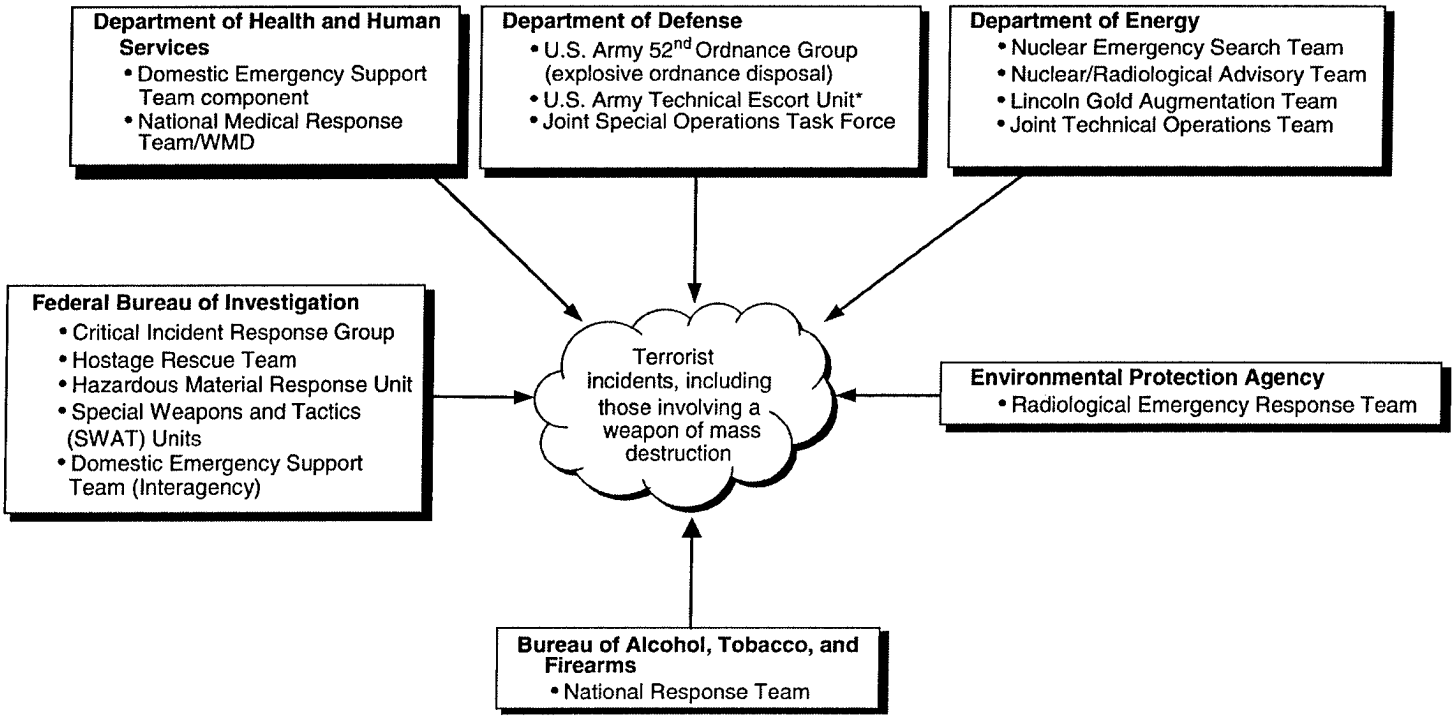
The FBI leads a variety of potential federal teams for crisis management. In exceptionally grave situations, DOD could play an important role in crisis management. FEMA also leads a variety of potential federal teams for consequence management. We found that these consequence management teams generally do not duplicate each other due to their unique capabilities and other mission requirements. Other federal assets, such as mobile laboratories to perform an initial on-site analysis of a weapon of mass destruction, would potentially support crisis and consequence management.

FBI Leads Federal Crisis Management Response Teams

The Department of Justice, acting through the FBI, is the overall lead federal agency for domestic terrorist incidents and the FBI is the lead agency for crisis response to domestic incidents. Crisis response assets within the FBI include the Critical Incident Response Group, which integrates the tactical and investigative expertise necessary to deal with terrorist incidents. The group includes crisis managers, hostage negotiators, behaviorists, and surveillance assets. The group also contains the Hostage Rescue Team, which can operate in a chemical and biological

environment, and is trained in hostage rescue, precision shooting, advanced medical support, and tactical site survey. Furthermore, all but one of the FBI's 56 field offices include a Special Weapons and Tactics (SWAT) team trained to plan and execute high-risk tactical operations. Numerous other federal agencies may be called upon for support as needed. The FBI uses the United States Interagency Domestic Terrorism Concept of Operations Plan (CONPLAN) (discussed in ch. 3) to manage its operations with interagency and intergovernmental partners. Figure 3 illustrates key federal crisis management teams.

Figure 3: Key Federal Crisis Management Response Teams



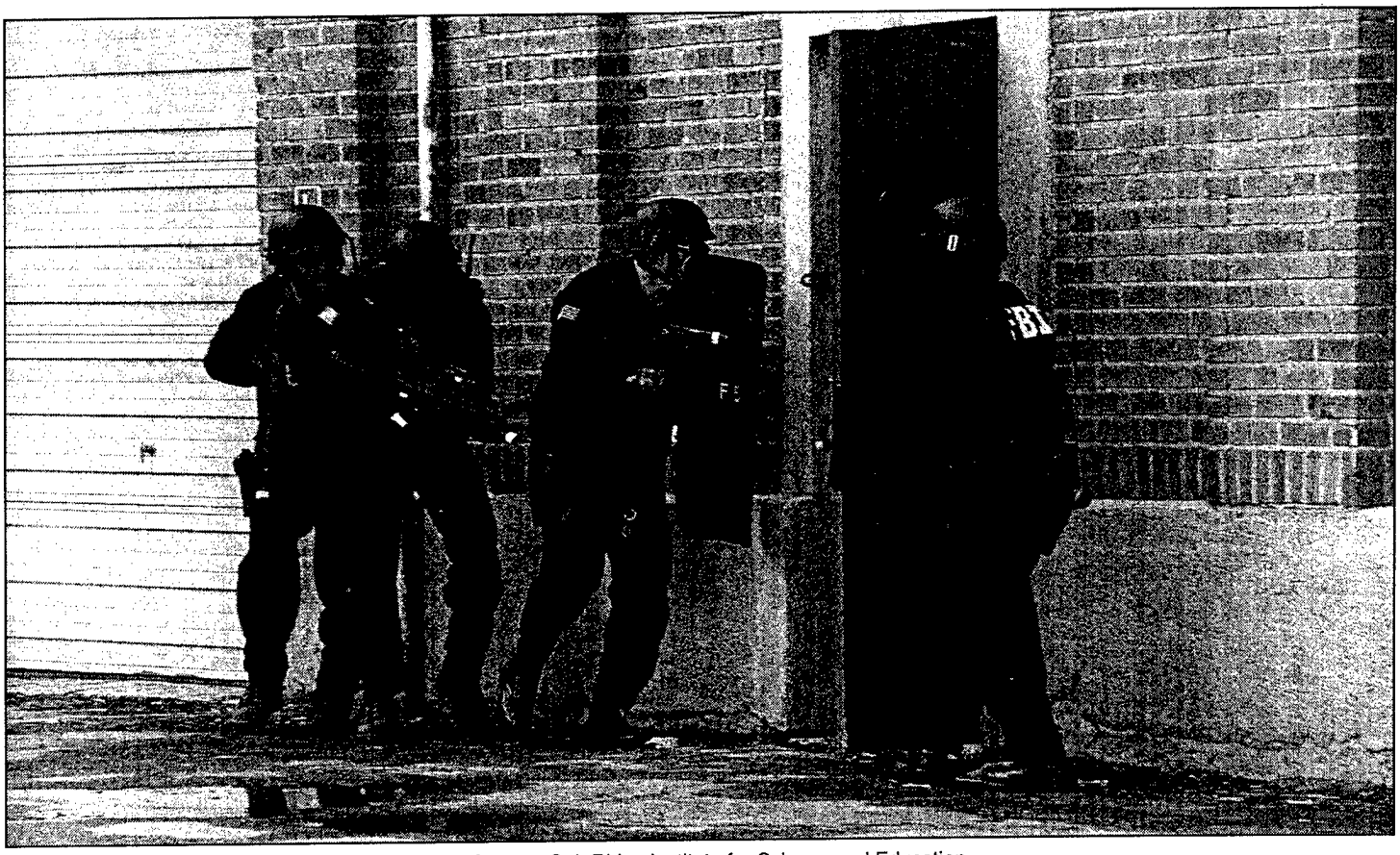
Note: The U.S. Army Technical Escort Unit has a dual role and may serve as a consequence management response team as well. It is marked with an asterisk.

Source: GAO analysis.

Appendix III provides more detailed information on the mission and personnel strength for the crisis management response teams shown in figure 3 above.

Figure 4 shows an FBI enhanced SWAT team executing a law enforcement search of a building during the Wasatch Rings counterterrorism exercise in preparation for the 2002 Olympic Winter Games in Salt Lake City, Utah.

Figure 4: FBI Enhanced SWAT Team Executes Search During Wasatch Rings Exercise



Source: Oak Ridge Institute for Science and Education.

In Extreme Situations, Military Could Have Crisis Management Role

If an exceptionally serious terrorist threat or incident is beyond the FBI's capabilities to resolve, a military joint special operations task force may be established to respond in accordance with contingency plans developed by DOD. As a general principle, the Posse Comitatus Act and DOD regulations prohibit the Armed Forces of the United States from being used to enforce domestic law.[1] However, the Posse Comitatus Act is

[1]See 18 U.S.C. section 1385.

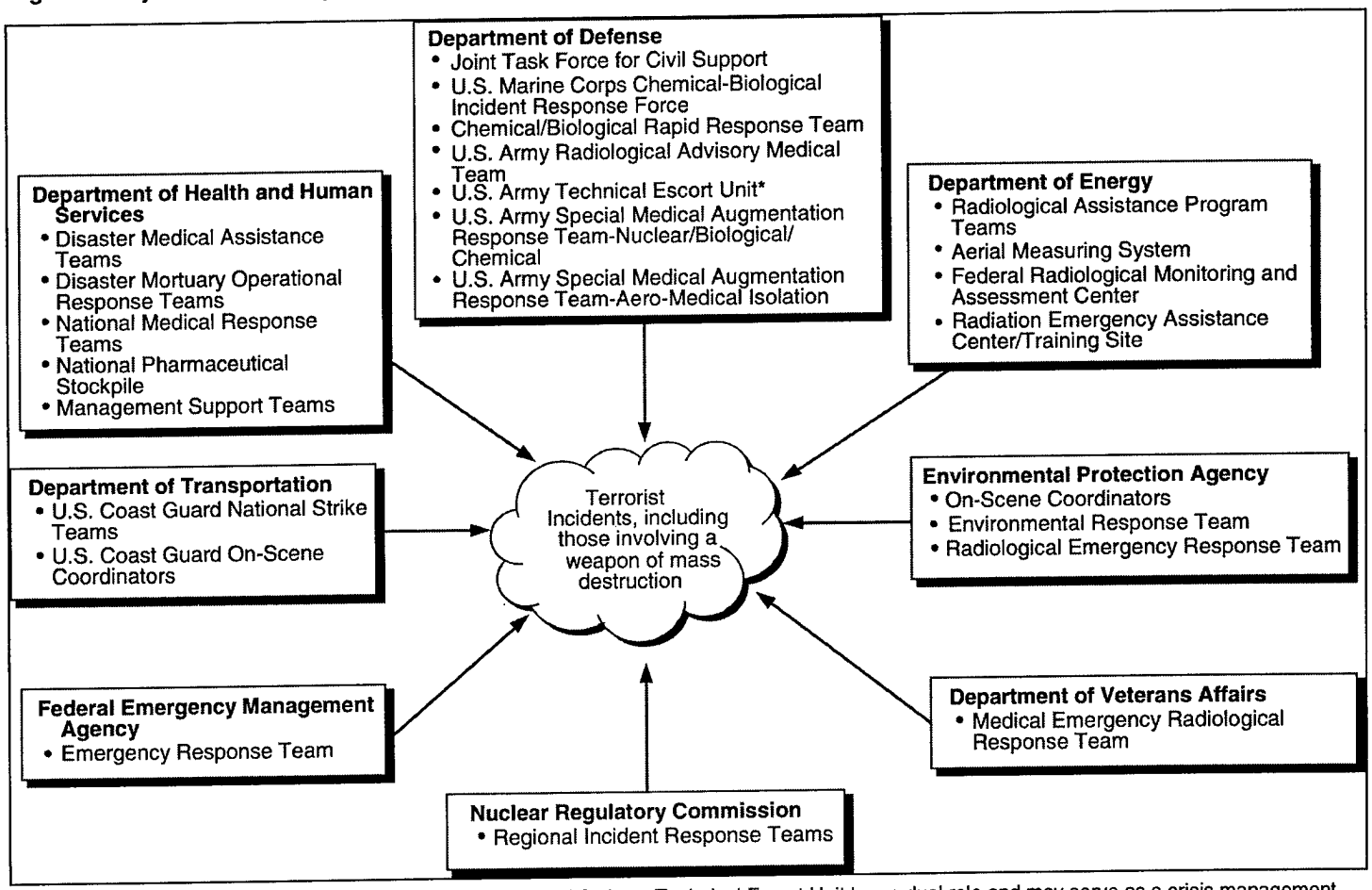
subject to exceptions that permit the use of the Armed Forces in dealing with domestic terrorist incidents in special situations. According to Department of Justice officials, these statutory exceptions would require a request from the Attorney General and concurrence by the Secretary of Defense. Department of Justice officials added that, in most cases, as a matter of policy, approval by the President will also be sought whenever possible. Further, Department of Justice officials state that if military forces are required to restore order as a result of an act of domestic terrorism that renders ordinary means of enforcement unworkable or hinders the ability of civilian law enforcement authorities, the President must issue an executive order and a proclamation. These documents are maintained in draft form and are ready for the President's signature, if needed.

If military force is required and approved, the on-scene FBI commander passes operational control of the incident site to the military commander. The military commander develops and submits courses of action to the National Command Authority. If the incident cannot be resolved peacefully, then the National Command Authority may order a military operation, including disabling a weapon of mass destruction. Once this is accomplished, the military commander returns operational control of the site to the FBI. To date, military action has never been required to resolve a domestic terrorist incident. Further, FBI officials stated that the FBI's own tactical skills to resolve a terrorist incident generally are equal to the military's, although technical assistance would be required in certain WMD incidents.

FEMA Leads Federal Consequence Management Response Teams

Although state and local governments have primary responsibility for managing the consequences of a domestic terrorist incident, their response capabilities may quickly become overwhelmed. Should state and local authorities request assistance, FEMA would coordinate federal agencies' responses and activities. The federal government can provide considerable assets to assist state and local authorities. For example, 8 federal agencies have 24 types of teams that could respond to terrorist use of weapons of mass destruction. FEMA uses the Federal Response Plan (discussed in ch. 3) to task and manage other federal agencies. Figure 5 illustrates key federal consequence management teams.

Figure 5: Key Federal Consequence Management Response Teams



Note: The U.S. Army Technical Escort Unit has a dual role and may serve as a crisis management response team as well. It is marked with an asterisk.

Source: GAO analysis.

In commenting on a draft of this report, the Department of State noted consequence management assets are finite and the same assets that would be used to respond to a domestic terrorist incident also would be used to respond to an overseas terrorist incident.

Appendix IV provides more detailed information on the mission and personnel strength for the consequence management response teams shown in figure 5.

Consequence Management Teams Generally Are Not Duplicative

While there are numerous federal teams, we found that the response teams do not duplicate one another for a number of reasons. In general, each team has a unique combination of capabilities and functions when deployed to or near the site of a terrorist incident. No single team or agency has all the capabilities and functions that might be required to respond to a terrorist incident. Some federal response teams have capabilities and functions that are clearly unique, such as the ability of HHS' Disaster Mortuary Operational Response Teams to process, prepare, and dispose of contaminated fatalities. Several federal teams would be more likely to respond to certain types of incidents because they have expertise concerning the type of agent used in the attack. For example, DOE teams specialize in responding to incidents involving radiological agents or weapons. Other teams have similar capabilities and functions, but there are also distinctions among these teams that differentiate them. One distinction is that they perform a wide variety of functions. In general, these functions fall into one of three categories: performing hands-on response functions; providing technical advice to federal, state, and local authorities; or coordinating the response efforts and activities of other federal teams. Because of the differences in the capabilities and expertise of teams, the type of incident would determine which individual teams would be most appropriate to deploy.[2]

Even in the absence of a terrorist threat, federal agencies still would need most of their response teams to carry out other missions. Most federal teams are long-standing and have purposes other than combating terrorism, such as responding to natural disasters, hazardous material spills, and military crises. For example, DOD teams can provide a wide variety of consequence management capabilities in response to domestic

[2]For a detailed review of federal consequence management response capabilities, see our report *Combating Terrorism: Federal Response Teams Provide Varied Capabilities; Opportunities Remain to Improve Coordination* (GAO-01-14, Nov. 30, 2000).

terrorist incident. However, these teams have a primary military role and mission.

Agency Laboratories Augment Federal Response Teams

A few agencies have fixed assets, such as laboratories, which may augment teams and the overall federal response in a chemical or biological terrorist incident. In some incidents, these laboratories may perform functions that enable deployed federal response teams to perform their role. For example, when a diagnosis is confirmed by one of the laboratories at the Centers for Disease Control and Prevention, the U.S. Army Medical Research Institute of Infectious Diseases, or those within the Laboratory Response Network, the National Medical Response Teams and the Disaster Medical Assistance Teams can begin to treat victims appropriately. According to HHS, this Laboratory Response Network has responded to hundreds of state and local events since its inception. It represents an operational partnership for early detection and laboratory confirmation between the Centers for Disease Control and Prevention, the FBI, DOD, and state and local health departments. The network has a common training doctrine and develops standardized assays that it distributes to its partners. It is a critical new component of national preparedness for bioterrorism.

Coordination of Special Events Has Improved

Federal capabilities are demonstrated and enhanced through agency participation in special events. These events provide federal agencies with valuable experience working together to develop and practice plans to combat terrorism. PDD 62 established a process to designate certain events as National Special Security Events. The FBI and the U.S. Secret Service have improved their cooperation for such events. For example, they now have a written agreement on command and control and conduct planning and exercises together.

Special Events Provide Coordination Experience

Special events are high-visibility events in which federal agencies initiate contingency measures against terrorist attacks and most agencies involved gain valuable experience coordinating their activities. PDD 62 created a category of special events called National Special Security Events, which are events of such significance that they warrant greater federal planning and protection than other special events. Upcoming events must be nominated by the NSC, then certified by the Attorney General and Secretary of the Treasury before they officially are designated as National Special Security Events. Such events have included the major political party conventions, Presidential inaugurations, Olympic games, and the

World Trade Organization Ministerial Meeting. For these events, PDD 62 reaffirmed the FBI's lead federal agency role for crisis management, but designated the U.S. Secret Service as lead federal agency for security design, planning, and implementation at such events. The directive also encouraged cooperation among federal agencies in counterterrorism planning for these events.

FBI and U.S. Secret Service Have Improved Coordination

In a previous report, we noted that the U.S. Secret Service and the FBI did not always coordinate their command and control structures or contingency plans, and agency officials acknowledged that their agencies had not worked well together.[3] Since then, special event cooperation and coordination between the U.S. Secret Service and the FBI has improved. Specifically,

- The FBI and the U.S. Secret Service have a written agreement on command and control arrangements for special events, and officials from both agencies agreed that this document is followed when preparing for special events.
- The FBI's Special Events Management Planning Handbook enumerates the roles and responsibilities of other federal agencies (including the U.S. Secret Service) for special events and stresses the need for cooperative planning for terrorist incidents.
- U.S. Secret Service evaluations on special events discuss interaction with the FBI and FEMA and identify the need for additional cooperative planning.
- We observed close cooperation and detailed planning between the U.S. Secret Service, the FBI, and other federal agencies during an exercise in preparation for the 2002 Olympic Winter Games in Salt Lake City, Utah.

Federal Counterterrorism Exercises Are Improving

To improve their preparedness to respond to a terrorist incident, federal agencies exercise their capabilities. The FBI has made progress in practicing its interagency and intergovernmental leadership role in crisis management through a number of exercises. FEMA has made some progress, but is not using exercises to fully practice its leadership role over consequence management. Two recent exercises, "Top Officials

[3] *Combating Terrorism: Issues to Be Resolved to Improve Counterterrorism Operations* (GAO/NSIAD-99-135, May 13, 1999).

(TOPOFF) 2000" and "Wasatch Rings," provide good examples of federally sponsored interagency and intergovernmental exercises.

Exercises Important to Response Readiness

PDD 39 required key federal agencies to exercise their capabilities to combat terrorism. Exercises test and evaluate policies and procedures, test the effectiveness of response capabilities, and increase the confidence and skill level of personnel. Exercises also identify strengths and weaknesses before they arise in an actual incident. Exercises further allow agencies to apply operational lessons learned from past exercises and actual deployments.

In counterterrorism, where federal operations are inherently interagency matters, exercises also allow various department and agency personnel to become familiar with each other's missions and procedures and learn to coordinate and operate together. Interagency exercises can help identify aspects of cooperation that work well and problems and conflicts that require interagency resolution. Interagency exercises are planned through an interagency Exercise Subgroup cochaired by the Department of State (for international exercises) and the FBI (for domestic exercises). The Department of State and the FBI alternate as host for bi-monthly exercise planning meetings. These meetings address both domestic and international exercise plans. The major agencies most likely to react to terrorist incidents participate regularly, and other agencies participate less frequently. The meetings allow various agencies to address issues, plan future exercises, and compare and resolve agency exercise schedule conflicts. They also serve as a forum for interagency discussion and planning for national-level counterterrorism exercises.

The FBI Regularly Practices Its Crisis Management Leadership Role Through Exercises

We previously reported that domestic crisis exercises led by federal law enforcement agencies did not include many of the federal, state, and local authorities that would be needed to effectively respond to a terrorist crisis. We noted that the FBI's domestic crisis response program was well developed with regularly scheduled field exercises that tested regional and field office capabilities at the tactical level, but generally did not exercise the broader interagency leadership role that the FBI would play in a major terrorist incident. In addition, we reported that crisis management exercises were ending in a successful tactical resolution of the incidents and did not include more likely scenarios where terrorist attacks were successful, requiring consequence management.

Since our earlier review, the FBI has taken steps to strengthen its leadership role through a number of interagency and intergovernmental exercises. In planning national-level field exercises, the FBI has given priority for state and local agencies' participation. In addition to its own regional field exercises, the FBI participated in or sponsored a major interagency and intergovernmental field exercises at least once per year. These have been field exercises that included both crisis and consequence management and tested interagency command and control and communications issues by establishing a Joint Operations Center. These exercises included the following:

- In June 1998, the FBI participated in the "Gauged Strength" exercise in Norfolk, Va. Although this exercise was sponsored by DOD, the FBI had robust participation and established interagency organizations, such as a Joint Operations Center and a Joint Information and Intelligence Support Element. State and local participation was limited by DOD classification requirements.
- In February 1999, the FBI sponsored the "Westwind" exercise in Los Angeles, Calif. This exercise, cosponsored by the state, tested the compatibility of federal, state, and local terrorism response plans through the integration of the Joint Operation Center and Incident Command Post. The exercise also tested the activation of the Terrorism Early Warning Group and the mobilization and deployment of the Domestic Emergency Support Team.
- In May 2000, the FBI participated in the TOPOFF 2000 exercise in three locations across the country. This Department of Justice-sponsored exercise included a radiological scenario in Washington, D.C.; a chemical scenario in Portsmouth, NH, and a biological scenario in Denver, Colo. The FBI established interagency Joint Operations Centers in all three cities. FBI officials told us that this was the largest, most complex federal counterterrorist exercise ever conducted.
- In April 2001, the FBI sponsored the Wasatch Rings exercise in Salt Lake City, Utah. This exercise, cosponsored by the state, tested federal, state, and local contingency plans related to the upcoming 2002 Olympic Winter Games. The FBI established a Joint Operations Center, which was co-located with a state and local command center. Again, the interagency Domestic Emergency Support Team was deployed.

For additional information and our observations on these last two exercises, see the information in the text boxes that follow.

FEMA Not Fully Practicing Its Leadership Role Through Exercises

FEMA was designated as the lead federal agency for consequence management under PDD 39 and was also tasked under a fiscal year 1995 emergency supplemental appropriation to develop exercises that focused on consequences of a terrorist incident.[4] We previously reported that FEMA held a number of tabletop exercises in response to these directives, but only planned or sponsored one interagency field exercise to test its consequence management leadership role. Tabletop exercises identify important policy and operational issues, but are not a substitute for field exercises that test the federal government's ability to use and coordinate teams and assets in a realistic setting.

Although federal agencies are beginning to work together to improve consequence management exercises, agency officials said the consequence management component needs to be carried out further to effectively test agency capabilities. For example, the consequences of a biological incident that can include mass casualties or an overwhelmed health care system have not been fully included as part of the consequence management exercises. These scenarios present unique challenges, such as identifying alternative facilities for mass casualties, identifying military reserve units that need to be brought in, determining how mass casualties would be moved, and establishing quarantine areas.

In our review of exercises over the last 3 years, we found that FEMA participated in some field exercises and held numerous tabletop exercises. However, FEMA generally did not sponsor any interagency field exercise. Without field exercises involving a consequence management component, federal agencies are not able to train and exercise their response capabilities, deploy personnel and equipment, and practice roles and responsibilities in realistic settings. One FBI official said that more of the major interagency field exercises could include a robust consequence management component if FEMA was more involved in the initial planning phases of the exercises within the interagency exercise group. FEMA, however, is taking on leadership roles during field exercises in which it participates. For instance, during the Wasatch Rings exercise briefing, we observed FEMA outlining various consequences to possible WMD scenarios and coordinating with federal agency officials on the appropriate response.

[4]Emergency Supplemental Appropriations for Additional Disaster Assistance, for Counterterrorism Initiatives, for Assistance in the Recovery From the Tragedy That Occurred at Oklahoma City, and Recission Act (P.L. 104-19, July 27, 1995).

FEMA's participation in the Interagency Working Group on Exercises has been sporadic. For example, during our observation of the January 2001 meeting of the Interagency Working Group on Exercises, FEMA did not actively participate. In March 2001, we were told that FEMA formally was attending meetings within the Exercise Subgroup. Active participation within the Exercise Subgroup allows federal agencies to establish objectives and prepare a schedule of large interagency counter-terrorist exercises. This also allows agencies the opportunity to discuss complex transfers of command and control between agencies. Without interagency exercise objectives set by the Exercise Subgroup, agencies are not likely to exercise key scenarios and, as a result, the federal government will be less prepared to respond in a tailored, synchronized manner if an incident occurs.

The following textbox provides our observations on TOPOFF 2000, a congressionally directed, Department of Justice and FEMA cosponsored field exercise to assess the nation's crisis and consequence management capacity.

GAO OBSERVATIONS ON THE TOPOFF 2000 EXERCISE

In May 2000, the Department of Justice and FEMA co-sponsored a congressionally directed no-notice field exercise, Top Officials (TOPOFF) 2000, to assess the nation's crisis and consequence management capacity. TOPOFF 2000 exercised federal, state, and local plans, policies, procedures, and systems in response to simulated terrorist incidents. TOPOFF 2000 represented progress over previous combating terrorism exercises. The scenarios included concurrent response to a radiological incident in the Washington, D.C., area; a chemical incident in Portsmouth, New Hampshire, a city that had received no domestic preparedness training; and a biological incident in Denver, Colorado, which had received such training.

TOPOFF 2000 was the first large-scale interagency and intergovernmental field exercise dealing with a biological terrorist incident. The state of Colorado, Denver County, and Arapahoe County cosponsored the TOPOFF 2000 to exercise their emergency management, health and medical agencies, fire, police, hazardous materials, public service, and non-governmental organizations. State officials said that the exercise offered the community a unique opportunity to broaden their understanding of bio-terrorism and adapt existing planning. Officials termed TOPOFF 2000 as a catalyst for future planning, coordination and communication for similar types of field exercises. The community received valuable training prior to TOPOFF 2000, although it served primarily to identify emerging bio-terrorism-unique issues. Officials said that more training was needed by state and local agencies to develop practical planning and training in preparation for the multi-agency exercise.

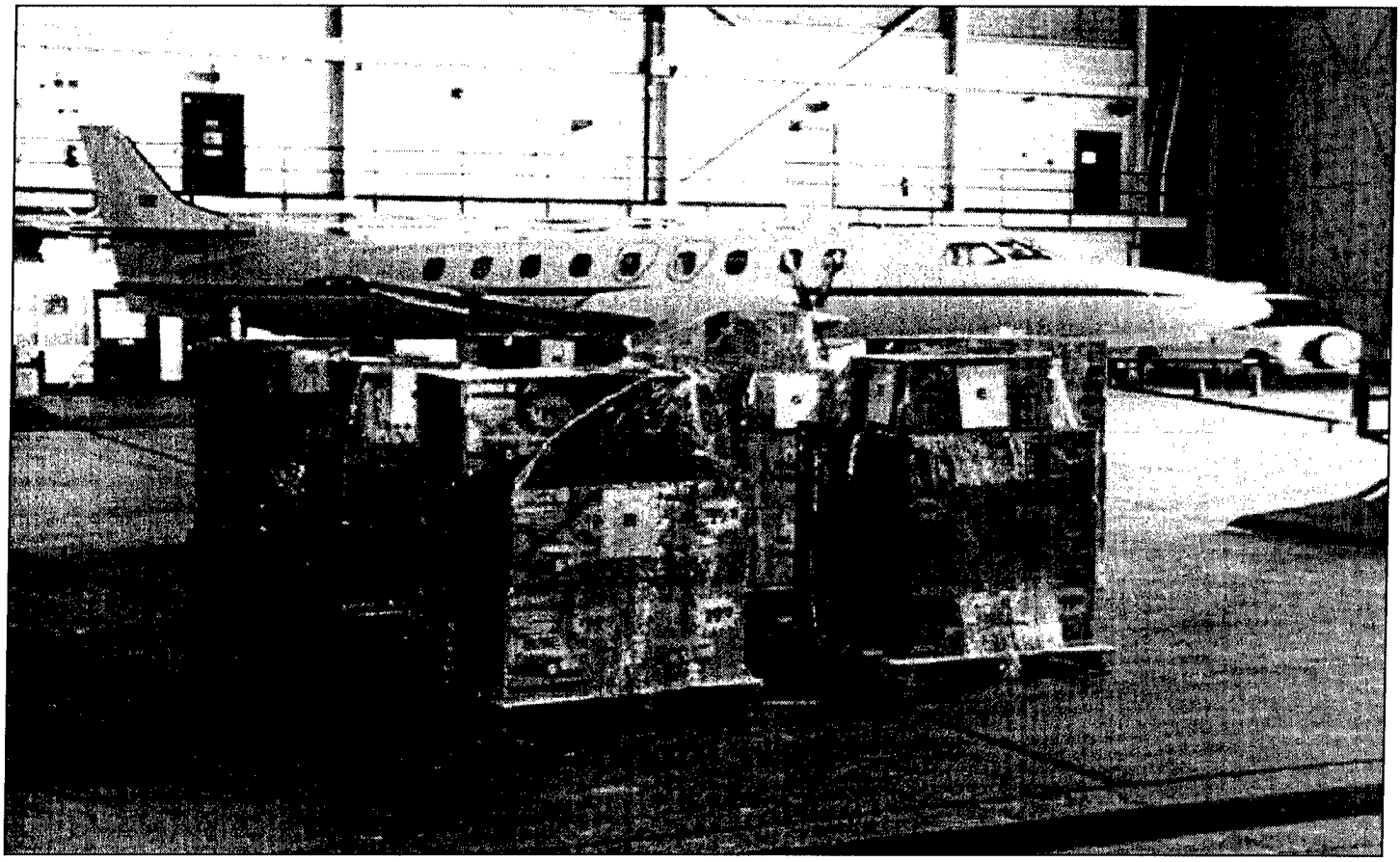
According to Colorado's evaluation of the exercise, the state was confronted with a number of challenges such as (1) management of the national pharmaceutical stockpile, (2) pubic information, (3) quarantine to restrict public movement, (4) mass casualty management and body disposal, and (5) resource management and coordination during response. The evaluation said the logistics of the exercise did not realistically support the national pharmaceutical stockpile, which highlighted problems in the coordination, breakdown, transport, security and distribution of the stockpile. Public information was also recognized as a critical function requiring a bio-terrorism-specific media campaign, but was under developed and not adequately played out as planned by the state. Efforts to control the contagious agent through quarantine surfaced major challenges for law enforcement agencies in handling the enforcement and rules of engagement. Another factor highlighted was that the curtailment of routine activities would have undermined the continuity of business, government, and society. There were also many unique challenges related to coordination, communication, and resource management for medical responses. Rapid depletion of these resources presented challenges to the emergency management and medical communities.

Overall, state and local officials felt that the exercise was extremely valuable, but complex because it was designed to prove that existing resources would be rapidly overwhelmed by a large-scale biological attack. They also questioned the value of having a no-notice exercise on this scale. These officials stressed that the federal structure, which was imposed on top of the local structure, did not have an all-hazards approach to responding to a terrorist incident. They said it was difficult to combine the deliberate medical culture with a crisis response culture requiring rapid decision making. Further, they noted that the federal government, including the Centers for Disease Control and Prevention, has little experience actually handling a disease outbreak of this magnitude.

Figure 6 shows simulated National Pharmaceutical Stockpile push-packages after they had been delivered and unloaded at Buckley Air National Guard Base in Denver, Colorado, for the first time in TOPOFF

2000 to treat victims exposed to plague. The items in the simulated stockpile were subsequently distributed to hospitals and other points of distribution, such as makeshift medical treatment centers, so that victims could be appropriately treated. The delivery of the stockpile during an exercise provided an opportunity for federal, state, and local governments to coordinate their respective responses.

Figure 6: Arrival of a Simulated National Pharmaceutical Stockpile Push-Package During TOPOFF 2000 Exercise

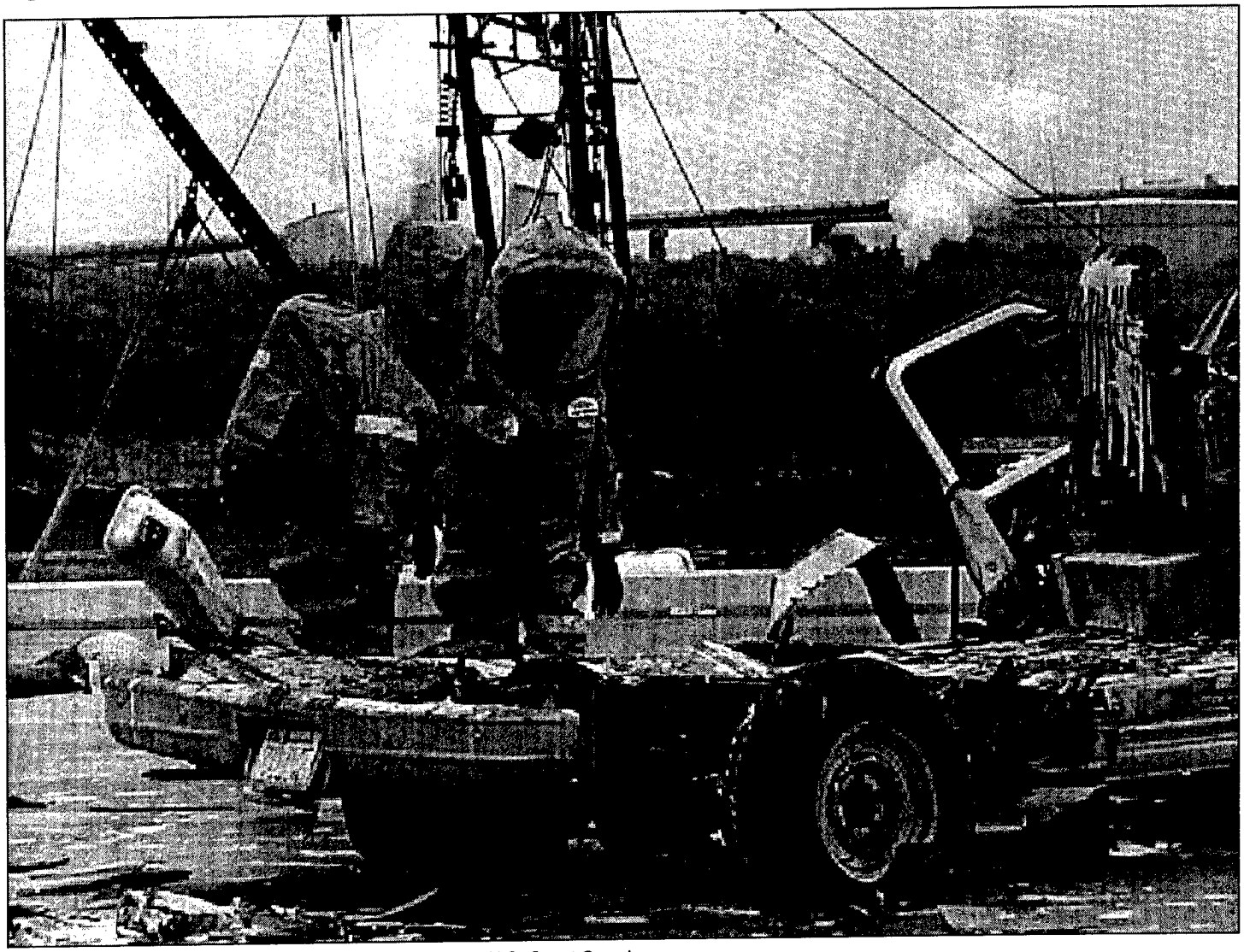


Note: The aircraft shown was used by technical assistance personnel; it is far too small to deliver an actual push-package from the National Pharmaceutical Stockpile. Also, the Stockpile uses specialized cargo containers for air transportation of its pharmaceuticals, supplies, and equipment.

Source: GAO.

Figure 7 shows members of the U.S. Coast Guard Atlantic Strike Team hazardous materials unit inspecting remains of a vehicle for chemical residue during the TOPOFF 2000 exercise in Portsmouth, New Hampshire.

Figure 7: U.S. Coast Guard Personnel Inspect Vehicle Remains for Chemical Residue During TOPOFF 2000 Exercise



Source: U.S. Coast Guard.

The following textbox provides our observations on Wasatch Rings, an FBI and Utah Olympic Public Safety Command cosponsored multi-agency WMD field training exercise in preparation for the 2002 Olympic Winter Games in Salt Lake City, Utah.

GAO OBSERVATIONS ON THE WASATCH RINGS EXERCISE

In April 2001, the FBI and the Utah Olympic Public Safety Command co-sponsored Wasatch Rings, a 2-day, multi-agency weapons of mass destruction field training exercise in preparation for the 2002 Olympic Winter Games in Salt Lake City. The major exercise was designed to test crisis and consequence management among federal, state, and local agencies that will provide safety and security for the Games. This no-fault exercise also provided agencies the opportunity to test joint command and control and communications in responding to terrorist incidents.

Several interrelated scenarios, initiated by a fictitious radical domestic terrorist group, were staged at various Winter Olympic venues. These scenarios included a plot to detonate an improvised explosive device during the Games, an overland manhunt, a kidnapping incident, a hostage barricade situation, a detonation of a radiation-laced bomb, a train derailment involving hazardous materials, and the interdiction of radiological material at the airport.

Rather than asking, "who's in charge?" we found that perhaps the more appropriate questions are "who's in charge of what?" and "when are they in charge?" Based on our observations, federal, state, and local agency officials knew who was in charge of a particular incident and each site. For example, the FBI was clearly in charge of crisis management involving kidnapping and hostage rescue scenarios. Bureau of Alcohol, Tobacco, and Firearms agents were in charge of a situation involving a bomb disposal. A local fire department was in charge of a train derailment site involving hazardous chemicals. We also observed that coordination between the FBI and FEMA at the tactical level was smooth. However, the exercise never fully transitioned from crisis management to full-scale consequence management. A major lapse was the delayed notification of local hospitals that a blast had occurred and that it was a radiological incident. By the time the hospitals were notified, they had become contaminated by self-referred patients, had to be closed, and could not treat other "victims." The exercise resulted in valuable lessons learned so that federal, state, and local agencies are better prepared to handle the Olympic Games safety and security and so that future interagency operations can be improved.

Figure 8 shows an FBI enhanced SWAT team seizing an aircraft suspected of carrying radiological material during the Wasatch Rings counterterrorism exercise in preparation for the 2002 Olympic Winter Games in Salt Lake City, Utah.

Figure 8: FBI Enhanced SWAT Team Seizes Aircraft Suspected of Carrying Radiological Material During Wasatch Rings Exercise

Source: Oak Ridge Institute for Science and Education.

Evaluations of Exercises Need Improvement

Federal capabilities also are enhanced when agencies learn lessons from their successes and mistakes from exercises and operations. As in our earlier work, we found that some federal agencies have relatively good processes in place to capture and share lessons learned internally within departments and externally with participating agencies, while others have less rigorous processes. Some federal agencies continue to work on implementing an interagency process to capture and share lessons learned; however, as yet, there is no regular process being used to capture and share lessons learned.

After-Action Reports Are Important Learning Tools

A valuable part of the lessons learned process is preparation of an after-action report (AAR) or other evaluation that documents the results of an exercise, special event, or operation. Characteristics of an AAR typically include a summary of objectives, operational limitations, major participants, a description of strengths and weaknesses, and corrective actions. Effective follow-up and validation of the strengths and weaknesses also are important steps in the process, as they are the means to ensure that problems are corrected. Dissemination of AARs within an organization, and when appropriate to other participating agencies, is another important feature that provides aspects of the operations that worked well and those that need improvement. For counterterrorism operations that are inherently interagency matters, the lessons learned should also address the interaction between different agencies to highlight problems for resolution in interagency forums.

Some Individual Agencies Have Improved After-Action Reports, Although Deficiencies Remain

In our prior review of agencies' processes to capture lessons learned, we found that while some agencies had relatively good processes in place to capture and share lessons learned, other agencies had less rigorous processes. For example, the other agencies did not have a written policy that required that they produce AARs or a formal process to capture lessons learned. The production of AARs by some of these agencies was sporadic, in particularly for operations, special events, and exercises led by other agencies. In addition, few of these other agencies included discussions of interagency issues in their AARs. The dissemination of AARs was limited at many agencies, which minimized the benefits of lessons learned. These limitations make it more difficult for the agencies to capture the strengths and weaknesses shown in operations or exercises so they can continue or expand good practices or take corrective actions when necessary to improve future performance.

In our most recent review from July 1998 to August 2001 of agencies' processes to capture lessons learned, we found that some agencies' processes had improved. HHS and the U.S. Secret Service have adopted a formal policy to produce AARs to capture lessons learned, while three other agencies, VA, EPA, and the FBI, are in the process of drafting a policy. In addition, those agencies that adopted a formal process generally produced AARs for special events and select exercises. HHS began producing AARs for special events while the U.S. Secret Service started producing AARs on special events and tabletop exercises. In other agencies, our review found little, if any, improvement. Performance by the Bureau of Alcohol, Tobacco, and Firearms (ATF) and FEMA, however, fared worse compared to our prior review because they did not capture

lessons learned for any exercises, special events, or operations. Overall, agency officials generally cited a lack of dedicated staff or the tempo of ongoing operations or exercises as reasons why they did not write AARs or capture lessons learned. Table 5 describes selected agencies' processes for capturing lessons learned and producing AARs.

Table 5: Characteristics of Federal Agencies' Processes to Capture Lessons Learned From Counterterrorist Operations, Special Events, and Exercises

Agency	Formal policy and/or process to capture lessons learned	Actual agency production of AARs	AAR discussion of interagency issues and dissemination	Changes from prior GAO review of AARs
DOE	Policy requires AARs; formal process is After Action Tracking System	Generally produces AARs for exercises, including those led by other agencies; AARs were not produced for special events	AARs generally discuss interagency issues; AARs disseminated internally and sometimes externally	No change in formal policy; AARs not produced for special events
FEMA	Policy requires AARs; formal process is the Corrective Action Program	Produces no AARs for exercises and special events	Not applicable; AARs not done	Performance degraded because FEMA previously produced AARs for its exercises
U.S. Coast Guard	Policy requires AARs; formal process is Coast Guard Standard After Action Information and Lessons Learned System (CGSails)	Produces AARs for some field exercises and some tabletop exercises	AARs generally discuss interagency issues; AARs disseminated widely via web-based system/reporting process	GAO previously did not conduct a detailed review of U.S. Coast Guard processes to capture lessons learned
DOD	Policy requires AARs; new formal process is the Joint Lessons Learned Program	Some units produce AARs; DOD does not have visibility over them to determine the extent to which the requirement is met	When produced, AARs generally discuss interagency issues and are disseminated internally and sometimes externally	Adopted new formal policy to capture lessons learned; new office reviews and analyzes terrorism-related operations and exercise lessons learned
FBI	Formal policy is being drafted	Produces no AARs for operations or special events; generally, produces AARs for FBI field exercises, but not tabletop exercises	AARs generally discuss interagency issues; AARs disseminated internally to participating FBI offices, but not externally	No change in production of AARs; FBI is in the process of drafting a formal policy
U.S. Secret Service	Policy requires AARs to capture lessons learned	Generally produces AARs for special events and some tabletop exercises; rarely produces AARs for field exercises	AARs generally discuss interagency issues; AARs are disseminated internally, but not externally	Adopted formal policy to capture lessons learned; produced AARs for special events and some tabletop exercises

Agency	Formal policy and/or process to capture lessons learned	Actual agency production of AARs	AAR discussion of interagency issues and dissemination	Changes from prior GAO review of AARs
HHS	Policy requires AARs to capture lessons learned	Produces AARs for special events; rarely produces AARs for exercises	AARs generally discuss interagency issues; AARs disseminated internally, but not externally	Generally produces AARs for special events; adopted formal policy to capture lessons learned
EPA	Formal policy is being drafted	Produced AAR for exercise sponsored by another agency	Not applicable; AARs not done	EPA is in the process of drafting a formal AAR policy
USDA	No formal policy or process	Produces AARs for some exercises	AARs generally discuss interagency issues; AARs disseminated internally	GAO previously did not conduct a detailed review of USDA processes to capture lessons learned
VA	Formal policy is being drafted	Produces AARs for field exercises	AARs generally discuss interagency issues; AARs are disseminated internally, but not externally	GAO previously did not conduct a detailed review of VA processes to capture lessons learned
ATF	No formal policy	Does not produce AARs for exercises and special events	Not applicable; AARs not done	Performance degraded because AARs previously were produced for ATF exercises

Note: The period of review was July 1998 to June 2001.

Source: GAO analysis.

Interagency Process to Capture After-Action Reports Is Not in Place

Although some agencies adopted formal policies to capture lessons learned, there were recurring interagency problems because there was no central place where officials assembled and analyzed AARs together to discuss interagency problems. The Exercise Subgroup discussed developing a formal interagency process and has looked specifically at the processes being used by DOD and DOE, although no process has been adopted and developed. At the interagency level, there continues to be no formal process implemented to review and analyze AARs. The lack of an interagency process to centralize lessons learned prevents agencies from learning or cause them to make the same mistakes. This problem is further magnified because agencies that participated in national-level field exercises may have to wait up to a year before reviewing AARs because of the time it takes agencies to prepare AARs. After more than a year, the Department of Justice's Office for State and Local Domestic Preparedness Support released its AAR on the TOPOFF 2000 no-notice field exercise. Without AARs, agencies may not be able to correct previously identified shortfalls or fully implement lessons learned. The Office currently is planning the TOPOFF II exercise for fiscal year 2003.

Research and Development Enhances Future Federal Capabilities

Federal capabilities to combat terrorism can be enhanced through research and development. The considerable risk, long development time, and high cost necessitate federal government involvement to promote research and development related to WMD terrorism. Federal research and development programs are coordinated through a variety of mechanisms, but primarily through an interagency working group called the Technical Support Working Group (TSWG).[5] However, coordination is limited by a number of factors, raising the potential for duplicative efforts among federal agencies.

Research and Development Enhances Response Capabilities

Federally sponsored research and development efforts enhance the government's capability to combat terrorism by providing products that meet a range of crisis and consequence management needs. Federal agencies and interagency working groups have or are developing a variety of products to combat terrorism. Examples of recently developed and fielded technologies include products to detect and identify weapons of mass destruction, transport contaminated materials, and validate protection equipment life spans, such as

- tools for assessing exposure risks of airborne chemical and biological agents in new and existing structures in order to compare the relative risk to occupants under different release and protection scenarios,
- puncture- and tear-resistant containers in multiple sizes for the initial packaging and transport of chemical- and biological-contaminated objects,
- tests to determine the life span of chemical gas mask canisters when removed from protective containers and attached to gas masks, and
- computer-based information and instruction tool sets for first responders.

Additional technologies presently are under development by TSWG and federal agencies. These endeavors include developing continuous-monitoring chemical detectors for facility protection, filtration

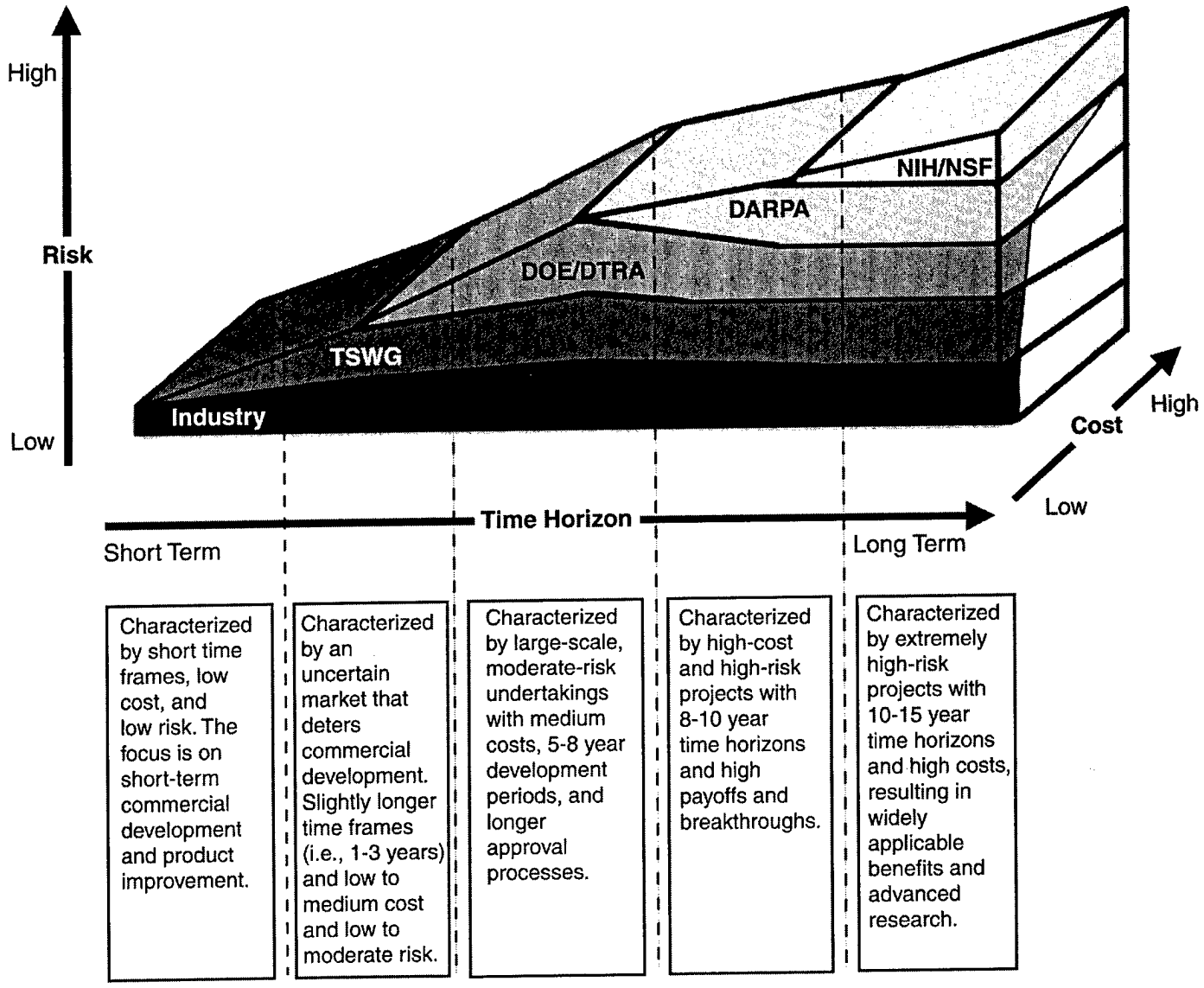
[5]TSWG was established as the technology development component of the Department of State-chaired Interagency Group on Terrorism. Its mission is to conduct the national interagency research and development program for combating terrorism. TSWG operates under the policy oversight of the Department of State Office of the Coordinator for Counterterrorism and the management and technical oversight of the DOD Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. An Executive Committee chaired by a Department of State representative provides program direction. Members of the Executive Committee include representatives from DOD, DOE, and the FBI. DOD manages and executes the program through the Combating Terrorism Technology Support Office.

systems for small rooms and buildings, modeling systems that project the spread of animal or plant disease outbreaks resulting from terrorist attacks, vehicle explosive screening and barrier technologies, and decontamination technologies for urban facilities, including subways and airports. The National Institutes of Health is engaged in research that will lead to the development of new or improved vaccines, antibiotics, and antivirals. The Centers for Disease Control and Prevention, in collaboration with other federal agencies, is conducting research on the diagnosis and treatment of smallpox. The Food and Drug Administration is investigating a variety of biological agents that could be used as terrorist weapons.

Research and Development Will Likely Require Government Involvement

Research and development related to WMD terrorism can involve considerable risk, lengthy development times, and high costs as well as specific requirements not available in off-the-shelf products. These factors not only limit and affect the type of research and development in which various sectors of the private and public markets engage, but necessitate federal government involvement and collaboration to promote research and development. For example, the Defense Advanced Research Projects Agency and the National Institutes of Health conduct high cost, very high risk, and time-intensive research and development in which industry typically may not engage. Figure 9 below depicts the relationship between risk, time, and cost associated with the development of products to combat terrorism, demonstrating that the federal government is the primary driver of WMD research and development.

Figure 9: Relationships Between Risk, Time, and Cost in Developing Products to Combat Terrorism



Source: GAO analysis of TSWG data.

Federal Research and Development Is Coordinated in a Variety of Ways

The Assistant to the President for Science and Technology heads the Office of Science and Technology Policy and serves on the cabinet-level National Science and Technology Council. These entities advise the President on the coordination of federal research and development investments and macro-level policies, plans, and programs. The Council establishes national goals for federal science and technology investment and prepares research and development strategies that are coordinated across federal agencies. The Council's Committee on National Security provides a formal mechanism for interagency policy review, planning, and coordination as well as the exchange of information regarding national security-related research and development. However, these organizations have not created a national research and development strategy specific to combating WMD-related terrorism. They also do not coordinate individual agency projects. As a result, the management of technology research and development at the agency-level is self-governing and highly dependent on voluntary coordination mechanisms. Individual agencies have a number of research and development or applied technology programs that are coordinated in varying ways and degrees with other agencies through formal and informal mechanisms.

The primary coordination mechanism for terrorism-related research and development is TSWG, an interagency working group that, in fiscal year 2000, coordinated more than $60 million in research and development activities across the counterterrorism community in eight categories of terrorism-related products. The eight categories are (1) explosives detection and defeat; (2) personnel protection; (3) tactical operations support; (4) infrastructure protection; (5) chemical, biological, radiological, and nuclear countermeasures; (6) investigative support and forensics; (7) physical security; and (8) surveillance, collection, and operations support. TSWG serves an important function, providing a way for technologies to be developed when a single agency cannot invest sufficiently in a technology that would benefit multiple agencies, collaborate directly with other agencies in such investments, or afford to risk investing scarce operational resources and manpower in unproven technologies. TSWG's purview represents a minor share of all terrorism-related research and development being conducted across the federal government because numerous federal agencies also independently engage in research and development or technology application projects specific to their respective agency missions for combating terrorism. In addition, TSWG's activities are limited to the development of products of use to—and supported by—the majority of its members.

Federal agencies also depend on informal coordination mechanisms, such as liaison programs and personal relationships, to facilitate information sharing concerning ongoing and planned research and development activities. For example, DOE maintains an informal liaison program with other agencies, including the Federal Aviation Administration. However, officials acknowledge that informal relationships cannot be expected to capture the universe of projects or inform agencies of all relevant and related research and development projects. For example, the Defense Advanced Research Projects Agency was unaware of U.S. Coast Guard plans to develop methods to detect biological agents on infected cruise ships and, therefore, was unable to share information on its research to develop chemical and biological detection devices for buildings that could have applicability in this area.

In commenting on a draft of this report, OSTP described more recent mechanisms to coordinate research and development related to combating terrorism within the NSC's Policy Coordinating Committee on Counterterrorism and National Preparedness. In implementing National Security Presidential Decision-1, dated February 2001, the NSC established the NSC-chaired Preparedness Against Weapons of Mass Destruction Group. It has eight subgroups, including the OSTP-chaired Research and Development Subgroup, which reports to the NSC chair. According to OSTP, all federal departments and agencies with interests, equities, or needs in research and development for combating terrorism are represented on the Research and Development Subgroup. To ensure communication and coordination of Subgroup activities and TSWG, a TSWG cochair is a member of the Subgroup.

According to OSTP, the Subgroup assesses federal research and development programs to help agencies integrate the highest priority items into their budgets, thereby reducing gaps and duplication in efforts to prevent, counter, and respond to chemical, biological, radiological, or nuclear terrorist attack. The Subgroup has a broad role in identifying long-range, large-scale research and development issues that involve preventing, countering, and responding to chemical, biological, radiological, or nuclear terrorist attacks. According to OSTP, the Subgroup is consulting with other subgroup chairs to identify comprehensive research and development needs in preparedness for combating terrorism; identifying and prioritizing research and development gap-filling objectives; implementing a process for reporting progress toward achieving research and development objectives; and continuing the ongoing effort to achieve concordance of research and development objectives with agency programs.

Limits to Coordination Raise Potential for Duplication

We reported in 1999 that current formal and informal research and development coordination mechanisms may not ensure that potential overlaps, gaps, and opportunities for collaboration are addressed.[6] A number of factors continue to limit research and development coordination, creating the potential for duplicative efforts among federal agencies. For example, TSWG's scope is limited to projects with relatively short-term development cycles and member federal agencies only propose and discuss projects that they believe will garner broad interest and support from other agencies. Information concerning research and development projects with more narrow applicability, but potentially of equal importance, either are not shared or are communicated through alternate methods. Furthermore, excluding TSWG, federal agency announcements and requests for proposals generally do not require contractors and national laboratories to disclose whether they are conducting the same or similar projects for other agencies or even to identify other requesters.

Federal agencies need to coordinate their research and development efforts because they pursue many of the same capabilities and may contract with many of the same laboratories and industries to perform research and development work. A DOE official acknowledged that a national laboratory developed similar products for multiple agencies and charged each of them separately. For example, two offices within Sandia National Laboratory concurrently and separately worked on similar thermal imagery projects for two different federal agencies, rather than consolidating the requests and combining resources. The Attorney General's Five-Year Plan recommended that responses to federal research and development requests for proposals identify pending similar submissions to mitigate against duplicate funding for essentially the same project and to facilitate collaboration among federal agencies.

The extent of compartmentalization of research and development activities further limits coordination. Many programs are compartmentalized or classified; therefore, results often are not widely shared, even among agencies with similar missions and, in some instances, even within the same agency. For example, DOE has three programs that focus on agency mission-specific research, development, and applied technology. DOE coordinates some programs' activities with a number of

[6] *Chemical and Biological Defense: Coordination of Nonmedical Chemical and Biological R&D Programs* (GAO/NSIAD-99-160, Aug. 16, 1999).

interagency organizations and groups, but does not coordinate other initiatives due to classification concerns. However, some DOE program officials coordinate with or participate in at least 12 interagency organizations and groups involved in technology application programs for combating terrorism.

Federal coordination is limited by the lack of formal mechanisms to capture the entire universe of governmentwide research and development efforts. The absence of a single oversight and coordinating entity to ensure against duplication further hinders coordination. To address this problem, the Attorney General's Five-Year Plan calls for a comprehensive mechanism and research and development strategy consistent with and complementary to the nation's overall technology goals. The plan advocates setting national counter-terrorism priorities, tracking ongoing projects consistent with these priorities, defining near- and longer-term technology needs, supporting fundamental research in targeted technical sectors, and promoting technological breakthroughs.

The development of such a plan may benefit individual agency efforts. Some individual agencies, such as DOE and the Department of Transportation, have developed agency-specific research and development plans that are linked to their overall agency strategic plans that may identify agency-specific research and development goals and objectives as well as the roles of other federal agencies in achieving those goals. For example, the Department of Transportation Research and Development Plan supports the Department's budget and program development process, establishes priorities, and links research and technology development initiatives occurring throughout the Department to specific strategic goals. By focusing on research and development needs that concern the Department as a whole, the plan allows the Department of Transportation to transcend individual research and development projects and facilitates internal planning and coordination. If a governmentwide research and development strategy to combat terrorism was completed, then it would provide a way for agencies, through their own plans or related efforts, to link their research and development to related efforts where appropriate.

Conclusions

Although FEMA has made some progress, it is not using exercises to fully practice its leadership role over consequence management. If FEMA played a larger role in managing federal exercises to combat terrorism, then it would improve federal agencies' overall readiness in consequence management. In addition, if FEMA was more involved in the initial planning phases of field exercises within the Interagency Working Group

on Exercises, then major interagency field exercises could include a more robust consequence management component. Active leadership and participation within the Working Group would allow FEMA to (1) establish objectives and prepare a schedule of large interagency counter-terrorist exercises and (2) ensure that complex transfers of command and control between agencies are exercised. Without field exercises involving a consequence management component, federal agencies are not able to train and exercise their response capabilities, deploy personnel and equipment, and practice roles and responsibilities under realistic conditions.

To ensure that individual agencies learn lessons after each federal counterterrorism exercise, special event, or operation, agencies should prepare a timely AAR or other evaluation that documents the results. Dissemination of AARs within an agency—and, whenever possible and appropriate, to other participating agencies—would provide participants with information on the operations that worked well and those that need improvement. Finally, taking corrective action and effective follow-up would help ensure that problems are corrected.

At the interagency level it is also important to capture and evaluate lessons learned. While most agencies are making progress evaluating their own exercises, little progress has been made at the interagency level. There is a need for a regular lessons learned process for major interagency exercises.

Although research and development efforts are being coordinated through a variety of mechanisms, development of a strategic plan for research and development could help prevent duplication and leverage resources. OSTP's efforts are on hold pending the Vice President's review of national preparedness.

Recommendations for Executive Action

To improve readiness in consequence management, we recommend that the Director of the Federal Emergency Management Agency play a larger role in managing federal exercises to combat terrorism. As part of this, FEMA should seek a formal role as a cochair of the Interagency Working Group on Exercises and help to plan and conduct major interagency counterterrorist exercises to ensure that consequence management is adequately addressed.

To ensure that agencies benefit fully from exercises in which they participate, we recommend that the Secretaries of Agriculture, Defense, Energy, Health and Human Services, and Veterans Affairs; the Directors of the Bureau of Alcohol, Tobacco, and Firearms, Federal Emergency

Management Agency, Federal Bureau of Investigation, and the U.S. Secret Service; the Administrator of the Environmental Protection Agency; and the Commandant of the U.S. Coast Guard require their agencies to prepare AARs or similar evaluations for all exercises they lead and for all field exercises in which they participate.

To ensure that individual agencies capture, evaluate, and disseminate interagency lessons learned after each federal counterterrorism exercise, special event, or operation, we recommend that the President direct the focal point for overall leadership and coordination (discussed at the end of ch. 2) to develop a formal process to capture and evaluate interagency lessons learned from major interagency and intergovernmental federal exercises to combat terrorism. While agencies sponsoring and participating in such exercises should continue to collect and analyze information on their individual performance, the focal point should analyze interagency lessons learned and task individual agencies to take corrective actions as appropriate.

To reduce duplication and leverage resources, we recommend that the Assistant to the President for Science and Technology complete efforts to develop a strategic plan for research and development to combat terrorism, coordinating this with federal agencies and state and local authorities. If our recommendation in chapter 2 is adopted and a single focal point is established in the Executive Office of the President to lead and coordinate federal programs to combat terrorism, then the focal point should also ensure that a research and development strategy for combating terrorism is integrated or coordinated with the national strategy to combat terrorism (see Recommendations for Executive Action in ch. 2).

Agency Comments and Our Evaluation

Agency comments on a draft of this report were based on their efforts prior to the September 11, 2001, terrorist attacks. FEMA agreed with our recommendation that it play a larger role in managing federal exercises to combat terrorism. FEMA said the creation of the Office of National Preparedness in FEMA to coordinate all federal programs dealing with WMD consequence management and its May 8, 2001, charge (see app. VII) by the President to work with the Department of Justice to ensure that "all facets of our response to the threat from weapons of mass destruction are coordinated and cohesive" will improve consequence management readiness and will ensure that FEMA plays a larger role in federal exercises. FEMA also agreed with our recommendation that it should seek a formal role as cochair of the Interagency Working Group on Exercises.

The Departments of Energy and Health and Human Services and EPA also agreed that exercises to combat terrorism need a more robust consequence management emphasis. For example, DOE said it would be very beneficial to exercise the complete domestic counterterrorism command and control and response mechanisms using a realistic, progressive, end-to-end scenario with participation by the actual decision makers through both the crisis management and consequence management phases. In general, EPA is in agreement with the report. One of EPA's principal concerns has been the lack of development of consequence management in exercises. Beyond the immediate consequences caused by the use of a weapon of mass destruction, the long-term consequences of cleaning up to a safe level have not been played out.

The Departments of Defense, Energy, Justice, and Veterans Affairs and FEMA concurred with our recommendation that agencies prepare AARs or similar evaluations for all exercises they lead and for all field exercises in which they participate. DOD encourages this practice. DOE said the report's recommendations on the importance of interagency exercises and feedback on lessons learned are completely accurate. FEMA said it will review and evaluate its current procedures regarding AARs and make any necessary changes to ensure that its AARs for weapons of mass destruction are completed in a timely fashion.

The Department of Agriculture agreed with the practice of writing AARs, but asked that we delete our recommendation to the Secretary of Agriculture because the Department already produces AARs for exercises it sponsors. We continue to believe that this is a valid recommendation because the Department could learn important lessons when it participates in field exercises sponsored by other agencies.

The Department of Health and Human Services, ATF, the U.S. Secret Service, EPA, and U.S. Coast Guard did not comment on this recommendation.

The Department of Justice supported our recommendation about agencies capturing and sharing lessons learned at the interagency level. The Department also cited efforts begun by the NDPO to develop a program to address this concern. This program would include a mechanism for not only identifying interagency problems, but assigning responsibility for corrective actions and tracking progress as well. The Executive Office of the President did not comment on our recommendation that the President

direct the focal point to develop a formal process to capture and evaluate interagency lessons learned from exercises to combat terrorism.

DOE said it shares our observations on the importance of an aggressive counterterrorism research and development effort. DOE stated that better interagency communication and a more extensive and formal coordination mechanism would increase efficiency, be more cost effective, and ensure against duplication of effort. Department of Transportation officials commented that the report may help them in their research and development efforts. The Executive Office of the President—and the Office of Science and Technology Policy—did not comment on our recommendation that the Assistant to the President for Science and Technology complete efforts to develop a strategic plan for research and development to combat terrorism. Notwithstanding agencies' lack of comment on this recommendation, we still believe it has merit as one method to better coordinate research and development.

Chapter 5: Federal Assistance to State and Local Governments Can Be Consolidated

The federal government has several programs to train and equip state and local authorities to respond to terrorist WMD incidents. These programs have improved domestic preparedness training and equipped over 273,000 first responders. The programs also have included exercises to allow first responders to interact with themselves and federal responders. Some of these programs initially were implemented without appreciation for existing state and regional structures for emergency management. In addition, the fact that these programs have been led by three different federal agencies—DOD, the Department of Justice, and FEMA—created overlapping and duplicative activities. The multitude and overlap of these programs led to confusion on the part of state and local officials. These officials asked the federal government to establish a single federal liaison for them. In 1998, the Attorney General established the National Domestic Preparedness Office (NDPO) within the FBI to serve as such a liaison. However, the Office never met its expected role due to a variety of reasons related to its budget, personnel, and location. In May 2001, the President asked the Director of FEMA to establish an Office of National Preparedness to coordinate all federal programs dealing with WMD consequence management programs. This new Office provides a logical location for consolidating many programs to assist state and local governments, including some programs currently under the Department of Justice and the FBI. Federal assistance also has been provided in the form of special National Guard teams that are trained and equipped to provide states with capabilities to detect and analyze WMD agents and provide technical advice. These teams continue to experience problems with readiness, doctrine and roles, and deployment that undermine their usefulness in an actual terrorist incident.

Federal Programs Have Provided Training, Equipment, and Exercises

The federal government has had several programs that train and/or equip state and local authorities to respond to terrorist WMD incidents. Whereas DOD ran the Domestic Preparedness Program from 1997 until 2000, the Department of Justice, HHS, and FEMA are the main agencies now conducting these programs. They also have included exercises to allow first responders to interact with themselves and federal responders in realistic field settings. These programs are as follows:

- DOD began the Domestic Preparedness Program in 1997 to enhance the nation's ability to mitigate the effects of terrorist use of weapons of mass

destruction.[1] The program identified 120 cities to receive training, exercises, and funding for training equipment support. The program provided cities with classroom training, exercises, and 5-year renewable loans of equipment to be used for training. Beginning in fiscal year 2001, the President transferred responsibility for the program from DOD to the Department of Justice.

- The Department of Justice's Office for State and Local Domestic Preparedness Support, which was created in 1998, provides assistance to state and local governments. This Office has a variety of programs, such as its Metropolitan Firefighters and Emergency Medical Services program. Since fiscal year 2001, it also implements the domestic preparedness program formerly managed by DOD. The Office also uses DOD's Pine Bluff Arsenal, the National Sheriff's Association, the International Association of Fire Fighters, private corporations, and the National Domestic Preparedness Consortium to train first responders.[2] In total, the Office provides 30 courses using 10 different partner organizations to deliver training.
- FEMA provides WMD-related courses at its National Fire Academy and Emergency Management Institute in Maryland. The Academy and Institute also provide WMD course materials to local and state organizations for their use in training first responders. FEMA makes grants for terrorism-related training to states at either local or FEMA regional locations. FEMA also makes grants to help states develop and test their emergency plans through exercises.
- HHS supports the development of Metropolitan Medical Response Systems in order to enhance local planning and health care capacity to respond to the health consequences of a WMD release. This program encourages local jurisdictions to strengthen regional and state response relationships. Begun in 1996, the program now includes 97 metropolitan jurisdictions or areas with a total population of approximately 150 million people. The U.S. Public Health Service Noble Training Center, located in the former Noble Army Community Hospital at Fort McClellan in Anniston, Alabama, provides a unique medical training facility dedicated to preparing health personnel to respond to chemical and biological weapons attacks.

[1]The program was directed by the Defense Against Weapons of Mass Destruction Act of 1996 (P.L. 104-201, Sept. 23, 1996). Because of the Senators who authored the original bill in the U.S. Senate, the program was also known as the Nunn-Lugar-Domenici program.

[2]The consortium consists of five facilities that provide training, including Fort McClellen, Ala., New Mexico Institute of Mining and Technology, Texas A&M University, Louisiana State University, and the Nevada Test Site.

Several other federal organizations offer courses that are not directed specifically at responding to WMD incidents, but provide first responders with valuable skills and knowledge in handling hazardous materials. For example, the EPA offers several courses in how to handle incidents involving hazardous materials and DOE offers several courses aimed at handling the consequences of radiological incidents. In addition, HHS' National Institute for Occupational Safety and Health offers training to the health community in areas such as hazardous materials. Many of these courses are related to the agencies' core mission and basic functions independent of combating terrorism.

Through these programs, thousands of first responders have been trained and now have a greater awareness of how to respond to a potential chemical or biological terrorist incident. For example, local officials credited DOD's Domestic Preparedness Program with bringing local, state, and federal regional emergency response agencies together into a closer working relationship. As of October 1, 2000 (when the Department of Justice took over the program), DOD had completed training in 105 cities that included 4 days of training plus a chemical tabletop exercise. In addition, 68 of those 105 cities also received additional training, which included delivery of equipment plus a chemical field exercise and a biological tabletop exercise. Table 6 shows the number of first responders trained by DOD, the Department of Justice, and FEMA.

Table 6: State and Local Responders Receiving Federal WMD Training, Fiscal Years 1998 to 2001

Federal WMD Training Program	FY 1998	FY 1999	FY 2000	FY 2001	Total
Department of Justice Metropolitan Firefighters and Emergency Medical Services Program	24,955	20,925	4,221	1,695	51,796
Department of Justice National Domestic Preparedness Consortium	49	2,022	9,375	14,059	25,505
Department of Defense/Department of Justice Domestic Preparedness Program	9,348	9,119	9,077	630	28,174
FEMA National Fire Academy and Emergency Management Institute	43,759	51,693	40,982	31,891	168,325
Total	78,111	83,759	63,655	48,275	273,800

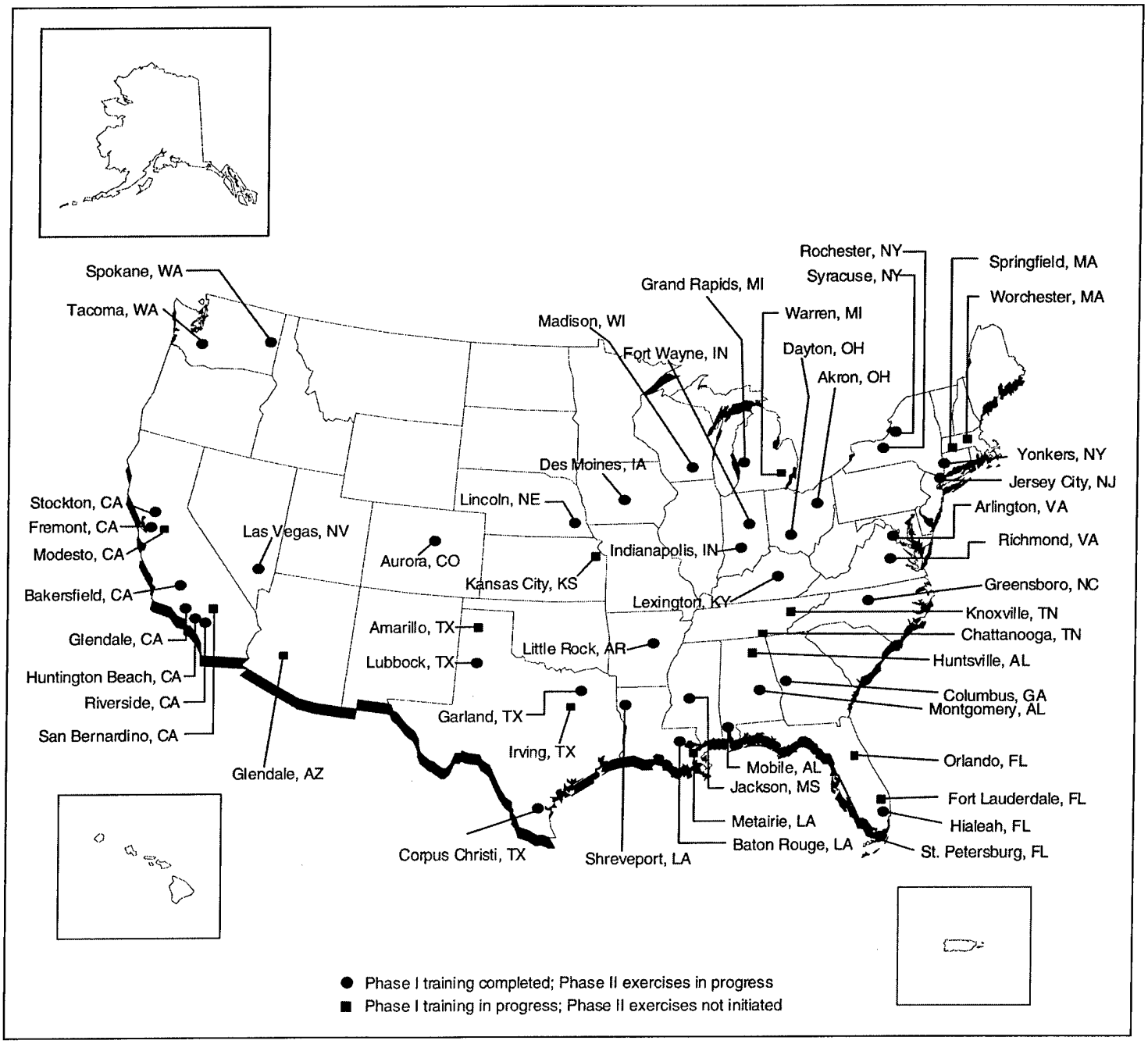
Note: Fiscal year 1998-2000 data are complete. Department of Justice data for fiscal year 2001 are through August 31, 2001; and FEMA data for fiscal year 2001 are through July 31, 2001. All Domestic Preparedness Program training for fiscal years 1998-2000 was conducted by DOD; thereafter, by the Department of Justice.

Source: Data from DOD, the Department of Justice, and FEMA.

Figure 10 shows the status of 53 remaining cities that are receiving Domestic Preparedness Program first responder training. These 53 cities represent the number of the original 120 cities that remained after DOD

transferred the program to the Department of Justice on October 1, 2000. As shown by the map, about two-thirds of the cities have completed the initial training and have begun the exercise phase. The remaining one-third of the cities have initiated the training phase, but have not begun the exercise phase. Phase I initial training includes 4 days of training and a 1-day chemical tabletop exercise. Phase II consists of equipment support and exercises.

Figure 10: Status of 53 Remaining Cities Receiving Domestic Preparedness Program First Responder Training



Note: Data are current as of August 31, 2001.

Source: Department of Justice.

Figure 11 shows an intergovernmental exercise in which federal, state, and local emergency responders exercised together.

Figure 11: Salt Lake City, Utah, Fire Department Personnel Treat "Victim" During Wasatch Rings Exercise in Preparation for the 2002 Olympic Winter Games

Source: GAO.

Improvements Made in Delivery and Coordination of Assistance

As we reported earlier, some WMD training programs initially failed to leverage existing state and local response mechanisms.[3] DOD provided training to cities without taking advantage of the existing state emergency management structures, mutual aid agreements among local jurisdictions, or other collaborative arrangement for emergency response. For example, California has a Specialized Training Institute that provides emergency management training to first responders statewide; in Texas, the state's Division of Emergency Management conducts training for local responders. Use of these capabilities and mechanisms could have allowed training consolidation and could have resulted in far fewer training sessions. Training in fewer locations and taking advantage of existing emergency response structures could have hastened the accomplishment of program goals and have the added benefit of reinforcing local response integration. Such an approach also could have covered a greater percentage of the population and make effective use of existing state emergency management training venues.

In taking over the DOD domestic preparedness program, the Department of Justice has taken a number of steps to improve the delivery of the program to better leverage existing state and local programs. For example, the Department plans to modify the former DOD program's delivery in metropolitan areas by requiring cities to include their mutual aid partners in all training and exercise activities. The Department also has made the training timeline more flexible, to better fit into state and local training schedules. In addition, the Department has provided grants to defray administrative costs of conducting analysis and planning for the programs. Equipment loans from DOD—a source of confusion and frustration among local officials over maintenance responsibility and the final disposition of the equipment—were converted into a grant program when the Department of Justice took over.

FEMA programs did not appear to have these deficiencies. FEMA already leveraged state and local mechanisms by delivering numerous courses through and in cooperation with state and local fire training academies and emergency managers.

Our earlier reports also found that federal assistance programs were overlapping and potentially duplicative. In a March 2000 report, based

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

upon an extensive review and comparison of training programs and curriculum, we found that federal training programs on WMD preparedness are not well coordinated among agencies, resulting in inefficiencies and concerns in the first responder communities.[4] The three main agencies at that time—DOD, the Department of Justice, and FEMA—were providing similar awareness courses as part of their train-the-trainer programs. We recommended that DOD, the Department of Justice, and FEMA eliminate their duplicative training programs.

Based upon our previous recommendation, a number of steps have been taken to reduce duplication and improve coordination. DOD transferred its Domestic Preparedness Program to the Department of Justice starting in fiscal year 2001. The Department of Justice is integrating the DOD program into its own program. It conducted a side-by-side analysis of course content, learning objectives, and instructional methods for its existing program and the DOD program it took over. The Department of Justice eliminated DOD's awareness course because it duplicated a similar course. The Department of Justice and FEMA have coordinated their awareness training courses, with the FEMA course being delivered to state training academies and the Department of Justice course being delivered to local jurisdictions that have not been reached by the state academies.

Efforts also have increased to coordinate assistance efforts across all agencies. The NSC established an interagency working group on Assistance to State and Local Authorities to review and guide WMD training and equipment programs. Several other agencies involved in training have established a Training Resources and Data Exchange working group. This group has initiated the development of agreed-upon learning objectives by discipline and competency level for federal training efforts. Other efforts include an interagency joint course development and review process. According to the Department of Justice, this group represents an effort towards the elimination of duplicative federal efforts and non-standard federal training curriculum. The Department of Justice has set up a centralized scheduling desk to help manage the many training and exercise activities in which state and local governments participate.

Despite these changes, state and local officials have expressed concerns about duplication and overlap among federal programs for WMD training

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

and other related courses. Some officials said that the number of federal organizations involved in WMD training creates confusion about which federal organization is in charge of that training. Department of Justice officials believe that their efforts have eliminated confusion among state and local officials. However, our recent discussions with state and local officials from Colorado and recent testimonies by organizations representing first responders, indicate that there still is confusion about federal assistance programs. For example, a representative of the International Association of Fire Chiefs—a Department of Justice partner for providing training to state and local governments—testified that it has been their experience in a number of jurisdictions that efforts undertaken to date at the federal level, while by themselves valuable, would benefit greatly from an increased level of coordination and accountability. According to the Association, efforts that may be duplicative or worse, contradictory, lead to confusion at the local level and expend precious federal resources unnecessarily. The Association said efforts underway at the federal, state, and local levels of government ought to be better synchronized for the benefit of public safety. At the federal level, there certainly is expertise located in different agencies that should be leveraged to create the most effective preparedness effort possible. The Association representative believed this could be better accomplished by designating one federal official with responsibility and authority to coordinate and deliver these programs. The Association has in the past requested a single point-of-contact in Washington to whom it can turn for answers and provide input.[5]

Federal Liaison for State and Local Responders Did Not Meet Expectations

Groups representing first responders repeatedly called for a single liaison in the federal government to provide "one stop shopping" for federal assistance. They said that first responders were confused by the multitude of federal programs from different agencies. In response to these concerns, the Attorney General established the NDPO in October 1998 under the management of the FBI to serve as a single point of contact for state and local authorities. NDPO was to be staffed by personnel detailed from a variety of federal, state, and local governments with consequence

[5]See *Preparedness Against Domestic Terrorism Act of 2001 (H.R. 525)*, Statement by the International Association of Fire Chiefs before the Subcommittee on Economic Development, Public Buildings and Emergency Management, Committee on Transportation and Infrastructure, U.S. House of Representatives, May 9, 2001, pp. 2-3. Officials from other organizations representing first responders, such as the National Emergency Management Association and the National League of Cities, made similar comments.

management roles. NDPO was to coordinate federal efforts and resources to assist state and local governments in planning, training, exercising, and providing equipment to enhance their readiness to respond to a WMD incident. NDPO officials have cited a number of accomplishments to include starting a state and local advisory group, developing planning guides, and publishing an on-scene commander's guide.

However, groups representing first responders have said that the NDPO had not met their expectations. Our work indicates that there were several reasons for NDPO not realizing its original purpose, including the following.

- There was insufficient funding for NDPO (it had no direct funding for its first 2 years).
- There was little staffing from NDPO's interagency and intergovernmental partners, so the Office lacked key functional expertise.
- There was no consensus on NDPO's role in relation to other federal entities.
- NDPO's location in the FBI building hampered interaction with first responders.
- First responders did not perceive NDPO as independent.

New Office Offers Potential to Consolidate Assistance Programs Under FEMA

In May 2001, the President announced the establishment of a new Office of National Preparedness in FEMA that will lead the federal government in the oversight, coordination, integration, and implementation of domestic preparedness and consequence management programs and activities for WMD-related threats. The new Office will be expected to coordinate all federal programs to support state and local preparedness and consequence management response involving planning, training, exercises, research and development, expert advice, and equipment acquisition. At the time of our review, FEMA was still planning this Office. We believe the creation of this Office is a positive development for three reasons. The first reason is that FEMA—as the lead agency for consequence management and preparing state and local governments for WMD terrorism—is the most logical agency to coordinate these functions. The second reason is that the announcement, coming from the President, clearly puts FEMA in the lead for this governmentwide matter. Finally, we believe the creation of the new Office of National Preparedness within FEMA provides the opportunity to consolidate certain programs or offices currently run by the Department of Justice and the FBI. However, the Department of Justice and the FBI would retain their law enforcement and investigative roles and responsibilities.

Establishment of the Office of National Preparedness creates the potential to consolidate some Department of Justice assistance programs into FEMA. The Department of Justice's Office for State and Local Domestic Preparedness Support provides assistance to state and local governments in the form of grants and exercise support. This Department of Justice Office also performs substantial liaison with state and local governments when administering its grants. In fact, the lead recipients of these Department of Justice grants are the state emergency management agencies—the core clients for FEMA's assistance programs. These Department of Justice programs might be more appropriately consolidated within FEMA because it is the lead agency for domestic preparedness as well as emergency management in general. While it is unclear whether the new FEMA Office will administer grants and related assistance, having such programs consolidated under FEMA, in proximity to its new Office of National Preparedness, may simplify federal assistance from the perspective of state and local governments. Conversely, the continuance of multiple assistance programs run by FEMA and the Department of Justice may continue the current confusion and frustration among the first responder community.

In addition, the creation of the Office of National Preparedness provides the opportunity to consolidate the NDPO or its functions into FEMA. As stated above, the new FEMA Office will be expected to coordinate all federal consequence management programs to support state and local preparedness involving planning, training, exercises, expert advice, and equipment acquisition. These activities are very similar to the purpose of the NDPO. Once the Office of National Preparedness is in place, we believe that the continued existence and operations of the NDPO would not be needed. As with the Office for State and Local Domestic Preparedness Support, the existence of both the NDPO and the new Office of National Preparedness will continue to create confusion and frustration among the first responder community. As of August 2001, negotiations were ongoing between the Attorney General and the Director of FEMA about transferring NDPO's functions and some of its personnel to FEMA's new Office of National Preparedness. Once the new Office is operational, the Department of Justice plans to shut down NDPO.

Federally Funded National Guard Teams Continue to Experience Problems

In addition to training and equipping first responders, the federal government has provided assistance to state governments by establishing specialized National Guard teams, known as Weapons of Mass Destruction Civil Support Teams. These teams—originally called Rapid Assessment and Initial Detection or "RAID" teams—were developed to assist state and local authorities in responding to a terrorist incident involving weapons of mass destruction. Although the federal government funds the teams, they are considered state assets operating under the Governor and Adjutant General of their state.[6] Twenty-seven teams have been established and the Congress has authorized an additional five teams. DOD plans—and officials suggested—that there eventually should be a team in each state, territory, and the District of Columbia, for a total of 54 teams. At least one state, California, has two teams. The teams are composed of 22 full-time members of the National Guard, organized into six functional areas. The teams include personnel with a military occupational specialty in WMD warfare.

Earlier GAO and DOD Inspector General reports, as well as our more recent observations, indicated there are continued problems with these teams regarding their readiness, doctrine, roles compared to other teams, and time to deploy.[7] DOD concurred with recent recommendations by its Inspector General to address these problems. The specific problems experienced by these teams are as follows.

- The readiness of the teams has fallen behind schedule. In the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999, the Congress required that none of the National Guard teams could be used to respond to an emergency unless the Secretary of Defense certifies that the team has the requisite skills, training, and equipment to be proficient in all mission requirements. According to the DOD Inspector General, the Army's process for certifying the teams lacked rigor and would not provide meaningful assurance of their readiness. As a result, the program schedule has slipped. Although the first 10 teams originally were

[6]Although the National Guard teams generally would remain as state assets when activated in response to a terrorist incident under title 32, they could be federalized into the U.S. military under title 10.

[7]Our earlier report was *Combating Terrorism: Use of National Guard Response Teams Is Unclear* (GAO/NSIAD-99-110, May 21, 1999). The DOD Inspector General report was *Management of National Guard Weapons of Mass Destruction-Civil Support Teams* (DOD-IG D-2001-043, Jan. 31, 2001).

scheduled to be fully operational by January 2000, a total of nine teams had been certified as operational during July and August 2001.

- The doctrine and role for the teams were not well developed. According to the DOD Inspector General, the Army developed doctrine for the teams independently, without coordinating with appropriate military and civilian organizations. Specifically, the Army developed the doctrine independent of the Joint Task Force for Civil Support (which would be the higher headquarters for the teams if they were federalized) and the FBI (which would act as the lead federal agency during a crisis). The absence of finalized doctrine has encouraged and promoted an environment of persistent changes to operational concepts and mission requirements. The DOD Inspector General recommended that DOD coordinate with the FBI to determine the exact roles and missions that the National Guard teams would fulfill.
- The teams' original role of planning for follow-on military assets is now done by another organization. Both DOD and the Army have stated that the National Guard teams could be used to identify additional military units that could provide support in an incident. However, the establishment of the Joint Task Force for Civil Support in October 1999 made this task no longer necessary for the National Guard teams. The Joint Task Force for Civil Support is DOD's single point for command, control, and advice on DOD support to terrorist WMD incidents.
- The team's role in providing technical assistance overlaps with other federal teams. There are numerous other military and federal organizations that can help incident commanders deal with WMD by providing advice, technical experts, and equipment. As in our earlier review, officials with the two agencies responsible for managing the federal response to a terrorist incident—the FBI and FEMA—continue to be skeptical about the role of the National Guard teams. For example, the head of the FBI's Hazardous Materials Response Unit noted that the FBI unit, not the National Guard teams, would be the authoritative source of technical advice on WMD matters during crisis management. The FBI official also noted that many of the same federal experts from DOD, HHS, and DOE would be providing advice to both the National Guard teams and the Hazardous Materials Response Unit.
- The teams' role in providing technical assistance may also overlap with state and/or local teams. There are over 600 local and state hazardous materials teams in the United States that daily have to assess and take appropriate actions in incidents involving highly toxic industrial chemicals and other hazardous materials. Large jurisdictions, for example, usually have robust capabilities to deal with hazardous materials. DOD's plans for the National Guard teams did not consider these state and local teams.

- The teams' deployment times remain uncertain. The original plans for the teams were based upon an assumption that they would deploy and arrive quickly. Although plans call for the teams to deploy within 4 hours, transporting the team to a distant location with its equipment may require military airlift. However, there are no plans to arrange for dedicated airlift to the teams in case of contingencies. In our earlier review, officials at the state and local level cited the importance of the first 2 hours and thus questioned the benefits of the National Guard teams because of potential time lags before they arrive. For example, officials from two states indicated that the usefulness of the National Guard teams may have been overstated in the recent TOPOFF 2000 exercise because both were essentially pre-deployed.

In our earlier report, we stated that the Congress may wish to consider restricting the use of appropriated funds for any additional National Guard teams without further assessments. Similarly, the DOD Inspector General recommended that DOD conduct a thorough program evaluation of the teams, including such areas as operational concept and doctrine. DOD concurred with the recommendations of the Inspector General to address these problems and is initiating a comprehensive review of the teams. DOD, among other corrective actions, has agreed to coordinate the roles of the National Guard teams with the FBI. However, our assessment is that, until some of the above issues are resolved, the roles and use of these National Guard teams are unclear.

Conclusions

Despite efforts to reduce duplication in assistance programs, there are still multiple programs that create confusion among the first responders these programs are meant to serve. Based upon our earlier recommendations, the Executive Branch has taken steps to reduce duplication and improve coordination of assistance programs. However, an attempt to create a single liaison for state and local governments through the NDPO was not successful for a variety of reasons. The creation of the new Office of National Preparedness in FEMA, while leaving the Department of Justice's Office of State and Local Domestic Preparedness Support and FBI's NDPO programs in place, will create additional duplication of effort and more confusion among the first responders. The new FEMA Office provides a logical location for consolidating federal programs to assist state and local governments, including the Office for State and Local Domestic Preparedness Support and the NDPO.

National Guard Weapons of Mass Destruction Civil Support teams continue to experience problems with readiness, doctrine and roles, and

deployment that could undermine their usefulness in an actual terrorist incident. The establishment of any additional teams would be premature until DOD has completed its coordination of the teams' roles and missions with the FBI—the lead federal agency for crisis management. In our view, such coordination will not be complete until there is a written agreement between the DOD and the FBI that clarifies the roles of the teams in relation to the FBI.

Recommendations for Executive Action

To eliminate overlapping assistance programs and to provide a single liaison for state and local officials, we recommend that the President, working closely with Congress, consolidate the activities of the FBI's National Domestic Preparedness Office and the Department of Justice's Office for State and Local Domestic Preparedness Support under the Federal Emergency Management Agency.

To clarify the roles and missions of specialized National Guard response teams in a terrorist incident involving weapons of mass destruction, we recommend that the Secretary of Defense suspend the establishment of any additional National Guard Weapons of Mass Destruction Civil Support Teams until DOD has completed its coordination of the teams' roles and missions with the FBI. We also recommend that the Secretary of Defense reach a written agreement with the Director of the FBI that clarifies the roles of the teams in relation to the FBI.

Agency Comments and Our Evaluation

Agency comments on a draft of this report were based on their efforts prior to the September 11, 2001, terrorist attacks. The Department of Justice agreed with our recommendation that the NDPO be consolidated into FEMA's new Office of National Preparedness. The Department said it is prepared to coordinate the transfer of the functions of that office to FEMA, including the detailing of staff as appropriate, once the new Office is operational.

However, the Department of Justice disagreed with our recommendation that its Office for State and Local Domestic Preparedness Support also be consolidated into FEMA. According to the Department, shifting the facilitation and coordination function to FEMA should not affect its programs in the Office of Justice Programs, including the Office for State and Local Domestic Preparedness Support. The Department stated that those programs "fit squarely" within the Office of Justice Program's mission of providing grant assistance to state and local governments. We are not challenging the basic mission of the Office of Justice Programs to

provide grant assistance to state and local governments. However, it is important to note that other federal agencies, including FEMA, also provide grants to state and local governments. The key question is what agency is the most appropriate one to provide such assistance specifically related to domestic preparedness. In our view, FEMA is the lead agency for domestic preparedness and should, therefore, coordinate and implement such programs. Therefore, we continue to believe our recommendation has merit.

In technical comments that supplemented their letter, officials from the Department of Justice and its Office for State and Local Domestic Preparedness Support cited additional reasons why they did not agree with our recommendation that the Department's assistance programs be consolidated under FEMA. They said that the responsibilities we state for FEMA's new Office of National Preparedness are broader than those announced by the President and those agreed upon between FEMA and the Department of Justice. They also said that our recommendation was based upon the erroneous conclusion that FEMA is the lead agency for preparing state and local governments to deal with the consequences of WMD terrorism. These officials stated that from both a legal and programmatic perspective, the Department of Justice clearly is the lead agency for domestic preparedness and such programs are already consolidated there. We disagree. While the responsibilities of FEMA's new Office of National Preparedness are still in development, we continue to believe that FEMA is the lead agency for preparing state and local governments for the consequences of WMD terrorism.[8]

Officials from the Office for State and Local Domestic Preparedness Support also said that our recommendation was done without any analysis of FEMA's capacity or capability to lead national preparedness efforts. Specifically, they said that "investing domestic preparedness programs responsibilities in a sub-Cabinet agency charged with dealing with dozens of disasters and emergencies each year places responsibility in an agency that will be severely challenged to provide the necessary sustainment and continuity." We disagree with this position because we believe that FEMA's continuous experience in dealing with the consequences of a wide variety of disasters—through both preparedness programs and responses

[8]FEMA is responsible for emergency preparedness under 42 U.S.C. chapter 68. FEMA also has lead responsibilities for emergency preparedness under Executive Order 12656 and is responsible for ensuring that state plans are adequate and capabilities are tested under PDD 39.

to real incidents—makes it the most appropriate agency to lead national preparedness efforts. FEMA officials indicated to us that the new Office of National Preparedness would be responsible for providing sustainment and continuity to the efforts—by both FEMA and the rest of the federal government—to improve national preparedness.

FEMA indicated that our recommendation to consolidate programs was premature. FEMA believes that before any additional mandates or changes are placed on the new Office of National Preparedness, it needs a chance to accomplish its tasks as put forth by the President—to coordinate federal programs dealing with WMD consequence management, working closely with state and local governments to ensure that their needs are addressed. FEMA said there are no plans to take programs away from other departments or agencies. However, officials from FEMA told us they disagreed with the position taken by the Office for State and Local Domestic Preparedness Support that the Department of Justice, and not FEMA, is the lead agency for preparing state and local governments for WMD terrorism. These officials stated that FEMA is designated the lead agency, and that the President's May 8, 2001, statement (see app. VII) clearly reinforces FEMA's lead role.

Although the Department of Justice and FEMA did not support our recommendation, we still believe it has merit. Consolidation of DOD's programs to the Department of Justice simplified the delivery of assistance and resulted in reduced duplication. Further consolidation under FEMA—the lead agency for domestic preparedness—could simplify and coordinate these programs even more. Contrary to Department of Justice assertions, confusion still exists among first responders regarding the multitude of federal agencies involved. Organizations representing first responders still are calling for a single coordination point. In addition, the fundamental disagreement between the Department of Justice and FEMA as to which agency is the lead for national preparedness reinforces our recommendations that a single focal point is needed above the level of individual agencies (see ch. 2) and our recommendation above that preparedness programs should be consolidated.

The Department of Defense concurred with GAO's recommendation that the Secretary of Defense suspend the establishment of any additional National Guard Weapons of Mass Destruction Civil Support Teams until the Department has completed its coordination of the teams' roles and missions with the FBI. Finally, the Department concurred with GAO's recommendation that the Secretary of Defense reach a written agreement with the Director of the FBI that clarifies the roles of the teams in relation

to the Bureau. FEMA, in its response to a draft of this report, said DOD also should consult with FEMA on the role of the Civil Support Teams.

Chapter 6: Limited Progress in Implementing a Strategy to Counter Computer-Based Threats

In addition to efforts to combat terrorism discussed in chapters 2 through 5, the federal government has begun to develop and implement a strategy for combating the threat of cyber, or computer-based, attacks. Protection against cyber attacks requires vigilance against a broader array of threats, to include not only terrorists, but nation states, criminals, and others. The strategy was outlined in PDD 63, issued in May 1998, which describes a plan for protecting the nation's critical computer-supported infrastructures, such as telecommunications, power distribution, financial services, national defense, and critical government operations, from physical and cyber attacks.

The computer-based risks to these infrastructures have increased during the 1990s due to their growing dependence on computers and the greater interconnectivity among computers. While no devastating instances of "cyber-terrorism" have occurred, computer-based incidents, such as the ILOVEYOU virus in May 2000, have caused significant disruptions and damage. In addition, the number of incidents reported has increased dramatically, as have the number of computer crime cases opened by the FBI and other law enforcement agencies. As a result, government officials are increasingly concerned about attacks from individuals and groups with malicious intentions.

In accordance with PDD 63 and other information security requirements outlined in laws and federal guidance, an array of efforts has been undertaken to address these risks. However, progress in certain key areas has been slow. For example, federal agencies have taken initial steps to develop critical infrastructure protection (CIP) plans. However, independent audits continue to identify persistent, significant information security weaknesses at virtually all major federal agencies that place their operations at high risk of tampering and disruption.[1] Outreach efforts by numerous federal entities to establish cooperative relationships with and among private and other non-federal entities have raised awareness and prompted information sharing, and the federal government and the private sector have initiated a variety of CIP research and development efforts. However, substantive analysis of interdependencies within and among industry sectors and related vulnerabilities has been limited.

[1] *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, (GAO/AIMD-00-295, Sept. 6, 2000).

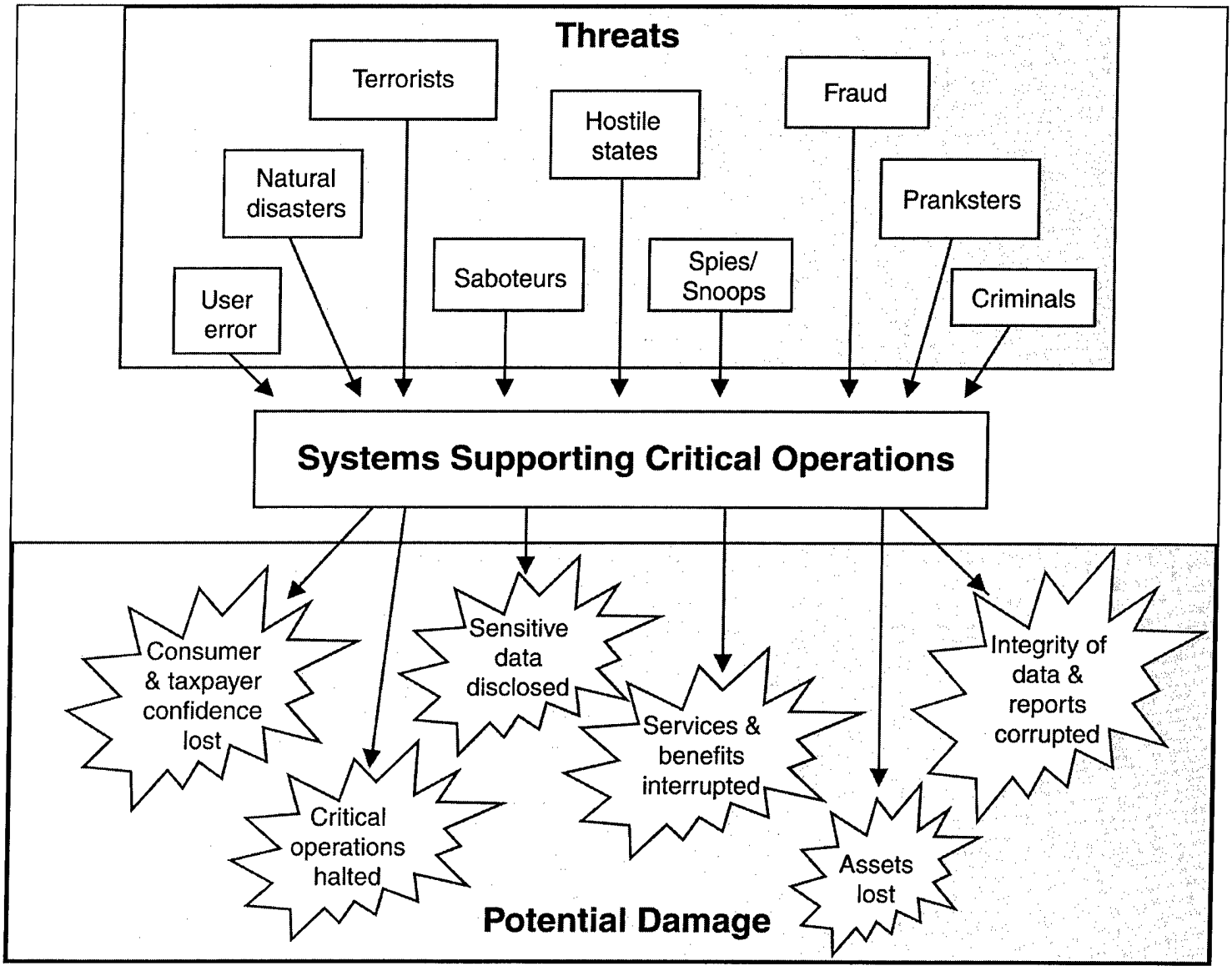
An underlying deficiency impeding progress is the lack of a national plan that fully defines the roles and responsibilities of key participants and establishes interim objectives.

Risks of Cyber-Attacks and Related Government Strategy

The risks associated with our nation's reliance on interconnected computer systems are substantial and varied. Attacks could severely disrupt computer-supported operations, compromise the confidentiality of sensitive information, and diminish the integrity of critical data. A significant concern is that terrorists or hostile foreign states could severely damage or disrupt critical operations resulting in harm to the public welfare. Threats are increasing, in part, because the number of individuals with computer skills is increasing and because intrusion, or "hacking," techniques have become readily accessible through magazines, computer bulletin boards, and Internet web sites. In addition, the Director of Central Intelligence has stated that some terrorists groups are acquiring rudimentary cyber-attack tools.[2] Further, according to the National Security Agency, foreign governments already have or are developing computer attack capabilities and potential adversaries are developing a body of knowledge about U.S. systems and methods to attack these systems. However, the sources of and motives behind cyber-attacks often cannot be readily determined. This is because groups or individuals can attack remotely from anywhere in the world, over the Internet, other networks, or dial-up lines, and they can disguise their identity, location, and intent by launching attacks across a span of communications systems and computers. As a result, efforts to combat such attacks must consider the entire range of threats, including criminals intent on fraud and disgruntled employees. Accordingly, efforts to protect critical infrastructures from devastating computer-based attacks by terrorist and hostile nation states are similar to and must be integrated with other federal computer security activities. Figure 12 provides an overview of the related risks.

[2]Prepared statements by George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, Feb. 7, 2001, and Feb. 2, 2000.

Figure 12: Risks to Computer-Based Operations



Source: GAO analysis.

While complete data are not available because many incidents are not reported, available data show that the number of attacks is increasing. The number of incidents reported to Carnegie-Mellon University's CERT

Coordination Center[3] has increased from about 1,300 in 1993 to about 9,800 in 1999 and to over 21,000 in 2000—figures that the Center estimates may represent only about 20 percent of the incidents that are actually occurring because most are not detected or reported. Similarly, the FBI reports that its caseload of computer intrusion-related investigations more than doubled from 1998 to 2000. Additionally, other federal law enforcement agencies have reported significant increases in the number of computer intrusion-related investigations. While PDD 63 covered both physical and computer-based threats, federal efforts to meet the directive's requirements have pertained primarily to computer-based threats, since this was an area that the leaders of the administration's critical infrastructure protection strategy viewed as needing attention.

Concerns about computer-based vulnerabilities have been publicly reported repeatedly during the 1990s. In 1991, the National Research Council studied the issue and reported that "as computer systems become more prevalent, sophisticated, embedded in physical processes and interconnected, society becomes more vulnerable to poor system design, accidents that disable systems, and attacks on computer systems."[4] In July 1996, the President's Commission on Critical Infrastructure Protection was established to investigate the nation's vulnerability to both cyber and physical threats. The Commission's October 1997 report, *Critical Foundations: Protecting America's Infrastructures*, described the potentially devastating implications of poor information security from a national perspective. Also, since 1996, congressional interest in protecting national infrastructures has remained strong and, since 1997—most recently in January 2001—GAO has designated information security as a governmentwide high-risk area, in reports to the Congress.[5]

[3]Originally called the Computer Emergency Response Team (CERT), the CERT Coordination Center was established in 1988 by the Defense Advanced Research Projects Agency. The center is charged with (1) establishing a capability to quickly and effectively coordinate communication among experts in order to limit the damage associated with, and respond to, incidents and (2) building awareness of security issues across the Internet community.

[4]*Computers at Risk: Safe Computing in the Information Age*, The National Research Council, 1991.

[5]*High-Risk Series: Information Management and Technology* (GAO/HR-97-9, Feb. 1, 1997); *High-Risk Series: An Update* (GAO/HR-99-1, Jan. 1999); and *High-Risks Series: An Update* (GAO-01-263, Jan. 2001).

In response to the Commission's 1997 report, the President issued PDD 63, which called for a range of activities to improve federal agency security programs, improve the nation's ability to detect and respond to serious attacks, and establish a partnership between the government and private sector. The directive called on the federal government to serve as a model of how infrastructure assurance is best achieved and designated "lead agencies" to work with private-sector and government entities in each of eight infrastructure sectors and five special function areas. PDD 63 further stated that the United States would have an initial operating capability by the year 2000 and, by 2003, have developed the ability to protect the nation's critical infrastructures from intentional destructive attacks.

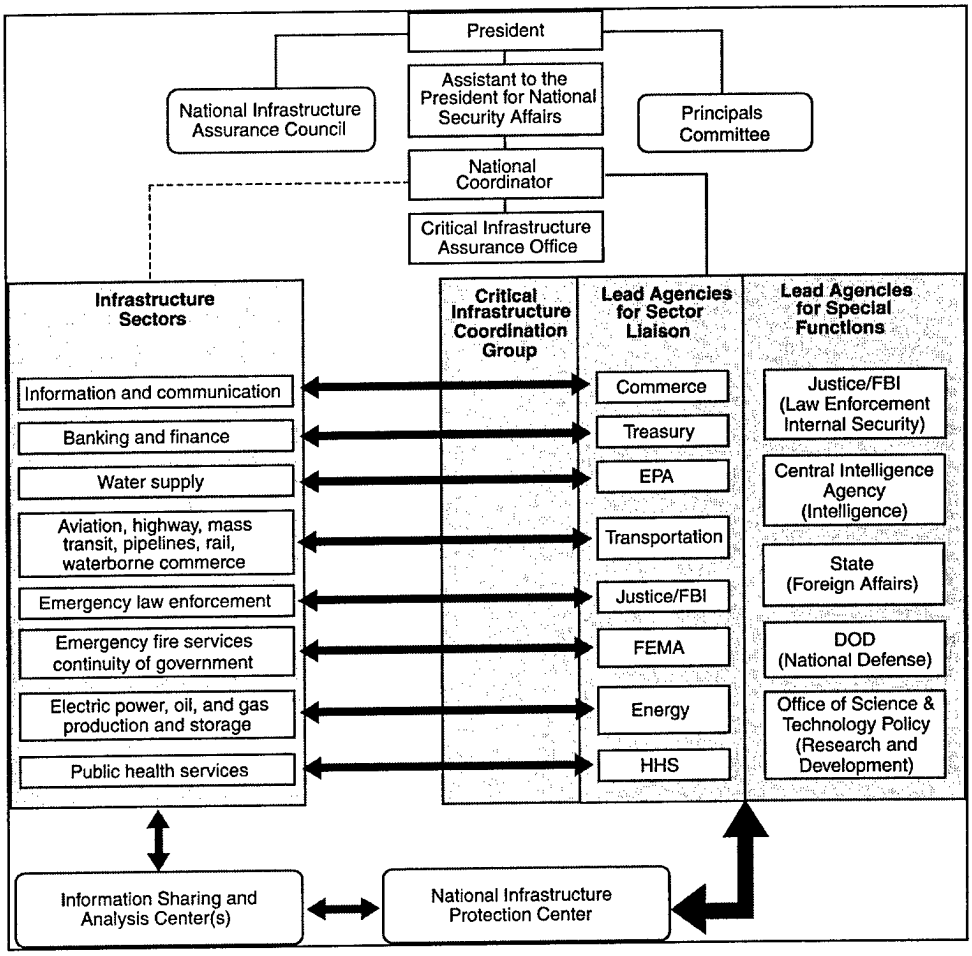
PDD 63 also designated and established entities to provide central coordination and support, including

- the National Coordinator for Security, Infrastructure Protection and Counterterrorism under the Assistant to the President for National Security Affairs, to oversee national policy development and implementation;
- a Critical Infrastructure Coordination Group, made up of senior level officials, to coordinate the implementation of PDD 63 with the National Coordinator;[6]
- the Critical Infrastructure Assurance Office (CIAO), housed in the Department of Commerce, to develop a national plan for critical infrastructure protection based upon infrastructure plans developed by the private sector and federal agencies; and
- the National Infrastructure Protection Center (NIPC) at the FBI as a national-level threat assessment, warning, vulnerability, and law enforcement investigation and response entity.

To facilitate private-sector participation, PDD 63 also encouraged creation of information sharing and analysis centers (ISAC) that could serve as mechanisms for gathering, analyzing, appropriately sanitizing, and disseminating information to and from infrastructure sectors and the NIPC. Figure 13 shows the responsibilities outlined in PDD 63.

[6]In February 2001, the Critical Infrastructure Coordination Group was replaced with the Information Infrastructure Protection and Assurance Group under the Policy Coordinating Committee on Counter-terrorism and National Preparedness.

Figure 13: CIP Responsibilities Outlined by PDD 63



Source: CIAO.

Despite Increased Efforts, Critical Federal Operations Remain at Risk

Federal entities have long been required to protect their computer systems and data. However, since 1998, a number of new activities have been initiated in response to the growing risks to critical operations and to respond to computer-based incidents. Key efforts include the following:

- The federal Chief Information Officers and the Chief Financial Officers Councils, under the auspices of OMB, have sponsored a number of activities, including security conferences, best practices initiatives, and distribution of model policies. Also, during 2000, the Chief Information Officers Council sponsored development of the Federal Information Technology Security Assessment Framework as a tool for measuring the

completeness and effectiveness of agencies' information security programs.

- The CIAO, as required in PDD 63, coordinated development of the *National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue*, which the White House released in January 2000. In addition, the CIAO has assisted federal agencies in identifying their critical assets and associated infrastructure interdependencies through a process referred to as Project Matrix. According to the *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities*, issued in January 2001, 14 federal departments and agencies had been asked to participate in Project Matrix.
- The Federal Computer Incident Response Center (FedCIRC), initially established by the National Institute of Standards and Technology in 1996 and, since 1998, operated by the General Services Administration, has coordinated the response to computer incidents of federal civilian agencies. In addition, it has provided civilian agencies technical information, tools, methods, and guidance; provided a mechanism for sharing information among agencies, law enforcement, the private sector and academia; and issued advisories.
- The Joint Task Force for Computer Network Defense was established in December 1998 by DOD as the primary agent to coordinate and direct the department's efforts to prevent and detect cyber attacks on DOD computers, contain damage, and restore computer functionality.[7] Its efforts include developing standard tactics, techniques, and procedures for responding to cyber incidents and sharing information on cyber threats and attacks.

Further, the Congress has continued to demonstrate its interest in improving the protection of federal operations through hearings and by enacting information security reform provisions as part of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 that supplement requirements outlined in the Paperwork Reduction Act of 1995 and the Computer Security Act of 1987 and that are consistent with National Institute of Standards and Technology and OMB guidance. These new provisions require agencies' information security programs to incorporate a cycle of risk management activities that

- assess risks and determine protection needs,

[7]In April 2001, the Joint Task Force for Computer Network Defense was renamed the Joint Task Force for Computer Network Operations.

- select and implement cost-effective policies and controls,
- promote awareness of risks, policies, and the need for controls, and
- implement a program of routine tests and examinations for evaluating the effectiveness of policies and related controls and report the results to those who can take appropriate corrective action.

The new provisions also require annual evaluations of agency information security programs by both management and agency inspectors general. The results of these reviews, which are initially scheduled to become available in late 2001, are expected to provide a more complete picture of the status of federal information security than currently exists, thereby providing the Congress and OMB an improved means of overseeing agency progress and identifying areas needing improvement.

In addition to these broad efforts, our recent audits have shown that individual agencies, including the EPA, the Internal Revenue Service, and VA, have taken significant actions to correct identified computer security weaknesses and improve their information security management programs. Further, according to the *President's Status Report*, the DOD has initiated efforts to bolster its encryption capabilities, advance its computer forensics capabilities by establishing a lab in September 1999, improve its ability to actively defend computer systems, focus attention on infrastructures critical to operations by designating lead components, and create better relationships between installation commanders and local and private sector leaders.

Despite the many improvements initiated, we reported in September 2000 and April 2001 that audits have continued to identify information security weaknesses in virtually every major federal agency.[8] These weaknesses place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. For example, weaknesses at the Department of the Treasury increased the risk of fraud and disruption associated with billions of dollars of federal payments and collections and weaknesses at DOD increase the vulnerability of various military operations. These weaknesses also place enormous amounts of confidential data, ranging from personal and tax data to proprietary business information, at risk of inappropriate disclosure.

[8](GAO/AIMD-00-295) and *Computer Security: Weaknesses Continue to Place Critical Federal Operations and Assets at Risk* (GAO-01-600T, Apr. 5, 2001).

In addition, a March 2001 report by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) identified significant deficiencies in agencies' implementation of PDD 63 based on reviews conducted by agency inspectors general.[9] For example, PDD 63 required federal departments and agencies to establish plans for protecting their own critical infrastructure that were to be implemented within 2 years, or by May 2000, and it required federal departments and agencies to develop procedures and conduct vulnerability assessments. However, the PCIE/ECIE report stated that

- many agency CIP plans were incomplete and some agencies had not developed CIP plans,
- most agencies had not completely identified their mission-essential infrastructure assets, and
- few agencies had completed vulnerability assessments of their minimum essential infrastructure assets or developed remediation plans.

The PCIE/ECIE report concluded that the federal government could improve its PDD 63 planning and assessment activities and questioned the federal government's ability to protect the nation's critical infrastructures from intentional destructive acts by May 2003, as required in PDD 63.

The results of our review of PDD 63-related activities at eight lead agencies were generally consistent with the PCIE/ECIE report's findings, although some agencies had made progress since their respective inspectors general reviews. For example, while five agencies had or were in the process of updating their plans based on inspector general reviews, other independent reviews, or more recent initiatives, three were not revising their plans to address reported deficiencies. In addition, while most of the agencies we reviewed had identified critical assets, many had not completed vulnerability assessments on all of their critical assets. For example, one agency had not performed vulnerability assessments on 4 of 13 of its critical assets. Another department had not supplemented its vulnerability assessment procedures to include CIP aspects, such as determining a system's significance to national security. Further, most of

[9]The PCIE primarily is comprised of the presidentially-appointed inspectors general and the ECIE is primarily comprised of the agency head-appointed inspectors general. In November 1999, PCIE and ECIE formed a working group to review the adequacy of federal agencies' implementation of PDD 63. The March 2001 report is based on reviews by 21 inspectors general of their respective agencies' PDD 63 planning and assessment activities.

the eight agencies we reviewed had not taken the additional steps to identify interdependencies and, as a result, some agency officials said that they were not sure which of their assets were critical from a national perspective and, therefore, subject to PDD 63. According to a report by the CIP Research and Development Interagency Working Group, the effect of interdependencies is that a disruption in one infrastructure can spread and cause appreciable impact on other infrastructures.[10] The report also stated that understanding interdependencies is important because the proliferation of information technology has made the infrastructures more interconnected and the advent of competition, "just in time" business, and mergers among infrastructure owners and operators have eroded spare infrastructure capacity.

We identified several factors that had impeded federal agency efforts to comply with PDD 63. First, no clear definitions have been developed to guide development and implementation of agency plans and measure performance. For example, PDD 63 established December 2000 as the deadline for achieving an initial operating capability and May 2003 for achieving full operational capability of key functions. However, the specific capabilities to be achieved at each milestone had not been defined. The PCIE/ECIE report noted that agencies had used various interpretations of initial operating capability and stated that, without a definition, there is no consistent measure of progress toward achieving full security preparedness.

Several agency officials said that funding and staffing constraints contributed to their delays in implementing PDD 63 requirements. According to one chief information officer, this may be because senior officials do not fully understand the importance of their agency's assets to the nation's critical infrastructures and the magnitude of the related risks. In addition, the availability of adequate technical expertise to provide information security has been a continuing concern to agencies. Further, though we specifically have not analyzed the technical skills of agency personnel involved in computer security across government, we have observed a number of instances where agency staff did not have the skills needed to carry out their computer security responsibilities and were not adequately overseeing activities conducted by contractors. Recognizing

[10]*Report on the Federal Agenda in Critical Infrastructure Protection Research and Development, Research Vision, Objectives, and Programs*, CIP Research and Development Interagency Working Group, Jan. 2001.

the need to improve the government's ability to attract and retain workers and expand training and education opportunities, the Chief Information Officers Council established a Federal Information Technology Workforce Committee to focus on this issue. In addition, in November 2000, the Office of Personnel Management established higher pay for information technology workers to give agencies flexibility in addressing recruitment and retention problems affecting the government's information technology workforce. These new pay rates became effective in January 2001.

Finally, since 1996, we have reported that poor security program management is an underlying cause of federal information security weaknesses and this has diminished agencies' ability to ensure that controls are appropriate and effective.[11] Specifically, many agencies have not developed security plans for major systems based on risk, documented security policies, and implemented a program for testing and evaluating the effectiveness of the controls they relied on. As a result, agencies

- were not fully aware of the information security risks to their operations,
- had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable,
- had a false sense of security because they were relying on controls that were not effective, and
- could not make informed judgments as to whether they were spending too little or too much of their resources on security.

For example, audits by us and DOD's Inspector General have reported that an underlying cause of weak information security at DOD is poor security management. The Department has taken steps to improve its information security—notably, establishing the Defense-wide Information Assurance Program under the jurisdiction of the Chief Information Officer and, as mentioned earlier, the Joint Task Force for Computer Network Defense. However, in March 2001, we reported that a number of challenges faced by both programs, including departmentwide planning, data collection and

[11] *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110, Sept. 24, 1996); *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, Sept. 23, 1998); and (GAO/AIMD-00-295).

integration, vulnerability assessment procedures, and performance management, have limited their progress.[12]

CIP Activities Have Raised Awareness and Prompted Information Sharing; However, Substantive Analysis of Infrastructure Vulnerabilities Has Been Limited

As required by PDD 63, federal entities have taken steps to foster cooperative relationships between the federal government and non-federal sectors. For example, in December 1999, the CIAO helped establish the Partnership for Critical Infrastructure Security as a forum of private-sector member companies for raising awareness and understanding of cross-industry critical infrastructure issues and as a catalyst for action among the owners and operators of the critical infrastructures. As of March 2001, the Partnership had 51 members from various infrastructure sectors. It also had created working groups to address interdependency vulnerability assessment; information sharing, awareness, and education; legislation and public policy objectives; research and development and workforce development; and organization issues/public private cooperation. Further, the CIAO has worked with the audit community to produce and distribute a guide for corporate boards on managing information security risks and coordinated or sponsored a series of conferences to raise awareness—including conferences for the legal community to advance the understanding of legal issues associated with information security.

The NIPC, which is responsible for analysis, warning, and response related to cyber incidents, also had made some progress in this area. Specifically, in April 2001,[13] we reported that the NIPC had worked to build information-sharing relationships with the private sector through the adoption and expansion of the InfraGard Program, which started in 1996, to provide a secure mechanism for two-way information sharing about intrusion, incidents, and system vulnerabilities. By early January 2001, 518 entities were InfraGard members—up from 277 members in October 2000. Members included representatives from private industry, other government agencies, state and local law enforcement, and the academic community. The NIPC also had established computer crime squads and teams in the FBI's 56 field offices across the country to support the investigation of the growing number of crimes involving attacks on

[12] *Information Security: Challenges to Improving DOD's Incident Response Capabilities* (GAO-01-341, Mar. 29, 2001) and *Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program* (GAO-01-307, Mar. 30, 2001).

[13] *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities* (GAO-01-323, Apr. 25, 2001).

computers. In addition, as of December 2000, one interagency task force had been created to coordinate investigative work and facilitate information sharing regarding computer crime with other law enforcement entities.

We also reported that the NIPC had (1) issued assessments, advisories, and alerts to warn the public about identified vulnerabilities, attacks underway, and potential attacks and (2) standardized its procedures for implementing crisis action teams and developed a detailed concept of operations to guide the federal government's response to computer-based attacks. However, the report stated that most of the NIPC's activities had been focused on tactical analysis related to individual cyber incidents or notices of recently reported vulnerabilities and that strategic analysis to determine the broader implications of individual incidents had been limited. We noted that the NIPC faced a number of impediments to developing more substantive analytical capabilities, including a lack of a methodology for strategic analysis, a lack of needed staff and expertise, and inadequate data on infrastructure vulnerabilities. We also identified barriers to issuing early warnings, including (1) a lack of a comprehensive governmentwide or nationwide framework for promptly obtaining and analyzing information on imminent attacks, (2) shortage of skilled staff, (3) the need to ensure that the NIPC does not raise undue alarm for insignificant incidents, and (4) the need to ensure that sensitive information is protected. Finally, we reported that the NIPC's plans for developing its analytical and warning capabilities were fragmented and incomplete.

To assist in establishing relationships with major infrastructure owners and operators, PDD 63 required lead agencies to assign a high-ranking official, as an agency sector liaison, to lead efforts in cooperation with the sector owners and operators in addressing problems related to critical infrastructure protection and, in particular, in recommending components of a national infrastructure assurance plan. Similarly, the directive required the agency sector liaison officials, after discussions and coordination with entities of their infrastructure sector, to identify infrastructure sector coordinators to represent their sector. In addition, PDD 63 outlined tasks that the lead agencies were to encourage and assist the infrastructure sectors in accomplishing, including developing vulnerability education and outreach programs, establishing ISACs, performing vulnerability assessments of the sectors, and developing related remediation plans.

As of March 2001, progress in meeting some of these requirements was well underway. Each of the eight lead agencies we reviewed had designated sector liaisons, and seven of the eight major infrastructure sectors had identified one or more individuals or groups as sector coordinators for their respective infrastructure sector. Infrastructure sector coordinators had not been selected for the public health services sector because, according to officials at the Department of Health and Human Services, the infrastructure owners and operators had not been fully identified due to the large and diverse communities involved. Also, according to relevant agency and private sector officials and the *President's Status Report*, most infrastructure sectors had planned or held education and outreach events, such as workshops, conferences, and industry meetings to address broad CIP needs and specific concerns. Further, six ISACs within five infrastructures had been established to gather and share information about vulnerabilities, attempted intrusions, and attacks within their respective infrastructures and to meet specific sector objectives. Three of these ISACs—for the telecommunications and electric power industries and emergency fire services segment—were based on groups that had existed previously. The three other ISACs—for the financial services, information technology, and emergency law enforcement sectors—had been established since October 1999. In addition, at the time of our audit, the formation of at least three more ISACs for various infrastructure segments was being discussed.

However, beyond building partnerships, raising awareness, and improving information sharing, substantive, comprehensive analysis of infrastructure sector vulnerabilities and development of related remedial plans had been limited. While some assessments had been performed for individual sector components, these did not necessarily consider the interdependencies within and among the infrastructures. For example, within the banking and finance sector, most large institutions individually had undergone vulnerability assessments. However, a vulnerability assessment of the most important banking and finance institutions as a group to identify interdependencies and events that could cause a system failure across the infrastructure had not occurred. Such sector-wide assessments had not yet been performed because sector coordinators were still establishing the necessary relationships, identifying critical assets and critical entities, and researching and identifying appropriate methodologies. In addition, some federal officials stated that their agencies did not have the resources to assist in the completion of sector vulnerability assessments. In addition, the emergency fire services sector liaison officials told us that a sector-wide vulnerability assessment would be impractical due to the thousands

of local organizations that would have to participate and the lack of national associations or government organizations of fire departments.

Table 7 shows the status of key CIP efforts in the eight infrastructure sectors as of March 2001.

Table 7: Status of Key CIP Efforts in Eight Infrastructure Sectors

Infrastructure sector	Sector liaisons and sector coordinators designated	Vulnerability assessments and remedial plans developed	Education and awareness programs implemented	Information sharing and analysis centers established
Banking and finance	Yes	• Some assessments performed • No remedial plans • Assessment methodology being researched	• Some efforts • Sector developing a program	• ISAC formally established in October 1999
Electric power, oil and gas	Yes	• Some assessments for electric and gas • No remedial plans	• Some efforts	• Electric industry ISAC only • None for oil and gas
Emergency fire services segment	Yes	• Some assessments performed • No remedial plans	• Some training for states and localities	• United States Fire Academy designated March 1, 2001
Emergency law enforcement	Yes	• No assessments • Methodology being researched • No remedial plans	• Some meetings to discuss legal issues • "Cybercitizen Partnership" to raise ethics issues with children	• NIPC designated to act as the sector ISAC in December 2000
Information and communication	Yes	• Methodology developed • No assessments yet performed • Department of Commerce coordinating with industry and DOD to perform regional communications assessments • No remedial plans	• Some meetings on CIP issues held	• Information Technology ISAC established January 2001 • Telecommunication ISAC function recognized in January 2000
Public health services	Liaison only	• No assessment • No remedial plans • Some discussions held about performing assessments	• Some meetings on CIP issues held	No
Transportation segments	• Liaison • Coordinator for rail and aviation only	• No sector assessments • DOT performed a surface transportation assessment • No remedial plans	• Some efforts	No
Water supply	Yes	• One assessment performed • Methodology being further tested • No remedial plans	• Some efforts	No

Factors cited by the private sector as impeding progress in building the necessary government/private-sector partnerships and identifying and addressing vulnerabilities included the following:

- Concerns have been raised that organizations potentially could face antitrust violations for sharing information with other industry partners, subject their information to Freedom of Information Act disclosures, or face potential liability concerns for information shared in good faith.
- An inadvertent release of confidential business information, such as trade secrets or proprietary information, could damage reputations, lower consumer confidence, hurt competitiveness, and decrease market shares of firms. Further, the private sector may have reservations about sharing information with law enforcement agencies because compliance with law enforcement procedures can be costly.
- Some senior executives are not fully aware of the importance of their assets to the national and economic security of the nation.
- Due to the complexity and breadth of some infrastructures, organizations and entities that could coordinate CIP efforts across the infrastructure do not exist.

In addition, PDD 63 called for a plan to expand international cooperation on critical infrastructure protection and designated the Department of State as the lead agency in this area. According to Department of State officials and the *President's Status Report on CIP*, an international strategy is being implemented that coordinates CIP outreach to other governments and international intergovernmental organizations and promotes CIP awareness, vigilance in security standards and practices, and law enforcement cooperation. As part of this strategy, the Department of State had organized meetings with key allies to discuss common issues related to infrastructure protection. Also, according to agency officials, in early 2001, the Department of State developed a United Nations Resolution on cyber-crime, which passed unanimously in the United Nations General Assembly and, as of March 2001, was developing follow-up actions. In addition, Department of Justice officials were negotiating a Council of Europe convention intended to facilitate international law enforcement issues related to computer crime and, as of March 2001, this treaty still was being negotiated. The Department of Justice also chairs the G-8 High Tech Crime Subgroup that is focused on enhancing law enforcement's abilities to prevent, investigate, and prosecute high-tech crime.[14] Further,

[14]Eight major industrialized countries comprise the G-8, which includes Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States.

Department of Commerce officials had participated in meetings with representatives from other countries to discuss and negotiate CIP issues, including the Council of Europe treaty.

Many Research and Development Efforts Are Underway

The *National Plan* recognized that a vigorous and effective program for CIP research and development should seek to enhance security by rapidly identifying, developing, and facilitating the fielding of technological solutions to existing and emerging infrastructure threats and vulnerabilities. According to PDD 63, OSTP is responsible for coordinating research and development efforts through the National Science and Technology Council. In January 2001, the CIP Research and Development Interagency Working Group, tasked by the National Science and Technology Council's Committee on National Science and Technology and the Critical Infrastructure Coordination Group, identified eight priority research and development areas:

- establishment of an Institute for Information Infrastructure Protection;
- education and training of research personnel;
- interdependency analyses;
- threat, vulnerability, and risk assessment studies;
- system protection and information assurance;
- reconstitution of damaged or compromised systems;
- security of automated infrastructure control systems; and
- intrusion detection and monitoring.

Assessing the extent to which these priorities are being addressed was not within the scope of our review. However, we identified a variety of research and development efforts that were either being planned or performed by federal entities and, in some cases, were being sponsored by the infrastructure sectors. These included the following:

- The National Institute of Standards and Technology has established the CIP Grants Program to fund research to provide commercial solutions to information technology security problems central to critical infrastructure protection that are not being adequately addressed. According to Department of Commerce officials, this initial funding is inadequate to address the scope and breadth of CIP research challenges.
- As part of a Department of Energy proposal to conduct nine complementary, interrelated CIP research and development programs encompassing analysis and risk management and protection and mitigation, work is underway to (1) develop energy infrastructure interdependencies analysis methodologies and tools and (2) develop and

leverage databases, methodologies, and tools to evaluate consequences of disruptions and processes for restoration.

- The Department of Transportation has ongoing projects to analyze the vulnerabilities of the Global Positioning System and identify cyber-security gaps in transportation information systems. In addition, the Department, under the National Science and Technology Council, has formulated a transportation infrastructure assurance research and development plan with the goal of developing a comprehensive approach to assessing threats to the nation's transportation system and preparing projects that provide solutions to these threats. The plan addresses security of vital communications, navigation, and information systems and networks.
- The Carnegie-Mellon CERT Coordination Center has ongoing research and development efforts pertaining to development of a risk assessment methodology—"OCTAVE" (Operationally Critical Threat, Asset, and Vulnerability Evaluation).
- The Banking and Finance Sector's Research and Development Working Group is undertaking projects to (1) model the infrastructure sector to identify vulnerabilities and (2) develop forensic tools needed by law enforcement in combating electronic crimes and attacks.
- The TSWG, an interagency group to coordinate and conduct research and development projects for combating terrorism, has funded efforts to examine vulnerabilities associated with specific types of attacks and determining the precise locations of critical assets.
- The Defense Advanced Research Projects Agency has supported efforts focusing on the security of the Internet and anomaly and misuse detection.
- The Department of State has sponsored international activities to coordinate CIP-related research and development with other nations, including (1) holding bilateral negotiations and meetings aimed at identifying, developing, and facilitating CIP solutions; (2) sponsoring with the European Union workshops to exchange information on cyber-security research; and (3) establishing dialogue on telecommunications-related issues.

According to the CIP Research and Development Interagency Working Group, one area that has received almost no attention is identifying the interdependencies and cascading effects among infrastructures. The working group's January 2001 report stated that, to address this deficiency, the government, the national laboratories, academia, and private industry were working to build understanding and tools to address interdependencies, including efforts to build test facilities and to learn

about secure operations of complex interactive networks and about various aspects of damage caused by earthquakes.[15]

National Plan Is Not Fully Developed; Responsibilities Still Are Evolving

In addition to the impediments previously identified, an underlying deficiency in the implementation of the strategy outlined in PDD 63 is the lack of a national plan that clearly delineates the roles and responsibilities of federal and non-federal entities and defines interim objectives. We first identified the need for a detailed plan in September 1998, when we reported that developing a governmentwide strategy that clearly defined and coordinated the roles of new and existing federal entities was important to ensure governmentwide cooperation and support for PDD 63.[16] At that time, we recommended that OMB and the Assistant to the President for National Security Affairs ensure such coordination.

PDD 63 required, within 180 days, a schedule for the completion of a national infrastructure assurance plan with milestones for accomplishing a number of tasks that included

- developing vulnerability assessments and related remedial plans,
- establishing a national center to warn of significant events,
- creating a system for responding to significant infrastructure attacks,
- developing an education and awareness program, and
- establishing a research and development program.

In January 2000, the President issued *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. The plan proposed achieving the twin goals of making the U.S. government a model of information security and developing a public-private partnership to defend our national infrastructures by achieving three crosscutting infrastructure protection objectives:

- minimize the possibility of significant and successful attacks;
- identify, assess, contain, and quickly recover from an attack; and
- create and build strong foundations, including people, organizations, and laws, for preparing, preventing, detecting and responding to attacks.

[15]CIP Research and Development Interagency Working Group Report, January 2001.

[16]*Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, Sept. 23, 1998).

However, this plan focused largely on federal CIP efforts, saying little about the private-sector role.

A more complete plan is needed because, although some progress has been made in implementing PDD 63, questions have surfaced regarding specific roles and responsibilities and the time frames within which objectives are to be met. For example, the PCIE/ECIE reported that several agencies had decided not to implement PDD 63 requirements because they believed that they were exempt from the directive. As a result, these agencies had not prepared CIP plans, identified critical assets, performed related vulnerability assessments, or developed remediation plans. However, according to the CIAO, PDD 63 requirements apply to all departments and agencies. Also, in a recent review of the NIPC, we found that various officials involved in critical infrastructure protection did not consistently interpret the NIPC's role. Several expressed an opinion that this lack of consensus had hindered the NIPC's progress and diminished support from other federal agencies. In addition, without clearly defined interim objectives and milestones, the success of efforts to improve federal and non-federal critical infrastructure protection cannot be measured. The PCIE/ECIE report noted that, as of March 2001, agencies still needed guidance for measuring their progress in identifying critical assets, performing vulnerability assessments, and developing and implementing remedial plans.

The new administration has been reviewing and considering adjustments to the government's CIP strategy that may address these deficiencies. In a May 2001 White House press statement, it was announced that the administration was reviewing how it is organized to deal with information security issues and that recommendations would be made on how to structure an integrated approach to cyber-security and critical infrastructure protection. Specifically, the announcement stated that the White House, federal agencies, and private industry had begun to collaboratively prepare a new version of the National Plan that would be completed later this year.

Conclusions

An array of efforts has been undertaken to address risks to the critical infrastructures and implement PDD 63 requirements. Many of these efforts have built on longstanding efforts to strengthen federal information security. However, substantive analysis and related remedial actions to protect critical infrastructures have been very limited. In addition, a national strategy has not been fully developed for accomplishing CIP goals and integrating CIP activities with the established framework of federal

information security laws and organizational responsibilities. Developing such a strategy and gaining both public and private sector support is important to ensuring that our nation has the capability to deal with the growing threat of computer-based attacks on our nation's critical infrastructures. Meeting the challenges of accomplishing these efforts will not be easy and will require clear central direction and dedication of expertise and resources from multiple federal agencies.

Recommendations for Executive Action

We have made scores of recommendations in reports to individual executive agencies regarding weaknesses in their individual computer security practices, and most agencies have corrective actions underway. Accordingly, we are making no additional recommendations to the agencies at this time. In addition, in our recent report regarding the progress of the NIPC, we made recommendations to the Attorney General and the Assistant to the President for National Security Affairs regarding the need to define more fully the role and responsibilities of the NIPC, develop plans for establishing analysis and warning capabilities, and improve information-sharing relationships between the private-sector and federal entities.

To supplement our previous recommendations, we further recommend that the Assistant to the President for National Security Affairs ensure that the federal government's CIP strategy, which is currently under review, define

- specific roles and responsibilities of organizations involved in critical infrastructure protection and related information security activities;
- interim objectives and milestones for achieving CIP goals and a specific action plan for achieving these objectives, including implementation of vulnerability assessments and related remedial plans; and
- performance measures for which entities can be held accountable.

We believe the federal government's cyber-security strategy should be linked to the national strategy to combat terrorism as discussed in chapter 3. However, the two areas are different in that the threats to computer-based infrastructures are broader than terrorism and programs to protect them are more closely associated with traditional information security activities.

Agency Comments and Our Evaluation

Agency comments on a draft of this report were based on their efforts prior to the September 11, 2001, terrorist attacks. In commenting on a draft of this report, none of the agencies addressed our recommendation. However, the agencies did provide us with comments on their concerns regarding the protection of the nation's critical computer-dependent infrastructures from computer-based attacks.

DOE highlighted two points in the area of critical infrastructure protection. First, DOE stated that while computer-based attacks are real and viable threats, and in some cases may be interpreted as terrorism, they cannot be labeled as such in many instances. Second, DOE raised the concern that we should not allow the highly visible cyber issues to overshadow the threat of possible physical attacks against other infrastructure elements, particularly energy, transportation, and water supply systems. In addition, DOE stated that further focus and resources need to be applied to better understand the threat and how best to protect, mitigate, respond, and recover from attacks against our critical infrastructures. DOE also made separate technical comments, which have been incorporated in the report, as appropriate.

The Department of Justice stated that establishing a central authority within the Executive Branch for formulating policy regarding computer-based attacks on critical infrastructure facilities may help coordinate efforts underway in agencies across the federal government. However, the Department added that careful consideration should be given to how such central authority would be administered, noting that data gathered under criminal and intelligence authorities often is carefully prescribed and that court-sanctioned criminal and intelligence techniques are subject to different legal requirements. The Department made no technical comments related to chapter 6.

HHS provided specific comments on its public health service critical infrastructure sector efforts. In particular, HHS stated that it was researching a vulnerability assessment methodology, had held some education and awareness meetings, was working jointly with the CIAO to develop an education and awareness program, and was developing a virtual ISAC. We made these changes in the report, as appropriate.

The Department of Commerce stated that the administration is reviewing the organizational structures for counter-terrorism and CIP to provide leadership and ensure effective coordination of federal government efforts. In addition, the Department said that the administration is committed to developing a new National Plan for Critical Infrastructure

Protection. The Department also provided technical comments, which have been incorporated in the report, as appropriate.
The Departments of the Treasury and Transportation also provided technical comments on the draft of this report. We made these changes in the report, as appropriate.

Despite the lack of agency comments on our recommendation, we still believe that it has merit and will supplement our previous recommendations.

Appendix I: Compendium of Relevant Federal Policy and Planning Documents

Appendix I describes, in chronological order, selected federal interagency policy and planning documents related to combating terrorism that form the foundation for the federal government's efforts to combat terrorism and protect the nation's critical infrastructure against attack. These documents delineate federal agencies' roles and responsibilities for responding to potential or actual terrorist threats or incidents as well as the processes and mechanisms by which the federal government mobilizes and deploys resources and coordinates assistance to state and local authorities.

National Contingency Plan (National Oil and Hazardous Substances Pollution Contingency Plan)

This August 1973 plan provides the organizational structure and procedures for preparing for and responding to discharges of oil and releases of hazardous substances, pollutants, and contaminants. The plan lists the general responsibilities of federal agencies regarding such incidents, identifies the fundamental kinds of activities that are performed pursuant to the plan, and describes the specific responsibilities of the National Response Team, the Regional Response Teams, the National Response Center, and the U.S. Coast Guard's National Strike Force Teams for planning and responding to such incidents.

Federal agencies may conduct consequence management activities in a terrorist incident under the National Oil and Hazardous Substances Pollution Contingency Plan because it provides authority and funding sources to respond to hazardous materials incidents regardless of the suspected cause. For example, a terrorist act may at first appear to be a routine hazardous materials incident, leading to the activation of a federal response under this plan. If the Federal Response Plan is activated, the response actions of the National Contingency Plan are conducted as one of the Federal Response Plan's emergency support functions.

The National Contingency Plan is authorized under section 105 of the Comprehensive Environmental Response, Compensation and Liability Act of 1980, 42 U.S.C. 9605, and 40 Code of Federal Regulations Part 300.

Executive Order 12656: Assignment of Emergency Preparedness Responsibilities

This November 1988 Executive Order assigns specific responsibilities during national security emergencies to federal departments and agencies based on extensions of their regular missions. The order also designates the National Security Council (NSC) as the principal forum for consideration of national security emergency preparedness policy, and instructs the Director of the Federal Emergency Management Agency (FEMA) to advise the NSC on issues of national security emergency preparedness, including mobilizing preparedness, civil defense, continuity

of government, technological disasters, and other issues. It also directs the FEMA Director to assist in the implementation of national security emergency preparedness policy by coordinating with other federal departments and agencies and with state and local governments.

Federal Response Plan and Terrorism Incident Annex

The April 1992 Federal Response Plan, as amended, lays out the manner in which the federal government, with FEMA coordinating the support/assistance efforts of other agencies, responds to domestic incidents or situations in which the President has declared an emergency requiring federal emergency disaster assistance. More specifically, the plan outlines the planning assumptions, policies, concept of operation, organizational structures, and specific assignment of responsibilities to lead departments and agencies in providing federal assistance. The plan also categorizes the types of federal assistance into specific emergency support functions, such as transportation, communications, fire fighting, and health and medical services.

The Terrorism Incident Annex establishes a general concept of operations for the federal response to a terrorist incident, including the concurrent operation under other plans such as the National Oil and Hazardous Substances Pollution Contingency Plan and the Federal Radiological Emergency Response Plan.

The Federal Response Plan is authorized under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5121 et seq., and 44 Code of Federal Regulations Subchapters D (Disaster Assistance) and F (Preparedness).

Presidential Decision Directive 39

This June 1995 directive sets forth U.S. general policy to use all appropriate means to deter, defeat, and respond to all terrorist attacks against U.S. interests. More specifically, Presidential Decision Directive (PDD) 39 directs federal departments and agencies to take various measures to (1) reduce vulnerabilities to terrorism (e.g., to assess the vulnerabilities of government facilities and critical national infrastructure); (2) deter and respond to terrorism (e.g., to pursue, arrest, and prosecute terrorists and to minimize damage and loss of life and provide emergency assistance); and (3) develop effective capabilities to prevent and manage the consequences of terrorist use of weapons of mass destruction.

Federal Radiological Emergency Response Plan

This May 1996 plan establishes an organizational and operational structure for coordinated responses by federal agencies to peacetime radiological emergencies, taking into consideration the specific statutory authorities and responsibilities of each agency. The plan provides guidance as to which agency will lead and coordinate the federal response to a radiological emergency (i.e., the lead federal agency). According to the guidance, the specific agency depends on the type of emergency involved. For example, the Nuclear Regulatory Commission is the lead agency for an emergency that occurs at a nuclear facility or any activity licensed by the Commission. The plan also identifies the specific roles and responsibilities of each federal lead agency, such as responding to requests from state and local governments for technical information and assistance.

This plan may be used whenever any of the signatory agencies respond to a radiological emergency, which would include terrorist acts to spread radioactivity in the environment. The Federal Response Plan may be implemented concurrently with the Federal Radiological Emergency Response Plan. The functions and responsibilities of the Federal Radiological Emergency Response Plan do not change, except for the coordination that occurs between the lead federal agency and the Federal Coordinating Officer (usually a FEMA official).

Presidential Decision Directive 62

This May 1998 directive attempts to increase the federal government's effectiveness in countering terrorism threats against U.S. targets. PDD 62 organizes and clarifies the roles and activities of many agencies responsible for combating a wide range of terrorism, including preventing terrorist acts, apprehending and prosecuting terrorists, increasing transportation security and protecting critical computer-based systems. This directive also provides for consequence management of terrorist incidents.

To carry out the integrated program, PDD 62 establishes the Office of the National Coordinator for Security, Infrastructure Protection and Counterterrorism. Working with the NSC, the National Coordinator is responsible for overseeing the wide range of policies and programs covered by PDD 62 and is to take the lead in developing guidelines that might be needed for crisis management.

Presidential Decision Directive 63

This May 1998 directive acknowledges computer security as a national security risk and established several entities within the NSC, the Department of Commerce, and the Federal Bureau of Investigation (FBI) to address critical infrastructure protection, including federal agencies' information infrastructures. PDD 63 tasks federal agencies with developing critical infrastructure protection (CIP) plans and establishing related links with private industry sectors. It called for the development of a national plan for critical infrastructure protection.

Attorney General's Five-Year Interagency Counterterrorism and Technology Crime Plan

The December 1998 classified Attorney General's Five-Year Plan and its annual updates are intended to provide a baseline strategy for coordination of national policy and operational capabilities to combat terrorism in the United States and against American interests overseas. The plan identifies several high-level goals aimed at preventing and deterring terrorism, facilitating international cooperation to combat terrorism, improving domestic crisis and consequence planning and management, improving state and local capabilities, safeguarding information infrastructure, and leading research and development efforts to enhance counterterrorism capabilities. It also identifies the specific tasks federal agencies perform when responding to terrorist incidents and sets forth current and projected efforts by the Attorney General in partnership with other federal agencies; the National Coordinator for Security, Infrastructure Protection and Counterterrorism; and state and local entities to improve readiness to address the threat of terrorism.

National Plan for Information Systems Protection

The January 2000 National Plan for Information Systems Protection provides a vision and framework for the federal government to prevent, detect, respond to, and protect the nation's critical cyber-based infrastructure from attack and reduce existing vulnerabilities by complementing and focusing existing Federal Computer Security and Information Technology requirements. Subsequent versions of the plan will (1) define the roles of industry and state and local governments working in partnership with the federal government to protect privately owned physical and cyber-based infrastructures from deliberate attack and (2) examine the international aspects of critical infrastructure protection.

The National Plan for Information Systems Protection is authorized by PDD 63, which calls for the development of a national plan for information system protection to prioritize CIP goals, principles, and long-term planning efforts.

Domestic Guidelines

The November 2000 Domestic Guidelines (Guidelines for the Mobilization, Deployment, and Employment of U.S. Government Agencies in Response to Domestic Terrorist Threat or Incidence in Accordance With Presidential Decision Directive 39) provide a road map for government agencies' mobilization, deployment, and use under PDD 39 in response to a terrorist threat or incident. The Domestic Guidelines describe specific procedures and responsibilities for deploying the Domestic Emergency Support Team, particularly in weapons of mass destruction (WMD) incidents, and facilitate interagency coordination in support of the lead federal agency's mission to combat terrorism in the United States.

CONPLAN

The January 2001 CONPLAN (U.S. Government Interagency Domestic Terrorism Concept of Operations Plan) provides overall guidance to federal, state, and local agencies concerning how the federal government would respond to a potential or actual terrorist threat or incident that occurs in the United States, particularly one involving weapons of mass destruction. The CONPLAN outlines an organized and unified capability for a timely, coordinated response by federal agencies—specifically, the Department of Justice, the FBI, Department of Defense, Department of Energy, FEMA, Environmental Protection Agency (EPA), and Department of Health and Human Services—to a terrorist threat or act. It establishes conceptual guidelines for assessing and monitoring a developing threat, notifying appropriate agencies concerning the nature of the threat, and deploying necessary advisory and technical resources to assist the lead federal agency in facilitating interdepartmental coordination of crisis and consequence management activities.

International Guidelines

The January 2001 International Guidelines (Coordinating Subgroup Guidelines for the Mobilization, Deployment, and Employment of U.S. Government Elements in Response to an Overseas Terrorist Incident) outline procedures for deploying the Foreign Emergency Support Team and otherwise coordinating federal operations overseas.

National Security Presidential Directive-1 (NSPD-1)

This February 2001 directive communicates presidential decisions concerning the national security policies of the United States. It also reiterates the role of the NSC system as the process to coordinate executive departments and agencies in the effective development and implementation of those national security policies. The directive designates the NSC Principals Committee as the senior interagency forum for consideration of policy issues affecting national security and tasks the

NSC Policy Coordination Committees with the management of the development and implementation of national security policies by multiple U.S. agencies. It also establishes the Policy Coordination Committees and defines their roles and responsibilities.

Appendix II: Individual Agency Plans and Guidance for Combating Terrorism

Appendix II describes, in chronological order, selected individual agency plans and guidance for combating terrorism that either have been completed recently or are being drafted. These documents clarify agencies' roles and procedures for responding to terrorist attacks; provide guidance for the allocation of resources for planning, exercising, and implementing agency plans and programs; and delineate agency strategies for addressing terrorism.

Department of Defense

DOD Directive 3025.15 Military Assistance to Civil Authorities

This unclassified directive issued on February 18, 1997, establishes DOD policy and assigns responsibility for providing military assistance to civil authorities. The employment of U.S. military forces in response to acts or threats of domestic terrorism is contingent upon authorization by the President as well as approval by the Secretary of Defense. The directive does not address non-federalized National Guard assets in support of local and/or state civil agencies approved by the governor.

Improving Local and State Agency Response to Terrorist Incidents Involving Biological Weapons. Interim Planning Guide

The guide includes a Biological Warfare Response Template that addresses both crisis and consequence management within five scenarios. States may use the template to formulate an integrated approach to biological weapons emergency responses. The Biological Weapons Improved Program was initiated in 1998 and the final draft of the planning guide was issued on August 1, 2000. The guide was developed as the result of the Defense Against Weapons of Mass Destruction Act of 1996 (P.L. 104-201, Sept. 23, 1996), which required the Secretary of Defense to develop and implement a program to improve the responses of federal, state, and local agencies to emergencies involving biological and chemical weapons. DOD developed the Biological Warfare Improved Response Program and coordinated the associated planning guide with the Department of Health and Human Services (HHS), Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigation (FBI), Environmental Protection Agency (EPA), the Department of Energy (DOE), and the Department of Agriculture.

Management of DOD Operational Response to Consequences of Certain Incidents Involving Chemical, Biological, Radiological, Nuclear, and High Yield Explosives

The August 10, 2000, memorandum states that some chemical, biological, radiological, nuclear, and high-yield explosive incidents may have qualitative and quantitative differences from routine incidents. Thus, all official requests for DOD support for chemical, biological, radiological, nuclear, and high-yield explosive incidents are routed through the Executive Secretary of the Department of Defense, who determines if the incident warrants special operational management. For incidents not requiring special operations, the Secretary of the Army will serve as the Executive Agent through the Director of Military Support channels.

Contingency Plans

DOD has several contingency plans to address its potential crisis and consequence management support roles in both domestic and international situations. Some of these are classified.

Department of Energy

Design Basis Threat for the Department of Energy Programs and Facilities

The April 1999 document, Design Basis Threat for the Department of Energy Programs and Facilities, identifies and characterizes potential adversary threats to DOE's programs and facilities that could adversely affect national security, the health and safety of employees, the public, or the environment. The document specifically addresses the protection of DOE facilities in the United States against terrorist attacks and is coordinated with DOD and the Nuclear Regulatory Commission as well as with the intelligence community and the FBI. It serves as the foundation for DOE's defensive policies and requirements, including facility protection strategies and countermeasures.

Department of Health and Human Services

Department of Health and Human Services Health and Medical Services Support Plan for the Federal Response to Acts of Chemical/Biological (C/B) Terrorism	The June 1996 plan provides a coordinated federal response for urgent public health and medical care needs resulting from chemical and/or biological terrorist threats or acts within the United States. The plan supports the FBI and FEMA by leading the Emergency Support Function No. 8 response to the health and medical aspects of a chemical or biological terrorist incident. It also supplements and assists affected state and local governments by providing resources from (1) HHS and its supporting federal agencies and departments and (2) non-federal sources, such as major pharmaceutical suppliers and international disaster response organizations like the Canadian Ministry of Health. The plan is an appendix to Emergency Support Function No. 8 of the Federal Response Plan. Portions of the plan may be implemented under HHS authorities prior to formal implementation of the Federal Response Plan.
Bioterrorism Readiness Plan: A Template for Healthcare Facilities	The April 1999 plan serves as a tool for infection control professionals and healthcare epidemiologists to guide the development of response plans for their institutions in preparation for a real or suspected bioterrorism attack and encourages institution-specific response plans to be prepared in partnership with local and state health departments. The plan is updated as needed to reflect public health guidelines and new information.
Preparedness and Response to Biological and Chemical Terrorism: A Strategic Plan	The unpublished April 2000 report outlines steps for strengthening public health and health care capacity to protect the United States against chemical and biological terrorism in cooperation with law enforcement, intelligence, and defense agencies in addition to the Centers for Disease Control and Prevention (CDC).
Centers for Disease Control and Prevention Smallpox Outbreak Response Plan and Guidelines	The June 2000 draft manual outlines criteria for implementation of the smallpox response plan and CDC vaccine and personnel mobilization activities. The draft manual assists state and local health officials with specific activities essential for the management of a smallpox emergency.

Fiscal Years 2002 and 2006 Plan for Combating Bioterrorism	The January 2001 departmental 5-year plan builds on HHS' strategic plan to include budget projections for the agencies and offices involved in achieving the department's goals for (1) prevention of bioterrorism; (2) infectious disease surveillance; (3) medical and public health readiness for mass casualty events; (4) the national pharmaceutical stockpile; (5) research and development; and (6) secure and continuously operating information technology infrastructure.
The Public Health Response to Terrorism: Planning Guidance for State Public Health Officials, Centers for Disease Control and Prevention.	This February 2001 draft-planning guidance is designed to help state public health officials determine their role in terrorism response and understand the emergency response roles of local health departments and emergency management communities. It also may be used to help coordinate efforts among state health departments and agencies and organizations at all levels of government that would respond to a WMD terrorist event.
U.S. Department of Health and Human Services Counterterrorism Concept of Operations Plan	The draft plan describes how HHS will provide coordinated federal assistance for public health and medical care needs resulting from terrorist threats or acts using weapons of mass destruction within the United States or its territories and possessions. The plan encompasses both crisis and consequence management responsibilities; describes the essential features for a systematic, coordinated and effective national health and medical response; and defines procedures for the use of Department resources to augment and support state and local governments.

Department of Justice/FBI

National Special Security Events Operations Manual	The December 1999 manual serves as a planning resource for special events held within the United States. It provides an overview of the issues FBI personnel consider when planning and coordinating support for special events and identifies the roles and functions of other federal agencies that often support special events.

Blueprint for the National Domestic Preparedness Office	The December 1999 blueprint discusses the role of the National Domestic Preparedness Office as a single coordinating office and information clearinghouse for federal assistance programs to prepare state and local officials to respond to WMD acts of terrorism within the United States.
Weapons of Mass Destruction Incident Contingency Plan	The plan provides guidance to the FBI On-Scene Commander to effectively respond to a WMD threat or incident. The plan highlights the FBI's policy for crisis management of WMD terrorist events and delineates specific responsibilities of FBI components during a WMD incident. The plan sets out procedures and resources available to support the FBI's investigative and crisis management responsibilities.

Department of Transportation/U.S. Coast Guard

Interim Guidance Regarding Coast Guard Response to Weapons of Mass Destruction (WMD) Incidents	This June 2000 interim document provides guidance to the U.S. Coast Guard concerning participation in WMD incidents and planning while recognizing resource and training shortfalls. It also provides guidance concerning command and control and operating procedures.
U.S. Coast Guard Marine Safety and Environmental Protection Business Plan, FY 2001-2005	The August 2000 plan provides a national framework for current and future U.S. Coast Guard program operations and strategies for attaining the Marine Safety and Environmental Protection Program's mission to protect the public, the environment, and U.S. economic interests through the prevention and mitigation of maritime accidents. The plan aims to reduce the vulnerability of the marine transportation system to intentional harm from terrorist acts. It also directs the U.S. Coast Guard to achieve a specific readiness level in interdiction and consequence management responsibilities concerning the use or threat of use of weapons of mass destruction. The Marine Transportation System Report submitted to the Congress in September 1999 and the President's Commission on Seaport Crime and Security, along with the Oceans Report to the President, "Turning to the Sea: America's Ocean Future," provide the blueprint for the U.S. Coast Guard to obtain these objectives as part of their responsibility for port security.

U.S. Coast Guard Contingency Preparedness Program Guidance

The December 2000 document provides guidance for the allocation of resources for planning, exercising, and executing the U.S. Coast Guard's contingency preparedness program that includes, but is not limited to, terrorist incidents. The guidance seeks to encourage standardization and consistency in the U.S. Coast Guard's contingency preparedness efforts and to help focus limited resources toward high-risk contingencies. It directs the U.S. Coast Guard to update outdated plans; strengthen ties with federal, state, and local governments, and industry to improve coordination during responses; develop a 5-year national exercise schedule to anticipate planning and resource requirements; and record all exercise after-action reports and lessons learned in a centralized U.S. Coast Guard database.

Environmental Protection Agency

Environmental Protection Agency Radiological Emergency Response Plan

The January 2000 plan supercedes the 1986 version and represents EPA's current programmatic and operational concepts for responding to radiological incidents and emergencies. It is used as a guide for planning and maintaining readiness to respond to those releases in accordance with EPA's mission to protect the environment and support the Federal Radiological Emergency Response Plan and National Oil and Hazardous Substances Pollution Contingency Plan. The plan covers both EPA's role as a lead federal agency for response coordination under the Federal Radiological Emergency Response Plan and its role as a lead agency for directing and managing an emergency response pursuant to the National Oil and Hazardous Substances Pollution Contingency Plan.

EPA Regional Counter-Terrorism Program Reference Manual including Annexes for EPA's Counterterrorism Planning, Preparedness, and Response Strategy

The March 2000 manual serves as a resource for EPA regional and headquarters personnel to use during domestic terrorism-related planning or response activities. Although the manual is not agency policy, EPA updates it periodically. It provides background information on the response framework and other agencies' responsibilities and presents details pertaining to the specific roles and responsibilities of EPA response personnel during a terrorist threat or incident.

Several annexes provide an overview of EPA's strategy for addressing counterterrorism, including the EPA organizations involved in developing and implementing its counterterrorism strategy to protect public health and the environment from the threat or adverse effects of nuclear,

biological, and/or chemical substances released during terrorist incidents. The annexes also discuss funding for regional counterterrorism activities, supporting legal authorities, and interagency counterterrorism workgroups.

Federal Emergency Management Agency

Strategic Plan Fiscal Year 1998 through Fiscal Year 2007 With Operational Objectives through Fiscal Year 2003

FEMA's September 1997 Strategic Plan presents three strategic goals that support the agency's mission to reduce the loss of life and property and protect U.S. institutions from all hazards by leading and supporting the nation in a comprehensive, risk-based emergency management program of mitigation, preparedness, response, and recovery. Several of the goals address FEMA's role as the lead agency for consequence management in a terrorist incident and describe related activities.

FEMA Terrorism Preparedness Strategic Plan

The June 2000 Terrorism Preparedness Strategic Plan outlines the mission, vision, and goals of FEMA's Terrorism Preparedness Program and supports FEMA's Strategic Plan by clarifying agency goals and objectives related to terrorism. The Terrorism Preparedness Strategic Plan presents several goals related to mitigation and preparedness. It emphasizes providing guidance on FEMA's roles and responsibilities in terrorism related activities; supporting federal, state, and local consequence management planning, training, and exercise programs; improving coordination and sharing of information at all levels of government; establishing an organizational structure for coordinating terrorism preparedness within FEMA; and developing systems to monitor and track resources needed to support FEMA's terrorism consequence management programs and activities.

FEMA Implementation Plan

The August 2000 plan clarifies roles and responsibilities in the implementation of FEMA-wide programs and activities in terrorism preparedness and supports FEMA's June 2000 Terrorism Preparedness Strategic Plan and overall FEMA Strategic Plan. Under this plan, the Senior Advisor for Terrorism Preparedness provides overall direction, coordination, and oversight for the implementation of FEMA's terrorism-related programs and activities. It also sets forth the roles and responsibilities of each of FEMA's directorates that support terrorism-related consequence management activities.

Attachment G: Terrorism Supplement to the State and Local Guide 101 for All-Hazard Emergency Operations Planning

In April 2001, FEMA issued Attachment G to the State and Local Guide 101 for All-Hazard Emergency Operations Planning under the authority of the Robert T. Stafford Disaster Relief Act and the Emergency Assistance Act, as amended. Issued in September 1996, the State and Local Guide 101 provides emergency managers with information on FEMA's concept for developing risk-based, all-hazard emergency operations plans. The voluntary guide provides a "toolbox" of ideas and advice for state and local authorities and clarifies the preparedness, response, and short-term recovery planning elements that warrant inclusion in state and local emergency operations plans.

Attachment G to the State and Local Guide 101 aids state and local emergency planners in developing and maintaining a Terrorist Incident Appendix to their Emergency Operations Plan for incidents involving terrorist-initiated weapons of mass destruction.

Appendix III: Selected Federal Crisis Management Response Teams

Appendix III lists selected federal crisis management response teams by agency. It describes their mission and number of personnel that could be deployed. If state and local first responders are unable to manage a weapons of mass destruction terrorist incident or become overwhelmed, the incident commander can request these and other federal assets.

Agency/Team	Mission	Number of personnel
Department of Defense		
U.S. Army 52nd Ordnance Group (Explosive Ordnance Disposal)	Trained on chemical and nuclear weapons of mass destruction and on specialized equipment for diagnostics and render-safe/mitigation of a nuclear device.	Three Explosive Ordnance Disposal companies located in San Diego, CA; San Antonio, TX; and Andrews AFB, Washington, D.C.
U.S. Army Technical Escort Unit	Provides field sampling, monitoring, recovery, decontamination, transportation, and verification of weaponized and non-weaponized chemical and biological materials.	Approximately 150 military and civilian personnel at Aberdeen Proving Grounds, MD; Pine Bluff Arsenal, AR; and Dugway Proving Grounds, UT.
Joint Special Operations Task Force	Determined based upon circumstances.	Determined based upon circumstances.
Federal Bureau of Investigation		
Critical Incident Response Group (includes Hostage Rescue Team, Crisis Negotiation, Crisis Management, and Behavioral Assessment)	Facilitates rapid response to and management of crisis incidents. Provides on-scene commander with rapid response/support in crisis incidents, including crisis negotiations, command post, behavioral assessment, and crisis information management.	Approximately 230, including the Hostage Rescue Team.
Hostage Rescue Team	Deploys to any location within 4 hours and conducts a successful rescue operation of persons held by a criminal or terrorist force.	Authorized about 90 personnel at the FBI Academy at Quantico, VA.
Special Weapons and Tactics (SWAT) Teams	Plan and execute high-risk tactical operations that exceed the capabilities of field office investigative resources. Provide management support of SWAT operations.	Over 1,000 trained personnel in 56 field offices, with nine enhanced SWAT teams.
Hazardous Materials Response Unit	Responds safely and effectively to incidents involving hazardous materials and develops the FBI's technical proficiency and readiness for crime scene and evidence-related operations in cases involving chemical, biological, and radiological materials.	Headquarters unit plus 17 smaller and less capable units through the United States.
Department of Energy		
Nuclear Emergency Search Team	Provides specialized technical expertise in resolving nuclear or radiological terrorist incidents. Searches for lost or stolen nuclear material, weapons, or devices.	Varies in size from a five-person technical advisory team to a tailored deployment of dozens. Basic team consists of seven persons.

Agency/Team	Mission	Number of personnel
Nuclear/Radiological Advisory Team	Provides technical advice, emergency response, and follow-on expertise to the On-Scene Commander.	Eight-person team.
Lincoln Gold Augmentation Team	Provides expert technical advice to deployable U.S. military Explosive Ordnance Disposal operators concerning diagnostics, render-safe procedures, weapons analysis, and device modeling and effects prediction.	Five-person team.
Joint Technical Operations Team	Provides advanced technical capabilities to move or neutralize nuclear weapons.	Thirty one-person team composed of 21 DOE and 10 DOD personnel, all of whom have other primary duties.
Department of Health and Human Services		
Domestic Emergency Support Team component	Provides technical assistance as needed.	The size and composition of each team is determined by the type and location of the event or threat.
National Medical Response Team/WMD	Each team provides an operational response capability, including a pharmaceutical cache for treating up to 5,000 people for chemical weapons exposure.	The size and composition of each team is determined by the type and location of the event or threat.
Bureau of Alcohol, Tobacco, and Firearms		
National Response Team	Assists federal, state, and local investigators in meeting the challenges faced at the scenes of significant arson and explosives incidents.	Four teams organized geographically to cover the United States.
Environmental Protection Agency		
Radiological Emergency Response Team	Conducts environmental monitoring, performs laboratory analyses, and provides advice and guidance on measures to protect the public.	As many as 60 personnel with these collateral duties are located in Las Vegas, NV, and Montgomery, AL.

Source: GAO analysis and discussions with agency officials.

Appendix IV: Selected Federal Consequence Management Response Teams

Appendix IV lists selected federal consequence management response teams by agency. It describes their mission and number of personnel that could be deployed. If state and local first responders are unable to manage a weapons of mass destruction terrorist incident or become overwhelmed, the incident commander can request these and other federal assets.

Response team	Mission	Number of team (dedicated/collateral) members and team's primary location
Department of Defense		
Joint Task Force for Civil Support	Supports lead federal agency, establishes command and control of designated Department of Defense (DOD) forces, and provides military assistance to civil authorities to save lives, prevent human suffering, and provide temporary critical life support.	Sixty dedicated personnel located at Fort Monroe, VA.
Chemical/Biological Rapid Response Team	Coordinates and integrates DOD's technical assistance for the neutralization, containment, dismantlement, and disposal of chemical or biological materials. Assists first responders in dealing with consequence management.	Fourteen dedicated personnel located at Aberdeen Proving Grounds, MD.
U.S. Army Technical Escort Unit	Provides chemical/biological advice, assessment, sampling, detection, field verification, packaging, escort, and render-safe for chemical/biological devices or hazards.	Approximately 190 personnel located at Aberdeen Proving Grounds, MD; Fort Belvoir, VA; Pine Bluff, AR; and Dugway, UT.
U.S. Army Special Medical Augmentation Response Team—Nuclear/Biological/Chemical	Provides technical advice in the detection, neutralization, and containment of chemical, biological, or radiological hazardous materials in a terrorist event.	Six teams located at various sites with six members per team who have these collateral duties.
U.S. Army Special Medical Augmentation Response Team—Aero-Medical Isolation	Provides a rapid response evacuation unit to any area of the world to transport and provide patient care under conditions of biological containment to service members or U. S. civilians exposed to certain contagious and highly dangerous diseases.	Approximately 20 personnel who have this collateral duty are stationed at Fort Detrick, MD.
U.S. Marine Corps Chemical-Biological Incident Response Force	Provides force protection or mitigation in the event of a terrorist incident, domestically or overseas.	Three hundred seventy-three dedicated personnel at Indian Head, MD.
U.S. Army Radiological Advisory Medical Team	Assists and furnishes radiological health hazard guidance to the on-scene commander or other responsible officials at an incident site and the installation medical authority.	Eight to 10 personnel who have these collateral duties are located at Walter Reed Army Hospital, Washington, D.C.
Department of Health and Human Services		
Management Support Teams	Manage federal medical teams and assets that are deployed in response to an incident.	Six to eight dedicated personnel located at Rockville, MD, supplemented by 18 to 20 Department of Veterans Affairs personnel who have these collateral duties.

Response team	Mission	Number of team (dedicated/collateral) members and team's primary location
National Medical Response Teams	Decontaminate casualties resulting from a hazardous materials incident, provide medical care, and deploy with pharmaceutical cache of antidotes and medical equipment.	Four teams located at Washington, D.C. (non-deployable); Winston-Salem, NC; Denver, CO; and Los Angeles, CA, with 36 members per team who have these collateral duties.
Disaster Medical Assistance Teams	Provide emergency medical care during a disaster or other event.	Forty-four teams at various locations nationwide with 34 members per team who have these collateral duties.
Disaster Mortuary Operational Response Teams	Provide identification and mortuary services to state and local health officials upon request in the event of major disasters and emergencies.	Ten teams at various locations nationwide with 25 to 31 members per team who have these collateral duties.
National Pharmaceutical Stockpile	Resupplies state and local public health agencies with pharmaceuticals and other medical supplies in the event of a terrorist incident.	Six rapid response inventories are located at five of six permanent sites.
Department of Energy		
Radiological Assistance Program Teams	Assist federal agencies, state and local governments, private business, or individuals in incidents involving radiological materials.	Twenty-six teams at various locations nationwide with seven members per team who have these collateral duties.
Federal Radiological Monitoring and Assessment Center[a]	Collects, evaluates, interprets, and distributes off-site radiological data in support of the lead federal agency, state, and local governments. Coordinates federal resources in responding to the off-site monitoring and assessment needs at the scene of a radiological emergency.	Team members deploy in phases. Phases I (15 members) and II (45 members) consist of Department of Energy personnel with these collateral duties from Nellis Air Force Base, NV, and other locations. Phase III (known as Full Federal Radiological Monitoring and Assessment Center) involves multiple federal agencies and may have 150 or more personnel from various federal agencies.
Aerial Measuring System	Detects, measures, and tracks ground and airborne radioactivity over large areas using fixed-wing and rotary-wing aircraft.	Five to 10 dedicated and collateral duty personnel located at Nellis Air Force Base, NV, and Andrews Air Force Base, MD.
Radiation Emergency Assistance Center/Training Site	Provides medical advice and on-site assistance in triage, diagnosis, and treatment of all types of radiation exposure events.	Four to eight dedicated personnel located in Oak Ridge, TN.
Department of Transportation		
U.S. Coast Guard National Strike Teams	Respond to oil and hazardous substance pollution incidents in and around waterways to protect public health and the environment. Area of responsibility includes all Coast Guard Districts and Federal Response Regions. Support Environmental Protection Agency's On-Scene Coordinators for inland area incidents.	Three teams located in Fort Dix, NJ; Mobile, AL; and Novato, CA, with 35 to 39 dedicated members per team.

Response team	Mission	Number of team (dedicated/collateral) members and team's primary location
U.S. Coast Guard On-Scene Coordinators	Coordinate all containment, removal and disposal efforts, and resources during a hazardous release incident in coastal or major navigational waterways.	Approximately 50 dedicated personnel in pre-designated Coast Guard regional zones at various locations nationwide.
Department of Veterans Affairs		
Medical Emergency Radiological Response Team	Provides technical advice, radiological monitoring, decontamination expertise, and medical care as a supplement to an institutional health care provider.	Twenty-one to 23 personnel with these collateral duties are located at various sites nationwide.
Environmental Protection Agency		
On-Scene Coordinators	Direct response efforts and coordinates all other efforts at the scene of a hazardous materials discharge or release.	Approximately 200 dedicated personnel, plus contractor support, at various locations nationwide.
Environmental Response Team	Provides technical support for assessing, managing, and disposing of hazardous waste.	Twenty-two dedicated personnel, plus contractor support, located in Edison, NJ, and Cincinnati, OH.
Radiological Emergency Response Team	Provides mobile laboratories for field analysis of samples and technical expertise in radiation monitoring, radiation health physics, and risk assessment.	As many as 60 personnel with these collateral duties are located in Las Vegas, NV, and Montgomery, AL.
Federal Emergency Management Agency		
Emergency Response Team	Coordinates federal response and recovery activities within a state.	Size is dependent on the severity and magnitude of the incident. Team members with these collateral duties are geographically dispersed at Federal Emergency Management Agency headquarters and 10 regional offices.
Nuclear Regulatory Commission		
Regional Incident Response Teams	Carry out the responsibilities and functions of the lead federal agency during incidents at licensed facilities, such as nuclear power plants.	Four teams located in Atlanta, GA; Lisle, IL; Arlington, TX; and King of Prussia, PA, with 25-30 members per team who have these collateral duties.

[a]The Department of Energy has the lead responsibility for coordinating the Federal Radiological Monitoring Assessment Center during the early phase of an emergency. The Environmental Protection Agency assumes control during later phases.

Source: GAO analysis and discussions with agency officials.

Appendix V: Compendium of Relevant GAO Recommendations

Appendix V provides a compendium of selected GAO recommendations for combating domestic terrorism made over the last 5 years. This appendix also provides the current status of GAO's prior recommendations.

Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination (GAO/NSIAD-98-39, Dec. 1, 1997). Recommendations, p. 13.

GAO recommendations	Status of recommendations
We recommend that consistent with the responsibility for coordinating efforts to combat terrorism, Assistant to the President for National Security Affairs, the National Security Council (NSC), in consultation with the Director, Office of Management and Budget (OMB), and the heads of other executive branch agencies, take steps to ensure that (1) governmentwide priorities to implement the national counterterrorism policy and strategy are established; (2) agencies' programs, projects, activities, and requirements for combating terrorism are analyzed in relation to established governmentwide priorities; and (3) resources are allocated based on the established priorities and assessments of the threat and risk of terrorist attack.	Recommendation partially implemented. (1) The Attorney General's Five-Year Counter-Terrorism and Technology Crime Plan, issued in December 1998, included priority actions for combating terrorism. According to the NSC and OMB, the Five-Year Plan, in combination with Presidential Decision Directives (PDD) 39 and 62, represent governmentwide priorities that they use in developing budgets to combat terrorism. (2) According to the NSC and OMB, they analyze agencies' programs, projects, activities, and requirements using the Five-Year Plan and related presidential decision directives. (3) According to the NSC and OMB, they allocate agency resources based upon the priorities established above. However, there is no clear link between resources and threats. No national threat and risk assessment has been completed to use for resource decisions.
To ensure that federal expenditures for terrorism-related activities are well-coordinated and focused on efficiently meeting the goals of U.S. policy under PDD 39, we recommend that the Director, OMB, use data on funds budgeted and spent by executive departments and agencies to evaluate and coordinate projects and recommend resource allocation annually on a crosscutting basis to ensure that governmentwide priorities for combating terrorism are met and programs are based on analytically sound threat and risk assessments and avoid unnecessary duplication.	Recommendation partially implemented. OMB now is tracking agency budgets and spending to combat terrorism. According to the NSC and OMB, they have a process in place to analyze these budgets and allocate resources based upon established priorities. However, there is no clear link between resources and threats. No national threat and risk assessment has been completed to use for resource decisions.

Combating Terrorism: Opportunities to Improve Domestic Preparedness Program Focus and Efficiency (GAO/NSIAD-99-3, Nov. 12, 1998). Recommendations, p. 22.

GAO recommendations	Status of recommendations
The Secretary of Defense—or the head of any subsequent lead agency—in consultation with the other five cooperating agencies in the Domestic Preparedness Program, refocus the program to more efficiently and economically deliver training to local communities.	Recommendation implemented. The Department of Defense (DOD) transferred the Domestic Preparedness Program to the Department of Justice on October 1, 2000. The Department of Justice has implemented this recommendation by emphasizing the program's train-the-trainer approach and concentrating resources on training metropolitan trainers in recipient jurisdictions.
The Secretary of Defense, or the head of any subsequent lead agency, use existing state and local emergency management response systems or arrangements to select locations and training structures to deliver courses and consider the geographical proximity of program cities.	Recommendation implemented. DOD transferred the Domestic Preparedness Program to the Department of Justice on October 1, 2000. The Department of Justice has implemented this recommendation by modifying the programs in metropolitan areas and requiring cities to include their mutual aid partners in all training and exercise activities.
The National Coordinator for Security, Infrastructure Protection and Counterterrorism actively review and guide the growing number of weapons of mass destruction (WMD) consequence management training and equipment programs and response elements to ensure that agencies' separate efforts leverage existing state and local emergency management systems and are coordinated, unduplicated, and focused toward achieving a clearly defined end state.	Recommendation partially implemented. The NSC established an interagency working group called the Interagency Working Group on Assistance to State and Local Authorities. One function of this working group is to review and guide the growing number of WMD consequence management training and equipment programs. However, as described in our current report, we believe that more needs to be done to ensure that federal efforts are coordinated, unduplicated, and focused toward achieving a clearly defined end state—a results-oriented outcome as intended for government programs by the Results Act. We make a related recommendation in this current report to consolidate assistance programs.

Combating Terrorism: Issues to Be Resolved to Improve Counterterrorist Operations (GAO/C-NSIAD-99-3, February 26, 1999). Recommendations, pp. 38, 39, and 65.

GAO recommendations	Status of recommendations
The Attorney General direct the Director, FBI, to coordinate the Domestic Guidelines and CONPLAN with all federal agencies with counterterrorism roles and finalize them. Further, the Domestic Guidelines and/or CONPLAN should seek to clarify federal, state, and local roles, missions, and responsibilities at the incident site.	Recommendation implemented. The Domestic Guidelines were issued in November 2000. The CONPLAN was coordinated with key federal agencies and was issued in January 2001.
The Secretary of Defense review command and control structures and make changes, as appropriate, to ensure there is unity of command to DOD units participating in domestic counterterrorist operations to include both crisis response and consequence response management and cases in which they might be concurrent.	Recommendation implemented. In May 2001, the Secretary of Defense assigned responsibility for providing civilian oversight of all DOD activities to combat terrorism and domestic WMD (including both crisis and consequence management) to the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict.
The Secretary of Defense require the services produce after-action reports (AAR) or similar evaluations for all counterterrorism field exercises that they participate in. When appropriate, these AARs or evaluations should include a discussion of interagency issues and be disseminated to relevant internal and external organizations.	Recommendation partially implemented. The Joint After Action Reports database contains lessons learned. These reports address interagency issues, where appropriate. Many DOD units produce AARs and many of them address interagency issues. However, DOD officials acknowledged that service units or commands do not always produce AARs and/or disseminate them internally and externally as appropriate. We make a similar recommendation to DOD and other agencies in this current report.

Combating Terrorism: Use of National Guard Response Teams Is Unclear (GAO/NSIAD-99-110, May 21, 1999). Recommendations, p. 20.

GAO recommendations	Status of recommendations
The National Coordinator for Security, Infrastructure Protection and Counterterrorism, in consultation with the Attorney General, the Director, FEMA, and the Secretary of Defense, reassess the need for the Rapid Assessment and Initial Detection teams in light of the numerous local, state, and federal organizations that can provide similar functions and submit the results of the reassessment to the Congress. If the teams are needed, we recommend that the National Coordinator direct a test of the Rapid Assessment and Initial Deployment team concept in the initial 10 states to determine how the teams can best fit into coordinated state and federal response plans and whether the teams can effectively perform their functions. If the teams are not needed, we further recommend that they be inactivated.	Recommendation partially implemented. With authorization from the Congress, DOD established additional National Guard teams and changed their names from Rapid Assessment and Initial Detection teams to WMD Civil Support Teams. However, subsequent to our report and a report by the DOD Inspector General, which found some similar problems, DOD has agreed to review the National Guard teams and work with other agencies to clarify their roles in responding to terrorist incidents. We make a similar recommendation in this current report.

Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attack (GAO/NSIAD-99-163, Sept. 7, 1999). Recommendations, p. 22.

GAO recommendations	Status of recommendations
The Attorney General direct the FBI Director to prepare a formal, authoritative intelligence threat assessment that specifically assesses the chemical and biological agents that would more likely be used by a domestic-origin terrorist—non-state actors working outside a state run laboratory infrastructure.	Recommendation partially implemented. The Federal Bureau of Investigation (FBI) agreed with our recommendation. The FBI, working with the National Institute of Justice and the Technical Support Working Group, has produced a draft threat assessment of the chemical and biological agents that would more likely be used by terrorists. Along these lines, we make a similar recommendation in this current report. The Department of Justice anticipated that a draft of the assessment would be available for interagency review and comment in September 2001 and the final assessment would be published in December 2001.
The Attorney General direct the FBI Director to sponsor a national-level risk assessment that uses national intelligence estimates and inputs from the intelligence community and others to help form the basis for, and prioritize, programs developed to combat terrorism. Because threats are dynamic, the Director should determine when the completed national-level risk assessment should be updated.	Recommendation partially implemented. According to the Department of Justice, the FBI is in the process of conducting such an assessment. The report will assess the current threat, the projected threat, emerging threats, and related FBI initiatives. Along these lines, we make a similar recommendation in this current report. The Department stated that this assessment is being finalized and anticipated that the classified report would be published in October 2001.

Combating Terrorism: Chemical and Biological Medical Supplies are Poorly Managed (GAO/HEHS/AIMD-00-36, Oct. 29, 1999). Recommendations, p. 10.

GAO recommendations	Status of recommendations
The Department of Health and Human Services' (HHS) Office of Emergency Preparedness (OEP) and Centers for Disease Control and Prevention (CDC), the Department of Veterans Affairs (VA), and U.S. Marine Corps Chemical-Biological Incident Response Force (CBIRF) establish sufficient systems of internal control over chemical and biological pharmaceutical and medical supplies by (1) conducting risk assessments, (2) arranging for periodic, independent inventories of stockpiles, (3) implementing a tracking system that retains complete documentation for all supplies ordered, received, and destroyed, and (4) rotating stock properly.	Recommendation partially implemented. All of the agencies have made significant progress toward implementing our recommendations. They have conducted risk assessments, completed periodic physical inventories of the stockpiles, and developed and implemented procedures for stock rotation. Each of the agencies is taking steps to replace their current tracking systems with ones that are capable of tracking pharmaceutical and medical supplies from the time an order is placed until the item is consumed or otherwise disposed of.

Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training (GAO/NSIAD-00-64, Mar. 21, 2000). Recommendations, p. 25.

GAO recommendations	Status of recommendations
The Secretary of Defense and the Attorney General eliminate duplicative training to the same metropolitan areas. If the Department of Justice extends the Domestic Preparedness Program to more than the currently planned 120 cities, it should integrate the program with the Metropolitan Firefighters Program to capitalize on the strengths of each program and eliminate duplication and overlap.	Recommendation partially implemented. DOD transferred the Domestic Preparedness Program to the Department of Justice on October 1, 2000. The Department of Justice, is attempting to better integrate the assistance programs under its management. We make a similar recommendation in this current report to further consolidate these programs.

Combating Terrorism: Federal Response Teams Provide Varied Capabilities; Opportunities Remain to Improve Coordination (GAO-01-14, Nov. 30, 2000). Recommendations, p. 27.

GAO recommendations	Status of recommendations
To guide resource investments for combating terrorism, we recommend that the Attorney General modify the Attorney General's Five-Year Interagency Counterterrorism and Technology Crime Plan to cite desired outcomes that could be used to develop budget requirements for agencies and their respective response teams. This process should be coordinated as an interagency effort.	Recommendation not implemented. The Department of Justice asserts that the current plan includes desired outcomes. As discussed in this report, we disagree with the Department and believe what it cites as outcomes are outputs—agency activities rather than results the federal government is trying to achieve. In this current report, we repeat this recommendation to the Attorney General. We also recommend that the President establish a single focal point for overall leadership and coordination to combat terrorism. If such a focal point is established, then we believe that the focal point, and not the Attorney General, should be responsible for developing a national strategy.
The Director, Federal Emergency Management Agency, take steps to require that the Weapons of Mass Destruction Interagency Steering Group develop realistic scenarios involving chemical, biological, radiological, and nuclear agents and weapons with experts in the scientific and intelligence communities.	FEMA said it will take steps to ensure that the Weapons of Mass Destruction Interagency Steering Group works with relevant scientific and intelligence communities in developing WMD scenarios.
The Director, Federal Emergency Management Agency, sponsor periodic national-level consequence management field exercises involving federal, state, and local governments. Such exercises should be conducted together with national-level crisis management field exercises.	FEMA stated it would support and sponsor periodic national consequence management field exercises to ensure better coordination among federal and state and local response teams. Along these lines, we make a similar recommendation in this current report.

Combating Terrorism: Accountability Over Medical Supplies Needs Further Improvement (GAO-01-463, Mar. 30, 2001). Recommendations, pp. 25 and 26.

GAO recommendations	Status of recommendations
We recommended that the Secretary of Health and Human Services require the Director of the Centers for Disease Control and Prevention to • execute written agreements as soon as possible with all CDC's partners covering the storage, management, stock rotation, and transporting of medical supplies designated for treatment of biological or chemical terrorism victims; • issue written guidance on security to private warehouses that store stockpiles; and • install proper fencing, to the extent practical, prior to placing inventories at storage locations.	Recommendation partially implemented. CDC's National Pharmaceutical Stockpile Program has final written agreements in place with most partners and anticipates finalizing those under negotiation within the next few months. CDC also issued written standard operating procedures that address security to its private warehouse partners and installed fencing at all locations where inventories are currently stored.
The Secretary of Health and Human Services require the Director of the Office of Emergency Preparedness (OEP) to • finalize, approve, and issue an inventory requirements list; • improve physical security at its central location to comply with DEA regulations, or move the supplies as soon as possible to a location that meets these requirements; • issue a written policy on the frequency of inventory counts and acceptable discrepancy rates; • finalize and implement approved national and local operating plans addressing VA's responsibilities for the procurement, storage, management, and deployment of OEP's stockpiles; • train VA personnel and conduct periodic quality reviews to ensure that national and local operating plans are followed; and • immediately contact FDA or the pharmaceutical and medical supply manufacturers of items stored at its central location to determine the impact of items exposed to extreme temperatures, replace those items deemed no longer usable, and either add environmental controls to the current location or move the supplies as soon as possible to a climate controlled space.	Recommendation partially implemented. OEP finalized its inventory requirements list in February 2001. In June 2001, the supplies stored at the central location were moved to a facility that meets security and controlled temperature requirements. Pharmaceuticals at the central cache are in the process of being potency tested by FDA, and VA has ordered drugs to replace those no longer deemed usable. Further, OEP issued written policies on the frequency of inventory counts and acceptable discrepancy rates. In March 2001, OEP issued national and local operating plans to VA and provided training and conducted periodic quality reviews to ensure that these plans are followed.
The Commandant of the Marine Corps direct the Marine Corps Systems Command to program funding and complete the fielding plan for the CBIRF-specific authorized medical allowance list, require the Commanding Officer of the CBIRF to adjust its stock levels to conform with this list, and remove expired items from stock and replace them with current pharmaceutical and medical supplies.	Recommendation partially implemented. The Marine Corps Systems Command programmed funding in June 2001 to cover deficiencies identified in its authorized medical allowance list. CBIRF expects to fill these deficiencies by October 1, 2001. Further, it removed and destroyed expired items from its stock.

Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities (GAO-01-323, Apr. 25, 2001). Recommendations, pp. 57, 68, and 85.

GAO recommendations	Status of recommendations
The Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies, • establish a capability for strategic analysis of computer-based threats, including developing a related methodology, acquiring staff expertise, and obtaining infrastructure data; • develop a comprehensive governmentwide data-collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources; and • clearly define the role of the National Infrastructure Protection Center (NIPC) in relation to other government and private-sector entities, including • lines of authority among the NIPC and the National Security Council, Justice, the FBI, and other entities; • the NIPC's integration into the national warning system; and • protocols that articulate how and under what circumstances the NIPC would be placed in a support function to either the DOD or the intelligence community.	Recommendation not implemented. The Administration currently is reviewing the federal critical infrastructure protection (CIP) strategy. As of July 2001, no final documents on this strategy had been issued.
The Attorney General task the FBI Director to require the NIPC Director to develop a comprehensive written plan for establishing analysis and warning capabilities that integrates existing planning elements and includes • milestones and performance measures; • approaches (or strategies) and the various resources needed to achieve the goals and objectives; • a description of the relationship between the long-term goals and objectives and the annual performance goals; and • a description of how program evaluations could be used to establish or revise strategic goals, along with a schedule for future program evaluations.	Recommendation not implemented. According to the Director of the NIPC, the NIPC has begun developing a plan that incorporates these elements.
The Attorney General direct the FBI Director to task the NIPC Director to • ensure that the Special Technologies and Applications Unit has access to the computer and communications resources necessary to analyze data associated with the increasing number of complex investigations; • monitor implementation of new performance measures to ensure that they result in field offices' fully reporting information on potential computer crimes to the NIPC; and • complete development of the emergency law enforcement plan, after comments are received from law enforcement sector members. As the national strategy for critical infrastructure protection is reviewed and possible changes considered, we recommend that the Assistant to the President for National Security Affairs define the NIPC's responsibilities for monitoring reconstitution.	Recommendation partially implemented. An emergency law enforcement services sector plan has been issued.

GAO recommendations	Status of recommendations
The Assistant to the President for National Security Affairs (1) direct federal agencies and encourage the private sector to better define the types of information that are necessary and appropriate to exchange in order to combat computer-based attacks and procedures for performing such exchanges; (2) initiate development of a strategy for identifying assets of national significance that includes coordinating efforts already underway, such as those at DOD and Commerce; and (3) resolve discrepancies between PDD 63 requirements and guidance provided by the federal Chief Information Officers Council regarding computer incident reporting by federal agencies. The Attorney General direct the FBI Director to direct the NIPC Director to (1) formalize relationships between the NIPC and other federal entities, including DOD and the Secret Service, and private-sector ISACs so that a clear understanding of what is expected from the respective organizations exists; (2) develop a plan to foster the two-way exchange of information between the NIPC and the ISACs; and (3) ensure that the Key Asset Initiative is integrated with other similar federal activities.	Recommendation partially implemented. The Administration currently is reviewing the federal CIP strategy. As of July 2001, no final documents on this strategy had been issued. The NIPC has created the Interagency Coordination Cell to foster cooperation across government agencies in investigative matters and on matters of common interest and has continued to foster better relationships with the information sharing and analysis centers.

Appendix VI: Organizations Visited and Contacted

During the course of our review, we visited and/or contacted officials from the following organizations:

Cabinet Departments and Related Agencies

Department of Agriculture

- Office of Crisis Planning and Management, Washington, D.C.
- Office of Procurement, Property and Emergency Preparedness, Washington, D.C.

Department of Commerce

- Office of the Chief Information Officer, Washington, D.C.
- Office of the Assistant Secretary of Commerce for Communications and Information, National Telecommunications and Information Administration, Washington, D.C.
- Critical Infrastructure Assurance Office, Washington, D.C.
- National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division, Gaithersburg, Md.

Department of Defense

- Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Principal Director (Acting), Security and Information Operations, Washington, D.C.
- Office of Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Director, Critical Infrastructure Protection, Arlington, Va.
- Office of the Assistant Secretary of Defense for Reserve Affairs, Washington, D.C.
- Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, Washington, D.C.
- Office of the Deputy Assistant Secretary of Defense for Counterterrorism, Plans, and Support, Washington, D.C.
- Office of the Joint Chiefs of Staff, Directorate of Operations (J-3), Chemical, Biological, Radiological, and Nuclear Material, or High-Yield Explosive Division, Washington, D.C.
- Defense Advanced Research Projects Agency, Arlington, Va.

Department of Energy

- Office of Defense Programs, Germantown, Md.
- Office of Non-Proliferation Research and Engineering, Washington, D.C.
- Office of Security and Emergency Operations, Washington, D.C.
- Office of the Chief Information Officer, Office of the Associate CIO for Cyber Security, Washington, D.C.

	• Office of Critical Infrastructure Protection, Washington, D.C.
	• Office of Security Affairs, Germantown, Md.
	  • Office of Safeguards and Security, Germantown, Md.
	• Office of Emergency Operations, Washington, D.C.
	  • Office of Emergency Management, Washington, D.C.
	  • Office of Emergency Response, Germantown, Md.

Department of Health and Human Services	• Office of the Assistant Secretary for Management and Budget, Office of Information Resources Management, Washington, D.C. • Office of Emergency Preparedness, Rockville, Md. • Centers for Disease Control and Prevention, Atlanta, Ga. • U.S. Public Health Service, Rockville, Md. • U.S. Public Health Service, Region VIII, Denver, Colo.

Department of Justice	• Office of the Deputy Attorney General, Washington, D.C.
	• Criminal Division, Computer Crime and Intellectual Property Section, Washington, D.C.
	• Justice Management Division, Washington, D.C.
	• Office of Justice Programs, Washington, D.C.
	  • Office for State and Local Domestic Preparedness Support, Washington, D.C.
	  • National Institute for Justice, Washington, D.C.
	• Federal Bureau of Investigation, Washington, D.C.
	  • Counter Terrorism Division, Washington, D.C.
	  • Domestic Terrorism/Counterterrorism Planning Section, Washington, D.C.
	  • Special Events Management Unit, Washington, D.C.
	  • National Domestic Preparedness Office, Washington, D.C.
	  • WMD Countermeasures Unit, Washington, D.C.
	  National Infrastructure Protection Center, Washington, D.C.
	  • Critical Incident Response Group, Quantico, Va.
	  • Crisis Management Unit, Quantico, Va.
	  • Hazardous Materials Response Unit, Quantico, Va.
	  • Salt Lake City Field Office, Utah

Department of State	• Office of the Undersecretary of Management, Bureau of Information Resource Management/Chief Information Officer, Washington, D.C. • Office of the Under Secretary for Arms Control and International Security Affairs, Bureau of Political-Military Affairs, Washington, D.C. • Office of the Undersecretary for Global Affairs, Bureau for International Narcotics and Law Enforcement Affairs, Washington, D.C. • Office of the Coordinator for Counterterrorism, Washington, D.C. • Technical Support Working Group, Arlington, Va.

Department of Transportation	• Office of the Secretary of Transportation, Washington, D.C.
	  • Office of Security and Administrative Management, Washington, D.C.
	• Office of Intelligence and Security, Washington, D.C.
	• Federal Aviation Administration, Office of the Assistant Administrator for Information Services and Chief Information Officer, Office of Information Systems Security, Washington, D.C.
	• Research and Special Programs Administration, Washington, D.C.
	  • Office of Emergency Transportation, Washington, D.C.
	  • Office of Innovation, Research and Education, Washington, D.C.
	• U.S. Coast Guard, Headquarters, Washington, D.C.
	  • National Response Center, Washington, D.C.

Department of the Treasury	• Office of the Under Secretary for Enforcement, Washington, D.C.
	  • Bureau of Alcohol, Tobacco and Firearms, Headquarters, Washington, D.C.
	  • United States Secret Service, Washington, D.C.
	  • Major Events Division, Washington, D.C.
	  • Technical Security Division, Washington, D.C.
	  • Office of Protective Operations, Olympic Coordinator, Salt Lake City, Utah
	• Office of the Assistant Secretary for Financial Institutions, Washington, D.C.
	• Office of the Deputy Assistant Secretary (Information Systems) and Chief Information Officer, Washington, D.C.

Department of Veterans Affairs	• Headquarters, Washington, D.C. • Office of Emergency Preparedness/Emergency Management Strategic Healthcare Group, Martinsburg, W.Va.

Other Agencies

Environmental Protection Agency	• Office of the Assistant Administrator for Environmental Information, Washington, D.C. • Office of the Assistant Administrator for Water, Office of Ground and Drinking Water, Washington, D.C. • Chemical Emergency Preparedness and Prevention Office, Washington, D.C. • Region VIII, Denver, Colo.
Executive Office of the President	• National Security Council Staff; National Coordinator for Security, Infrastructure Protection and Counterterrorism, Washington, D.C. • Office of Management and Budget, Headquarters, Washington, D.C.

	• Office of Science and Technology Policy, Headquarters, Washington, D.C.

Federal Emergency Management Agency	• Office of the Director, Washington, D.C.
	• Information Technology Services, Washington, D.C.
	• Office of the Inspector General , Washington, D.C.
	• Office of National Security Affairs, Washington, D.C.
	• Preparedness, Training, and Exercises Directorate, Washington, D.C.
	  • Readiness Division, Washington, D.C.
	  • Program Development Branch, Washington, D.C.
	• Response and Recovery Directorate, Washington, D.C.
	• Region VIII, Denver, Colo.

General Services Administration	• Federal Technology Service, Office of Information Assurance and Critical Infrastructure Protection, Washington, D.C. • Federal Computer Incident Response Center, Washington, D.C. • Office of the Inspector General, Washington, D.C.

State and Local Organizations

Adams, Arapahoe, and Douglas Counties, Colo.	• Tri-County Health Department, Commerce City, Colo.
Arapahoe County, Colo.	• Office of Emergency Management, Arapahoe County, Colo. • Sheriff/Emergency Law Enforcement Services Sector Coordinator, Arapahoe County, Colo.
Aurora, Colo.	• Aurora Fire Department, Aurora, Colo. • Office of Emergency Management, Aurora, Colo. • Aurora Police Department, Aurora, Colo. • Buckley Air National Guard Base, Aurora, Colo. • 8th Weapons of Mass Destruction Civil Support Team, Aurora, Colo.

City and County of Denver, Colo.	• Denver Police Department, Denver, Colo.
	• Department of Environmental Health, Denver, Colo.
	• Department of Fire, Denver, Colo.
	• Department of Safety, Denver, Colo.
	• Office of Health and Emergency Management, Denver, Colo.
	• Denver Health, Colo.
	  • Denver Public Health Department, Denver, Colo.
	  • Department of Emergency Medicine, Denver, Colo.

State of Colorado	• Colorado Department of Public Health and Environment, Denver, Colo. • Office of Emergency Management, Department of Local Affairs, Division of Local Government, Golden, Colo. • Rocky Mountain Poison and Drug Center, Denver, Colo.
State of Utah	• Department of Public Safety, Salt Lake City, Utah • Utah Olympic Public Safety Command, Salt Lake City, Utah
Private Sector	• Banking and Finance Infrastructure Sector Coordinator (a position outlined in Presidential Decision Directive 63), in Washington, D.C. • Financial Services—Information Sharing and Analysis Center, Reston, Va.

Appendix VII: Comments From the Executive Office of the President

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

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

September 4, 2001

Mr. Stephen Caldwell
Assistant Director, General Accounting Office
Washington, DC 20548

Dear Mr. Caldwell:

Enclosed is the consolidated response of the Office of Management and Budget, the Office of Science and Technology Policy, and the National Security Council to your draft GAO Report entitled Combating Terrorism (GAO-01-822) as you requested. Thank you for the opportunity to review the report prior to its official release. The report contains much useful information. Attached are comments that clarify the respective roles of the Technical Support Working Group and the Research and Development Subgroup of the Preparedness against Weapons of Mass Destruction Group. Please direct any questions you may have regarding our response to Mr. Mark Seastrom at (202) 395-4802.

Sincerely,

Robin Cleveland
Associate Director
National Security Programs

Enclosure

Enclosure: Comments on draft GAO Report on Combating Terrorism (GAO-01-822)

Now on p. 34.

- **Correction:**

p. 31 Table 1: in the last entry under the column "Current organization responsible for the function", replace "(via the Technical Support Working Group)" with "(via the Preparedness against Weapons of Mass Destruction R&D Subgroup)."

The Technical Support Working Group (TSWG) is more focused on near-term, requirements-driven, non-medical R&D with a focus on deployable technologies that will serve the needs of first responders. The assessment of overall R&D, including non-medical and medical areas, is currently aligned with the NSC under NSPD-1 which established the NSC-Chaired Preparedness against Weapons of Mass Destruction (PWMD) Group. The PWMD has eight subgroups including the Research and Development Subgroup chaired by OSTP. The purpose and operation of this interagency group are generally captured in the draft report, however, the roles of the PWMD Group and the PWMD R&D Subgroup are broader than currently indicated.

The TSWG was established as the technology development component of the Department of State (DOS) chaired Interagency Group on Terrorism. TSWG operates under policy oversight of the DOS Office of the Coordinator for Counterterrorism and the management and technical oversight of the DoD Office of the Assistant Secretary for Special Operations and Low-Intensity Conflict. TSWG's mission is to conduct the national interagency research and development program for combating terrorism through rapid research, development and prototyping.

The TSWG has a successful program of requirements-driven R&D that meets technical support needs of first responders to terrorist incidents. TSWG through its subgroups identifies short-term, non-medical, needs-based projects. In the course of conducting the needs survey and proposal review, TSWG also identifies, serendipitously, projects requiring longer-range R&D.

Now on p. 148.

- **Correction:**

p. 135 fifth row: when mentioning the Pharmaceutical Stockpile, the description seems to imply that the entire stockpile is located in Atlanta. To the best of our knowledge, this is not accurate, since the stockpile is in fact distributed at a number of sites.

Now on pp. 83, 85.

- **Suggested revision:**

p. 80 third paragraph: In order to clarify the complementary roles of the PWMD R&D Subgroup and the TSWG, we suggest deletion of the text with: "To meet these needs identified in the Five-Year Plan,..." through the end of the paragraph and insertion of the following alternative text after the first paragraph on p. 78.

"The overall assessment of research and development is currently aligned with an interagency R&D group under the NSC Policy Coordinating Committee (PCC) on Counter-terrorism and National Preparedness. In the implementation of NSPD-1, the NSC established the NSC-Chaired Preparedness against Weapons of Mass Destruction (PWMD) Group. It has eight subgroups including the OSTP-chaired R&D Subgroup. The PWMD R&D Subgroup reports to the NSC Chair.

All federal departments and agencies with interests, equities, or needs in research and development for combating terrorism are represented on the PWMD R&D Subgroup. To ensure

communication and coordination of activities of the R&D Subgroup and the TSWG, a TSWG co-chair is a member of the R&D Subgroup. The PWMD R&D Subgroup assesses federal R&D programs to help agencies integrate the highest priority items into their budgets, thereby reducing gaps and duplication in efforts to prevent, counter, and respond to chemical, biological, nuclear, and radiological terrorist attacks. It attempts to identify gaps, shortfalls, and overlaps in the federal effort and to develop programmatic objectives to increase our effectiveness in countering unconventional threats. It makes recommendations to the PWMD Group. Identifying such items is a key step in developing a Preparedness Against Weapons of Mass Destruction R&D strategy. The PWMD R&D subgroup has a broad role in identifying long-range, large-scale R&D issues involving preventing, countering, and responding to chemical, biological, radiological, and nuclear terrorist attacks causing mass effect.

In its current work plan, the PWMD R&D Subgroup is: consulting with other PWMD subgroup chairs to identify comprehensive R&D needs in preparedness for combating terrorism; identifying and prioritizing R&D gap-filling objectives; implementing a process for reporting progress toward achieving R&D objectives; and continuing the ongoing effort to achieve concordance of R&D objectives with agency programs."

President Bush on Domestic Preparedness Against Weapons of Mass Destruction

Washington, May 8, 2001 – Protecting America's homeland and citizens from the threat of weapons of mass destruction is one of our Nation's important national security challenges. Today, more nations possess chemical, biological, or nuclear weapons than ever before. Still others seek to join them. Most troubling of all, the list of these countries includes some of the world's least-responsible states – states for whom terror and blackmail are a way of life. Some non-state terrorist groups have also demonstrated an interest in acquiring weapons of mass destruction.

Against this backdrop, it is clear that the threat of chemical, biological, or nuclear weapons being used against the United States – while not immediate – is very real. That is why our Nation actively seeks to deny chemical, biological, and nuclear weapons to those seeking to acquire them. That is why, together with our allies, we seek to deter anyone who would contemplate their use. And that is also why we must ensure that our Nation is prepared to defend against the harm they can inflict.

Should our efforts to reduce the threat to our country from weapons of mass destruction be less than fully successful, prudence dictates that the United States be fully prepared to deal effectively with the consequences of such a weapon being used here on our soil. Today, numerous Federal departments and agencies have programs to deal with the consequences of a potential use of a chemical, biological, radiological, or nuclear weapon in the United States. Many of these Federal programs offer training, planning, and assistance to state and local governments. But to maximize their effectiveness, these efforts need to be seamlessly integrated, harmonious, and comprehensive.

Therefore, I have asked Vice President Cheney to oversee the development of a coordinated national effort so that we may do the very best possible job of protecting our people from catastrophic harm. I have also asked Joe Allbaugh, the Director of the Federal Emergency Management Agency, to create an Office of National Preparedness. This Office will be responsible for implementing the results of those parts of the national effort overseen by Vice President Cheney that deal with consequence management. Specifically it will coordinate all Federal programs dealing with weapons of mass destruction consequence management within the Departments of Defense, Health and Human Services, Justice, and Energy, the Environmental Protection Agency, and other federal agencies. The Office of National Preparedness will work closely with state and local governments to ensure their planning, training, and equipment needs are addressed. FEMA will also work closely with the Department of Justice, in its lead role for crisis management, to ensure that all facets of our response to the threat from weapons of mass destruction are coordinated and cohesive. I will periodically chair a meeting of the National Security Council to review these efforts.

No governmental responsibility is more fundamental than protecting the physical safety of our Nation and its citizens. In today's world, this obligation includes protection against the use of weapons of mass destruction. I look forward to working closely with Congress so that together we can meet this challenge.

The following are GAO's comments on the Office of Management and Budget's (OMB) letter dated September 4, 2001, which provided a consolidated response from selected offices within the Executive Office of the President, including OMB, the Office of Science and Technology Policy, and the National Security Council.

GAO Comments

We incorporated the consolidated comments where appropriate throughout the report. In addition to the letter reprinted in this appendix, OMB referred us to the President's May 8, 2001, statement about the Vice President's effort related to national preparedness. As a result, we have reprinted that statement in this appendix.

Appendix VIII: Comments From the Department of Agriculture

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

DEPARTMENT OF AGRICULTURE
OFFICE OF THE DEPUTY SECRETARY
WASHINGTON, D.C. 20250

Mr. Raymond J. Decker
Director
United States General Accounting Office
Washington, D.C. 20548

SEP - 5 2001

Dear Mr. Decker:

Thank you for the opportunity to provide comments on your proposed report entitled, "Combating Terrorism: Progress Made, but Executive Direction Needed to Address Evolving Challenges."

The report provides a broad overview of the terrorism issue facing this country and a good assessment of the challenges we face in interdicting, detecting, and responding to a terrorist act in a coordinated manner. The Department of Agriculture's role was not an integral part the draft report. There are many facets of the Department and its agencies that should be addressed throughout each chapter; due to time constraints, we are only able to provide brief comments that are included as an enclosure.

I urge the GAO to visit with the Department and key agency officials to get an overview of our issues and what resources and services we are providing. The Department is actually facing two "types" of terrorism and is attempting to address each. They can be characterized as (1) an attack aimed at the safety of our food supply and Agricultural infrastructure causing widespread and long-term damage, and (2) isolated incidents of domestic terrorism aimed at Departmental employees, facilities, and programs, at this time primarily being experienced by the Forest Service (FS), Animal and Plant Health Inspection Service (APHIS) and Agricultural Research Service (ARS). The report speaks almost solely to an act committed with the purpose of disrupting any one of a number of infrastructures in the country, with the exception of agriculture. While, in reality this is certainly a threat to be addressed and properly prepare for, the likelihood of it occurring is uncertain.

However, the reality of the isolated incidents of terrorism aimed at Agency employees, facilities, and programs is significant and they are increasing in intensity and frequency. The report does not address this issue at all. Environmental and genetic research are two issues targeted by domestic terrorists and agencies within the Department are heavily involved in both. For example, groups such as the Earth Liberation Front and Animal Liberation Front and the damage they have inflicted upon the animal & forestry industries, FS, APHIS and ARS research labs, FS timber sales and facilities, and private property, to name a few, are significant. The Department, again, urges the GAO to consider addressing this topic in the report. Not only are Agriculture employees at risk or targeted by these groups, all Government employees are vulnerable. I believe this topic warrants attention in the report.

The Department of Agriculture presents "evolving challenges" to the issue of terrorism within our borders. The challenge is that the Department may not fit the typical profile for terrorism issues. Rest assured, the Department plays an important role in protecting our nation's food supply; agricultural infrastructure; and agency employees, facilities, and programs. We would appreciate the opportunity to be included in the report in order to heighten awareness of the issues and concerns facing the Department of Agriculture and to provide us with the opportunity to be an active participant in the nation's preparation for and response to a terrorist attack.

Thank you for the opportunity to provide input to the report. Please contact Clifford Oliver, Director of the Office of Crisis Planning and Management at (202) 720-5711 if we can be of further assistance.

Sincerely,

James R. Moseley

James Moseley
Deputy Secretary

Enclosure

The following are GAO's comments on the Department of Agriculture's letter dated September 5, 2001.

GAO Comments

The Department of Agriculture (USDA) requested that we revise our discussion of after-action reports (AARs) in chapter 4. After USDA provided us with AARs, we updated table 5 in chapter 4 to indicate that the Department does produce evaluations for terrorism-related exercises that it sponsors. USDA agrees with the practice of writing AARs, but asked that we delete our recommendation to the Secretary of Agriculture because the Department already produces AARs for exercises that it sponsors. We continue to believe that this is a valid recommendation because the Department also could learn valuable lessons when it participates in field exercises sponsored by other agencies. We have incorporated this discussion at the end of chapter 4.

In addition, USDA requested that we revise the report to address the issue of terrorism targeted at U.S. agriculture and the role of the Department in such incidents. Its letter stated that an attack aimed at the safety of our food supply and agricultural infrastructure would cause widespread and long-range damage. As our report clearly states, the objectives and scope of our report focused on federal efforts to respond to terrorist using WMD directly against civilian targets. Therefore, we did not focus on terrorism directed against agricultural targets. Consequently, our discussion of USDA was limited.

The Department also requested that we address the issue of terrorism targeted at federal government employees, facilities, and programs. Its letter stated that there is an increase in the intensity and frequency of domestic terrorist incidents aimed at its employees, facilities, and programs—particularly those of the Forest Service, Animal and Plant Health Inspection Service, and Agricultural Research Service. Again, the objectives and scope of this report focused on federal efforts to respond to terrorist incidents involving WMD against civilian targets. Therefore, we did not focus on terrorism directed against federal government employees and programs.

The Department further requested that we revise the report to include agriculture in our discussion of critical infrastructures in chapter 6. The objectives and scope of this report focused on the critical infrastructures identified by the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office. While we recognize the importance of the food supply, agriculture has not been

designated as a critical infrastructure by either group; therefore, it was not included in our review.

The Department provided us with a separate discussion and summary of USDA's capabilities to prepare for and respond to a terrorist incident. Given the objectives and scope of our review, we have not reprinted that document in this report.

Appendix IX: Comments From the Department of Commerce

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

THE SECRETARY OF COMMERCE
Washington, D.C. 20230

SEP - 7 2001

Mr. Raymond J. Decker
Director
United States General Accounting Office
Washington, DC 20548

Dear Mr. Decker:

This is in response to your request for comments on the General Accounting Office's (GAO) draft report entitled, "Combating Terrorism: Progress Made, but Executive Direction Needed to Address Evolving Challenges." We appreciate GAO's work in this area.

The Department of Commerce agrees with the draft report's conclusion that the best strategy for the Federal Government to fight terrorism is through effective coordination among Federal agencies. The Bush Administration places a high priority on combating terrorism and protecting the Nation's critical infrastructures. It is reviewing the organizational structures for counter-terrorism and critical infrastructure protection to provide leadership and ensure effective coordination of Federal Government efforts. The Administration is also committed to developing a new National Plan for Critical Infrastructure Protection.

The GAO's report is a thorough analysis of a complex issue. While we agree with many of the findings and recommendations in the report, we do have comments on a number of issues. These are set forth in the enclosure. Thank you for the opportunity to comment on the GAO report.

Warm regards,

Donald L. Evans

Enclosure

Department of Commerce Comments:
GAO Draft Report *Combating Terrorism:*
Progress Made, but Executive Direction Needed to Address Evolving Challenges

Overall, the draft report is a thorough examination of a complex subject. U.S. policy on combating terrorism has evolved over the last 30 years as the nature and threat of terrorist attacks has become more intricate. The Department of Commerce carries out its counter-terrorism efforts through the licensing and enforcement efforts of the Bureau of Export Administration (BXA) and its critical infrastructure assurance role through the activities of BXA's Critical Infrastructure Assurance Office (CIAO), the National Telecommunications and Information Administration (NTIA), and the National Institute of Standards and Technology (NIST).

Each of these offices plays an important role in the government's overall efforts. BXA licenses and enforces U.S. laws dealing with the export of sensitive technologies to terrorist supporting states. The CIAO has a number of programs to increase national awareness of infrastructure threats and promote public-private dialogue on how to deal effectively with these threats. The CIAO provides technical assistance to federal agencies that are mapping their key assets and dependencies through its Project Matrix and coordinates the development of the national plan for critical infrastructure assurance. NTIA is a lead agency for the information and communications sector. NIST has long taken the lead in formulating standards and best practices, particularly in the computer security field.

Comment 1.

Now on p. 112.

Page 101 of the draft report notes that PDD-63 designated the CIAO to "plan infrastructure protection efforts." In fact, the CIAO was created, in part, to integrate the various infrastructure plans developed by the private sector and Federal lead agencies into the national plan for critical infrastructure assurance.

Comment 2.

Now on pp. 113-115.

On pages 102-104, we note that NIST has a long history of association with the development and implementation of federal infrastructure protection programs. For example, the Federal Computer Incident Response Center was first established by NIST. Additionally, NIST conducts a broad range of activities in computer security (unclassified/sensitive systems and information) that are related to critical infrastructure protection. These are, among other things, developing guidance for federal agencies, conducting research in cryptography and critical infrastructure protection, and providing computer security expert assistance to federal agencies. NIST also recently established new grants for funding research in critical infrastructure protection.

Comment 3.

Now on p. 124.

On page 113, in the paragraph describing the CIP Grants program, NIST is incorrectly identified. It should be titled "National Institute of Standards and Technology." Also, we propose adding the following sentence after the first sentence in the paragraph:

"This program resulted from a recommendation by the President's Committee of Advisors on Science and Technology (PCAST) that a sizeable investment (up to $100m/yr) be made to support such vital research. The first year (FY-01) has been funded at $5m, and award selections are being processed. This initial funding is inadequate to address the scope and breadth of CIP research challenges."

Comment 4.

Chapter 6 needs to make a more careful distinction between the roles of the Federal Government and the private sector. Most of the nation's critical infrastructures are owned and operated by the private sector. In particular, we believe the report needs to underscore the role played by the Partnership for Critical Infrastructure Security (PCIS). PCIS is a collaborative effort of industry and government to explore ways to assure delivery of vital services over the nation's critical infrastructures. Page 108 of the report states that the CIAO "organized" the PCIS. The CIAO helped in the establishment of the PCIS, but the partnership is an organization formed by private sector member companies to work among themselves and with the federal government to protect critical infrastructures.

Now on p. 119.

2

The following is GAO's comment on the Department of Commerce's letter dated September 7, 2001.

GAO Comment

We incorporated the Department's comments where appropriate in chapter 6.

Appendix X: Comments From the Department of Defense

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301-2500

SPECIAL OPERATIONS/
LOW-INTENSITY CONFLICT

AUG 27 2001

Mr. Raymond J. Decker
Director
Defense Capabilities and Management
United States General Accounting Office
441 G. Street, NW, Rm 4932
Washington, DC 20548

Dear Mr. Decker,

This is the Department of Defense (DoD) response to the General Accounting Office (GAO) draft report, "COMBATING TERRORISM: Progress Made, but Executive Direction Needed to Address Evolving Challenges," dated September 2001 (GAO Code 350016/OSD Case 01-822). The Department generally concurs with the recommendations which are specific to Defense issues (detailed comments are enclosed).

The Department appreciates the opportunity to comment on the draft report.

Daniel J. Gallington
Special Assistant to the Secretary for Policy Matters (Performing the Duties of ASD/SOLIC)

Enclosure
as stated

GAO DRAFT REPORT, 01-822, "COMBATING TERRORISM: Progress Made, but Executive Direction Needed to Address Evolving Challenges," Dated July 31, 2001 (GAO Code 350016/Case 01-822)

DEPARTMENT OF DEFENSE COMMENTS TO RECOMMENDATIONS ADDRESSED TO THE DOD

Now on pp. 17, 86-87.

RECOMMENDATION 1: To ensure that individual agencies benefit fully from exercises in which they participate, the GAO recommended that the Secretaries of Agriculture, Defense, Energy, Health and Human Services, and Veterans Affairs, the Directors of the Bureau of Alcohol, Tobacco, and Firearms, Federal Emergency Management Agency, Federal Bureau of Investigation, and U.S. Secret Service; the Administrator of the Environmental Protection Agency, and the Commandant of the U.S. Coast Guard, and their agencies provide after action reports (AARs) or similar evaluations for all field exercises in which they participate. (pp. 16, 82/ GAO Draft Report)

DoD RESPONSE: The Department concurs and encourages this practice.

Now on pp. 18, 104.

RECOMMENDATION 2: To clarify the roles and missions of specialized National Guard response teams in a terrorist incident involving weapons of mass destruction, the GAO recommended that the Secretary of Defense suspend the establishment of any additional National Guard Weapons of Mass Destruction Civil Support Teams until the DoD has completed its coordination of the team's roles and missions with the FBI. The GAO also recommended that the Secretary of Defense reach a written agreement with the Director, FBI, that clarifies the roles of the teams in relation to the FBI. (pp. 16, 95-96/GAO Draft Report)

DoD RESPONSE: The DoD concurs. The DoD has no plans to establish more WMD CSTs than currently required by law. DoD officials have met with the FBI's WMD Operations Unit to clarify the roles and missions of the WMD CSTs. They have no role or mission that conflicts with or would otherwise interfere with the FBI's responsibility for forensics and crime scene investigation during WMD incidents. WMD CSTs are primarily a state response asset and have no responsibility to collect evidence. Nevertheless, since a WMD incident site could be declared a crime scene, WMD CST members have been trained on chain of custody and evidence collection techniques. Discussions to determine the appropriate agreements between the FBI and DoD are ongoing.

The following are GAO's comments on the Department of Defense's letter dated August 27, 2001.

GAO Comments

We incorporated the Department's comments where appropriate in chapters 4 and 5. In addition to the letter reprinted in this appendix, officials from the Department provided us with technical comments, which we also incorporated where appropriate.

Appendix XI: Comments From the Department of Energy

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

Department of Energy
Washington, DC 20585
August 27, 2001

Mr. Raymond J. Decker
Director, Defense Capabilities
and Management
United States General Accounting Office
441 G Street , NW
Washington, DC 20548

Dear Mr. Decker:

Thank you for the opportunity to review and comment on your proposed report entitled *COMBATING TERRORISM: Progress Made but Executive Direction Needed to Address Evolving Challenges (GAO-01-822).* The Department agrees in general with the contents of the report, and as you requested, technical and administrative comments have been provided directly to your staff. We would however, like to offer our observations in several areas.

First, we commend the extensive research and reporting effort by your analysis team in drafting this comprehensive document. We believe the report accurately describes both the recent accomplishments and also the lack of progress within the interagency community in this area. Clearly much has been done over the years to ensure that the nation is prepared to counter terrorism and its consequences. However, the sheer magnitude of the effort and the ever-changing dynamics of the threat, coupled with the lack of communication and coordination that your report documents, has diminished efforts to develop a comprehensive and integrated national combating terrorism program. We agree that the first step toward developing a national strategy is to conduct a thorough threat and risk assessment to define and prioritize requirements.

We also agree that a single responsible and accountable "focal point" for combating terrorism should be established, independent of any existing federal agency. Regardless of where this entity is placed, it should be given the authority to cut across agency lines with a clear set of obtainable goals and milestones. The key to its success will be strong leadership, an organization with a sense of purpose, and access to the tools necessary to do the job. We believe that the current "Lead Federal Agency" structure for crisis management (Federal Bureau of Investigation, Department of State) has matured and is working well. We also feel that

Printed with soy ink on recycled paper

the Federal Emergency Management Agency is making substantial progress in the consequence management area. However, more needs to be done as the program develops and grows, especially at the State and local level.

The report's recommendations on the importance of interagency exercises and feedback on lessons learned are completely accurate. We believe it would be very beneficial to exercise the complete domestic counterterrorism command and control and response mechanisms using a realistic, progressive, end-to-end scenario with participation by the actual decision makers through both the crisis management and consequence management phases.

We share your observations on the importance of an aggressive counterterrorism research and development effort. Better interagency communication and a more extensive and formal coordination mechanism would increase efficiency, be more cost effective, and ensure against duplication of effort.

Concerning critical infrastructure protection we have two points. First, while computer-based attacks are real and viable threats, and in some cases may be interpreted as terrorism, they cannot be labeled as such in many instances. Second, we should not allow the highly visible cyber issues to overshadow the threat of possible physical attacks against other infrastructure elements, particularly energy, transportation, and water supply systems. The intricate interdependencies of these systems are not yet fully understood, and we are learning more about the critical impact of their relationships every day. In the new economy, these interconnected infrastructures are becoming increasingly fragile and subject to cascading disruptions that can have broad regional, national, and global consequences. Further focus and resources need to be applied to better understand the threat and how best to protect, mitigate, respond, and recover from attacks against our critical infrastructures.

The Department of Energy has a unique and vital role to play in the fight against terrorism and its consequences in three key areas. First we protect our own facilities and the Nation's nuclear assets in our custody, ensuring that these highly visible and critical targets are extremely unattractive to any terrorist attack. We also support a wide range of U.S. government agencies with a strong and robust technical base, especially in the nuclear and radiological areas where we have unique capabilities. Finally, the Department has a national mandate to help ensure the reliability of the Nation's energy infrastructure and its security from attack and from disruption.

If you have any questions please contact me, or Pat Daly of my staff, at (202) 586-3345. Again, thank you for the opportunity to comment on this report. We value your continued excellent efforts in this vital national program.

Sincerely,

J. S. Mahaley

Joseph S. Mahaley, Director
Office of Security and
Emergency Operations

The following is GAO's comment on the Department of Energy's letter dated August 27, 2001.

GAO Comment

We incorporated the Department's comments where appropriate throughout the report.

Appendix XII: Comments From the Department of Health and Human Services

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

DEPARTMENT OF HEALTH & HUMAN SERVICES Office of Inspector General

Washington, D.C. 20201

AUG 29 2001

Mr. Raymond J. Decker
Director
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Decker:

Enclosed are the Department's comments on your draft report, "Combating Terrorism: Progress Made, but Executive Direction Needed to Address Evolving Challenges." The comments represent the tentative position of the Department and are subject to reevaluation when the final version of this report is received.

The Department appreciates the opportunity to comment on this draft report before its publication.

Sincerely,

Michael Mangano

Michael F. Mangano
Principal Deputy Inspector General

Enclosure

The Office of Inspector General (OIG) is transmitting the Department's response to this draft report in our capacity as the Department's designated focal point and coordinator for General Accounting Office reports. The OIG has not conducted an independent assessment of these comments and therefore expresses no opinion on them.

Comments of the Department of Health and Human Services
on the General Accounting Office's Draft Report,
"Combating Terrorism: Progress Made, but
Executive Direction Needed to Address Evolving Challenges"

The Department of Health and Human Services thanks the General Accounting Office (GAO) for the opportunity to review and comment on your draft report.

Recently, the President announced that the Vice President is undertaking a comprehensive review of the strategic direction of Federal efforts to counter terrorist threats. We are certain that the observations and comments that have been made in this report will be useful.

The Department has been a full participant in developing our own capacities as well as those of State and local governments to respond to terrorist threats, including bioterrorism. The Department's Centers for Disease Control and Prevention has supported the improvement of the Nation's public health infrastructure to respond to terrorist incidents at all levels of government, including the creation of a national pharmaceutical stockpile; the Department's National Institutes of Health has supported the development of new pharmaceuticals and vaccines; and the Department's Office of Emergency Preparedness has supported the development of systems to care for the mass casualties that might result from terrorists successfully carrying out an attack.

The Department's testimony to Congress on many occasions has chronicled the development of our capacities and programs. Likewise, our budget requests and reports to Congress have described our program needs and progress. We are concerned that although we are making progress, much remains to be done to assure that our response to the health consequences of any terrorist attack will be effective in protecting the health of the American people.

In addition to these general observations, we offer the following specific comments and edits:

Now on p. 26.

Page 23, first paragraph, second sentence: Local and State authorities will be the first to respond to a terrorist attack, but any mass casualty producing event would prompt a rapid, vigorous Federal response, not just monitoring activity. There should be no possible inference of a delay in Federal assistance to local and State responders.

Now on p. 55.

Page 51, last paragraph: Delete all after " ...to the Federal Response Plan for biological terrorism." The need for the referenced annex has been superseded by the FBI/FEMA-published United States Government Interagency Domestic Terrorism Concept of Operations Plan and a new bioterrorism annex, which is currently being prepared by the Department.

Now on p. 56.

Page 52, first full paragraph, line 11: Insert "and the Office of Emergency Preparedness" following the "Centers for Disease Control and Prevention."

Now on p. 57.

Page 53, last paragraph, line 3: Delete "other related efforts" and replace with "similar plans of other agencies."

Now on p. 60.

Page 56, figure 3: In the Department's box, change "Chemical/Biological Rapid Deployment Team" to " Domestic Emergency Support Team component" and add "National Medical Response Team/WMD." The latter reference is to any of four teams nationwide that can be prepositioned in response to a weapons of mass destruction (WMD) threat to provide technical assistance, sample collection or other WMD crisis management-related functions.

Now on p. 65.

Page 61, first two lines: Delete "or" and insert a comma in its place, and insert "or those within the Laboratory Response Network," between "...Infectious Diseases," and "the National...." Replace the last three sentences of the paragraph with "This Laboratory Response Network has responded to hundreds of events, State and local, since its inception. It represents an operational partnership for early detection and laboratory confirmation between CDC, the FBI, DOD and State and local health departments. The network has a common training doctrine and develops standardized assays that it distributes to its partners. It is a critical new component of national preparedness for bioterrorism."

Now on p. 65.

Page 61, first full paragraph, line 5: Change "National Special Security Events" to "National Security Special Events."

Now on p. 71.

Page 67, last line: Change "a major disease outbreak." to "a disease outbreak of this magnitude." The CDC has responded to many major disease outbreaks in the United States and the world but arguably none affecting the number of people that might be affected over a short period of time by the most intense bioterrorism event.

Now on p. 72.

Page 68: Remove Figure 6 entitled "Arrival of a Simulated National Pharmaceutical Stockpile During TOPOFF 2000 Exercise." The photograph is misleading because 1) it shows an airplane that was used by technical assistance personnel and is far too small to deliver a push package from the National Pharmaceutical Stockpile (NPS), and 2) the simulated packages on the wooden pallets do not accurately represent items from the NPS--the NPS has specialized cargo containers for air transportation of its pharmaceuticals, supplies and equipment.

Now on p. 80.

Page 76, top paragraph: Add to the end, "NIH is engaged in research that will lead to the development of new or improved vaccines, antibiotics and antivirals. CDC, in collaboration with other Federal agencies, is conducting research on the diagnosis and treatment of smallpox, and the Food and Drug Administration is investigating a variety of biological agents that could be used as terrorist weapons."

Now on pp. 80-81.

Pages 76 and 77: There is reference on both pages to "very high-risk" NIH research. The definitions of "low-risk" and "high-risk" should be clearly stated.

Now on p. 91.

Page 85: We suggest adding a third bulleted paragraph that reads: "HHS supports the development of Metropolitan Medical Response Systems in order to enhance local planning and health care capacity to respond to the health consequences of a WMD release. This program encourages local jurisdictions to strengthen regional and State response relationships. Begun in 1996, the program now includes 97 metropolitan jurisdictions or areas with a total population of approximately 150 million people. The U.S. Public Health Service Noble Training Center, located in the former Noble Army Community Hospital at Ft. McClellan in Anniston, Alabama,

provides a unique medical training facility dedicated to preparing health personnel to respond to chemical and biological weapons attacks."

Now on p. 122.

Page 111: In the "Public health services" line, in the third column, change "No assessments" to "Assessment methodology being researched;" in the fourth column, change "No program" to two bullets to read "Some meetings on CIP issues held" and "Joint effort with CIAO to initiate program being developed;" and in the fifth column, change "No" to read "Virtual ISAC being developed."

Now on p. 146.

Page 133, under Department of Health and Human Services: Delete the current entries and replace with "Domestic Emergency Support Team component and National Medical Response Team/WMD (NMRT/WMD)" in the first column. In the second column, state "The Domestic Emergency Support Team component provides technical assistance as needed. Each NMRT/WMD provides an operational response capability, including a pharmaceutical cache for treating up to 5,000 people for chemical weapons exposures." In the third column state, "The size and composition of each team is determined by the type and location of the event or threat."

Now on p. 148.

Page 135: Change wording in the NPS mission to read "supplies" rather than "treatments."

The following is GAO's comment on the Department of Health and Human Service's letter dated August 29, 2001.

GAO Comment

We incorporated the Department's comments where appropriate throughout the report.

Appendix XIII: Comments From the Department of Justice

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

U.S. Department of Justice

Washington, D.C. 20530

SEP - 6 2001

Mr. Raymond J. Decker
Director
U.S. General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Decker:

The Deputy Attorney General has asked me to convey the comments of the Department of Justice (Department) concerning your draft report entitled "Combating Terrorism: Progress Made, but Executive Direction Needed to Address Evolving Challenges." The draft was reviewed by representatives of the Office of the Deputy Attorney General, the Criminal Division, the Office of Justice Programs, and the Federal Bureau of Investigation.

As you know, there is no higher priority than keeping Americans safe from terrorism, both at home and abroad. Thus, we welcome the General Accounting Office's (GAO) continued review of our multi-agency efforts to combat terrorism. Nevertheless, we have serious reservations about portions of the discussion and some of the recommendations in GAO's most recent review of federal efforts in this area. We are pleased to have the opportunity to summarize our concerns in this letter.

In Chapter 2, the report recommends that the President, working with Congress and in conjunction with the Vice President's terrorism review, appoint a single focal point -- in the Executive Office of the President -- having broad responsibility and authority for coordinating our response to terrorism. As the report recognizes, there is a focal point in the National Security Council (NSC), namely, the National Coordinator for Security, Infrastructure Protection and Counterterrorism. Through the mechanism of the NSC's Counter-Terrorism Security Group, the response of pertinent agencies to terrorism incidents and threats is coordinated in a manner that recognizes the unique roles and contributions of each agency to the overall effort. In our view, there is no need

at this time to change or expand that role. Moreover, in light of the Vice President's pending review -- aimed at the development of a coordinated national effort to ensure that we do the best possible job of protecting our citizens from catastrophic harm -- this recommendation is premature.

In Chapter 3, the report recognizes the substantial interagency effort that has been dedicated to the development of the Five-Year Interagency Counter-Terrorism and Technology Crime Plan (the Five-Year Plan), and refers to it as "the one document that could serve as the basis of a national strategy." Nevertheless, the report faults the Five-Year Plan as being more focused on agency activities than outcomes. It also recommends that the format of the Plan be altered to reflect measurable outcomes and to identify the roles of state and local governments in combating domestic terrorism.

As we have stated on other occasions, we disagree with this assessment. The Five-Year Plan, along with its accompanying July 17, 1999, Implementation Plan, outlines priorities and times frames and identifies those agencies responsible for achieving these goals and objectives. Each agency must have the flexibility to link the goals and objectives of the Five-Year Plan to its own strategic goals and measures.

We support the recommendation in Chapter 4 that there be an interagency process to draft lessons learned from multi-agency exercises that test our domestic preparedness. There are efforts underway to formalize this process. For instance, the Federal Bureau of Investigation's (FBI) National Domestic Preparedness Office (NDPO) has made strides on improving after-action reports. In partnership with DOD and others, the NDPO has begun developing an After Action/Lessons Learned/Remedial Action Program (ALRAP) geared to identifying gaps and shortfalls which occur during weapons of mass destruction (WMD) exercises. The ALRAP would enable the NDPO to collect, process, analyze, maintain, and distribute lessons learned and related issues and observations. The Remedial Action portion of the program has the capability to identify impediments to WMD exercises and assign responsibility for tracking and corrective action. ALRAP is based on the Air Force Instructional Input Program, which is a web-based user-friendly input program designed to track after action reports following WMD exercises. The software is unclassified and can be distributed to state and local emergency responders, and thus the program can identify vulnerabilities and formulate recommendations to WMD exercise participants.

In Chapter 5, the report recommends that the activities of the Department's Office for State and Local Domestic Preparedness Support (OSLDPS) and the FBI's NDPO be consolidated under the Federal Emergency Management Agency (FEMA). We disagree with the recommendation as it relates to OSLDPS, but have undertaken steps to transfer NDPO's functions to FEMA, once its Office of National Preparedness (ONP) is operational.

As to NDPO, on May 8, 2001, the President announced that he had asked Joe Allbaugh, the Director of FEMA, to create an Office of National Preparedness to coordinate all federal programs dealing with consequence management related to weapons of mass destruction. The President also directed that FEMA would coordinate closely with the Department of Justice. In reviewing the functions of NDPO, the Department has concluded that NDPO's core mission - the coordination of all federal programs dealing with consequence management related to weapons of mass destruction - should be transferred to the new ONP within FEMA, in compliance with the President's directive. The Department is prepared to coordinate that transfer, including the detail of staff from the NDPO and the Office of State and Local Domestic Preparedness Support (OSLDPS), once the ONP is fully funded and operational. This proposed transfer, of course, in no way affects the FBI's role as Lead Federal Agency to ensure multi-agency coordination in the case of a terrorist threat or incident. In the meantime, NDPO continues to meet the needs of state and local first responders.

The Department does not agree, however, that the functions of OSLDPS should be consolidated within FEMA. As the Attorney General assured Congress on May 9, 2001, following the President's announcement, the shifting of the facilitation and coordination function to FEMA should not affect our programs in the Office of Justice Programs, including OSLDPS. We believe these roles fit squarely within the Office of Justice Program's mission of providing grant assistance to state and local governments, and we see no reason for that to change. Indeed, it is our understanding that FEMA agrees.

We agree with the report's conclusion in Chapter 6 that establishing a central authority within the Executive Branch for formulating policy regarding computer-based attacks on critical infrastructure facilities may help coordinate efforts underway in agencies across the federal government. However, we submit that careful consideration should be given to how such central authority would be administered. For example, the operational authority of components of the Executive Branch with access to data that is gathered using both

criminal and intelligence authorities is often carefully prescribed. Court-sanctioned criminal and intelligence collection techniques are subject to different legal requirements. Therefore, the commingling of information gathered from such techniques raises significant legal and policy issues. Perhaps the best means of avoiding such problems is by ensuring that the individual or body possessing centralized policy-making authority for matters related to terrorism and critical infrastructure protection does not also possess or exercise operational authority and specifically, does not direct or control criminal or intelligence investigations.

In the spirit of the report, we will continue to build on the strong relationships that we have forged with other agencies, the intelligence community, and the private sector to ensure the protection of our critical infrastructure and to address effectively the threat of disruption posed by computer crimes.

We have provided separately some additional comments and proposed technical changes. We appreciate the opportunity to review and comment on the GAO draft report. If you should have any questions concerning our response, please do not hesitate to contact me.

Sincerely,

Janis A. Sposato
Acting Assistant Attorney General
for Administration

The following are GAO's comments on the Department of Justice's letter dated September 6, 2001.

GAO Comments

Regarding the Department of Justice's comments on chapter 2 about creating a single focal point, on chapter 3 about the Attorney General's Five-Year Plan, on chapter 4 about lessons learned, on chapter 5 about consolidating some of its functions under FEMA, and on chapter 6 about computer-based threats, we have incorporated its comments as appropriate in those respective chapters.

In addition to the letter in this appendix, the Department of Justice provided us with technical comments on our report. The Department's Office for State and Local Domestic Preparedness Support also provided us with extensive technical comments and supporting documentation. Because these points were not fully addressed in the Department's letter, we are summarizing them below, including our response.

- The Department commented that chapter 1 of our draft report needed to clarify its discussion of the concurrency of crisis and consequence management and the respective roles of lead and support agencies. We incorporated its comments as appropriate.
- The Department commented that chapter 3 of our draft report downplayed the significance of its efforts to help states and local governments conduct threat and risk assessments. It said that the Department plans to use the results of these assessments in deciding how to allocate its equipment, training, and exercise program resources consistent with previous GAO recommendations. We revised the report to discuss these assessments in more detail and to reflect their potential importance. We also separated our discussion of state and local-level assessments from our discussion of a national-level assessment that the FBI had previously agreed to produce.
- The Department commented that chapter 5 of our draft report did not adequately reflect its efforts to reduce duplication and improve the delivery and coordination of assistance to state and local governments. The Department said it had taken a number of actions to reduce duplication and better integrate these programs across the federal government. We updated the report to reflect these ongoing efforts. The Department also asserted that because of its efforts, state and local first responders are no longer confused by the multitude of federal assistance programs. We disagree with this point and revised the report by providing additional evidence of continued confusion.
- The Department commented that chapter 5 of our draft report incorrectly stated that FEMA was the lead agency for preparing state and local

governments to manage the consequences of WMD terrorism. The Office for State and Local Domestic Preparedness Support took the position that the Department of Justice, in both legal and programmatic terms, was the lead agency for preparing state and local governments for WMD terrorism. We disagree with the Office's position and discuss this issue at the end of chapter 5.

In addition, the Department provided us with an update related to chapter 3 on our previous recommendations that it develop threat and risk assessments. We updated chapter 3 of the report to reflect these efforts and provide the Department's latest milestones for their completion.

Appendix XIV: Comments From the Department of the Treasury

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

SEP 10 2001

Mr. Raymond J. Decker
Director
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Decker:

We have reviewed the GAO draft report entitled Combating Terrorism and request that you incorporate the enclosed technical comments from the U.S. Secret Service, the Bureau of Alcohol, Tobacco and Firearms and the Office of Enforcement.

We hope these comments will be beneficial in completing the final report. If you have any questions, please call me at (202) 622-0370.

Sincerely,

Anna F. Dixon
Director, Office of Finance
and Administration
Office of Enforcement

Enclosure

The following is GAO's comment on the Department of the Treasury's letter dated September 10, 2001.

GAO Comment

In addition to the letter reprinted in this appendix, the Department provided technical comments from the U.S. Secret Service; the Bureau of Alcohol, Tobacco and Firearms; and the Office of Enforcement. We incorporated these technical comments where appropriate throughout the report.

Appendix XV: Comments From the Department of Veterans Affairs

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

THE SECRETARY OF VETERANS AFFAIRS

WASHINGTON

SEP 0 5 2001

Mr. Raymond J. Decker
Director, Defense Capabilities
and Management Issues
U. S. General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Decker:

As public attention to terrorist threats has grown, the Department of Veterans Affairs (VA) has taken an increasingly active role in governmental efforts to combat them. In commenting on your draft report, ***COMBATING TERRORISM: Progress Made but Executive Direction Needed to Address Evolving Changes*** (GAO-01-822) I am pleased to convey VA's proactive interest in this increasingly confounding challenge.

VA's approach to combating terrorism includes the following three interrelated efforts: our Critical Infrastructure Protection Program, our Emergency Management Program, and our Weapons of Mass Destruction Incident Response Program. Within the context of each of these programs, we partner with other federal departments and agencies working to combat terrorism.

The Department has taken the necessary steps to protect its infrastructure from intentional acts that would significantly diminish its ability to perform its mission of serving American veterans and their families. Our Critical Infrastructure Protection Program addresses the protection of the Department's physical assets, personnel (employees as well as our veterans and other visitors to our facilities), telecommunications systems, and cyber systems.

We work closely with the Federal Emergency Management Agency to ensure compliance with the various Continuity of Government and Continuity of Operations requirements found in Presidential Decision Directive (PDD) 67, and support the Department of Health and Human Services (HHS) in disaster medical response, including response to terrorist incidents. As a partner in the National Disaster Medical System, we are involved in planning, coordinating, training, and participating in exercises in preparation for a variety of catastrophic events. Although VA has a demanding internal exercise program and participates in a wide range of tabletop and field exercises with other agencies at the local and state levels, we recognize the need to increase awareness and training within VA's headquarters elements. We support GAO's call for additional major interagency field exercises that would include a robust consequence management component.

Mr. Raymond J. Decker

However, while we concur with the intent of GAO's recommendation that would require federal agencies and organizations to "prepare after action reports (AARs) or similar evaluations for all exercises they lead and for all field exercises in which they participate," we suggest GAO modify this language. An improved statement would be, "prepare AARs or similar evaluations for all training activities in which they participate that are designated as federal interagency counterterrorist exercises by the lead federal agency (LFA)." The definition of "federal interagency counterterrorist exercise" is currently unclear. Prospective designation by a LFA would avoid misunderstandings. VA plans to implement the recommendation using the standard AAR policy our Veterans Health Administration's Emergency Management Strategic Healthcare Group developed to identify "Issues for Action" following counterterrorism exercises.

VA also supports the primary departments and agencies identified in PDD 62. We directly support HHS efforts to maintain adequate stockpiles of antidotes and other necessary pharmaceuticals nationwide by maintaining four pharmaceutical caches for immediate deployment (with an HHS National Medical Response Team) in the event of an actual incident that involves weapons of mass destruction. We maintain a fifth cache to place on site for special high-risk national events such as the Presidential Inauguration. Additionally, we recently made an agreement with the Centers for Disease Control and Prevention to establish another set of national stockpiles of supplies and equipment for response to biological or chemical incidents.

I appreciate the opportunity to comment on GAO's draft report.

Sincerely yours,

Anthony J. Principi

Anthony J. Principi

The following are GAO's comments on the Department of Veterans Affairs' letter dated September 5, 2001.

GAO Comments

The Department of Veterans Affairs (VA) concurred with the intent of our recommendation on after-action reports (AARs) in chapter 4 and agreed that it will implement the recommendation. Our past and ongoing work has already demonstrated that VA has a good record of producing AARs. However, VA asked that we change the wording of the recommendation to limit it to exercises that are "designated as federal interagency counterterrorist exercises by the lead federal agency." We disagree with this revision because it might limit the production of AARs in a manner to exclude important exercises. In our previous work, we found that some of the better consequence management exercises were sponsored by VA or the Department of Defense (DOD), not by FEMA—the lead federal agency for consequence management.[1] For example, in September 1997, VA and DOD sponsored a field exercise to practice providing medical care to victims of a terrorist WMD attack. That exercise, which had over 2,000 participants, also included state and local responders and local community hospitals. Changing the wording of our recommendation, as suggested by VA, might exempt agencies from producing AARs for such exercises. Given the Department's good record in producing AARs, even in cases when they were not "designated" by a lead federal agency, we believe that the wording in our recommendation will not place any additional burden upon the Department.

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

Appendix XVI: Comments From the Federal Emergency Management Agency

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

Office of the Director

Federal Emergency Management Agency

Washington, D.C. 20472

AUG 31 2001

Mr. Raymond J. Decker
Director
Defense Capabilities and Management
United States General Accounting Office
Washington, DC 20548

Dear Mr. Decker:

I am responding to your request of FEMA for comments on the draft GAO report entitled *Combating Terrorism: Progress Made, but Executive Direction Needed to Address Evolving Challenges*. After extensive agency reviews, the enclosed document represents the collective FEMA comments.

We appreciate the excellent working relationship that has been established with your office and staff in developing this report and others in the *Combating Terrorism* series. I trust this information is responsive to your request. If you need further assistance, please contact Tom Antush on 202-646-3617.

Sincerely,

John W. Magaw

John W. Magaw
Acting Director
Office of National Preparedness

Enclosure

FEMA's Comments in Response to the GAO Report
Combating Terrorism: Progress Made, but Executive Direction Needed to Address Evolving Changes
(September 2001)

Following are FEMA's comments in response to the draft GAO report, *Combating Terrorism: Progress Made, but Executive Direction Needed to Address Evolving Changes* (September 2001).

Now on p. 86.

Page 82. **Item**: To improve readiness in consequence management, we recommend that the Director of the Federal Emergency Management Agency play a larger role in managing federal exercises to combat terrorism. As part of this, FEMA should seek a formal role as co-chair of the Interagency Working Group on Exercises and help to plan and conduct major interagency counterterrorist exercises to ensure that consequence management is adequately addressed.

FEMA Comment: The President's statement of May 8, 2001 directed the Director of FEMA to create the Office of National Preparedness to coordinate all Federal programs dealing with WMD consequence management and to ensure that state and local governments' planning, training, and equipment needs are addressed. Additionally, FEMA was charged to work closely with DOJ to ensure that "all facets of our response to the threat from weapons of mass destruction are coordinated and cohesive." These efforts will improve consequence management readiness and will ensure that FEMA plays a larger role in Federal exercises. We agree with the recommendation that FEMA serve as a co-chair of the Interagency Working Group on Exercises and look forward to working with the interagency community to address this need.

Now on pp. 13, 17, 69-70.

Pages 12, 15, 62. **Item**: The Federal Emergency Management Agency is still not using exercises to fully practice its leadership role over consequence management.

FEMA Comment: Most WMD exercises involve a consequence management component. The Domestic Preparedness Program sponsored by DOJ is one example. In these exercises, first responders are required to decontaminate, transport, triage, and assist victims. FEMA agrees that using exercises to practice respective leadership roles is beneficial. We look forward to working with the interagency community to further exercise FEMA's leadership role, which is to serve as the primary coordinating agency for disaster response and recovery activities.

Now on p. 37.

Now on p. 52.

Page 34. **Item**: The President also asked the Director of FEMA to create a new Office of National Preparedness to assist the Vice President in implementing a national strategy on consequence management. **Page 47.** **Item**: FEMA's new Office of National Preparedness will develop a national strategy.

FEMA Comment: The President's statement does not explicitly direct either the Vice President or the Office of National Preparedness to develop a national strategy. According to the President's Statement of May 8, the VP is "to oversee the development of a coordinated national effort." The Office of National Preparedness is responsible for "implementing the results of those parts of the national effort overseen by Vice President that deal with consequence management." FEMA will therefore be guided by the efforts of the Vice President. We assume that these efforts will result in the development of a coordinate national strategy with measurable goals and objectives.

2

Now on pp. 14, 90, 99-100.
Now on p. 104.

Pages 13, 84, 91. **Item**: This new Office [ONP] provides an opportunity to consolidate federal programs to assist state and local governments, including some assistance programs currently under the Department of Justice and Federal Bureau of Investigation. **Page 95.** **Item**: Consolidate the activities of the Department of Justice's Office for State and Local Domestic Preparedness Support, and the FBI's National Domestic Preparedness Office under the Federal Emergency Management Agency.

FEMA Comment: FEMA believes that before any additional mandates or changes are placed on this new Office, we need to give it a chance to accomplish its tasks as put forth by the President – to coordinate Federal programs dealing with weapons of mass destruction consequence management, working closely with state and local governments to ensure that their needs are addressed. There are no plans to take programs away from other departments or agencies; rather, it will coordinate and better integrate programs to build upon existing efforts. The Attorney General is in the process of reviewing the role of the NDPO, and any changes to its role and/or function will be announced when this review is complete.

Now on p. 55.

Page 51. **Item**: FEMA is revising the Federal Response Plan to include an explanation of its relationship to other federal emergency plans, such as the National Oil and Hazardous Substances Pollution Contingency Plan (National Contingency Plan) or Federal Radiological Emergency Response Plan. Revisions will address responses for radiological releases.

FEMA Comment: We would recommend the use of the word *clarifying*, not necessarily *revising*. A change will be issued to section IV. B (p. 11) of the Federal Response Plan – *Concurrent Implementation of Other Federal Emergency Plans* – to expand and to clarify individual agency roles and responsibilities as well as funding arrangements. Federal agencies have tentatively agreed to the changes, and after it has been sent out to the agencies there will be a 60-day concurrence period. Once final approval has been given, then the changes will be issued as a change notice. Additionally, the current FRP will be renamed the *President's Federal Response Plan*. All Cabinet secretaries and agency heads will be asked to personally sign the Plan, recommitting their agencies to support the FRP concept of operations and carry out their functional responsibilities to ensure the orderly, timely delivery of Federal assistance in a major disaster or emergency that overwhelms the capabilities of State and local governments to respond effectively.

Now on p. 77.

Table 5, page 73. **Item**: FEMA – Policy requires After Action Reports (AARs); formal process is the Corrective Action Plan – Produces no AARs for exercises and special events.

FEMA Comment: We will review and evaluate our current procedures regarding after action reports and make any necessary changes to ensure that AARs for WMD are completed in a timely fashion.

Now on pp. 15, 103-104, 107.

Pages 14, 95-96. **Item**: Until the Department of Defense has completed its coordination of the Civil Support Teams (CSTs) roles and missions with the Federal Bureau of Investigation, the lead federal agency for crisis management, the establishment of any additional teams would be premature.

3

Now on p. 92.

See comment, p. 203.

Now on p. 122.

FEMA Comment: FEMA should also be consulted regarding the coordination of the CSTs, as they also play a role in the consequence management functions of response in the event of a WMD incident.

Table 6, page 86. Item: Awaiting data on FEMA National Fire Academy and Emergency Management Institute.

FEMA Comment: Under FEMA National Fire Academy and Emergency Management Institute, the following data should be included:

FY 1998	FY 1999	FY 2000	FY 2001	Total
37,354	39,545	26,713	18,274	121,886

Table 7, page 111. Item: Emergency fire services segment – no remedial plans – no information sharing and analysis center established.

FEMA Comment: The United States Fire Academy (USFA) has been designated as the sector ISAC and performing those duties since March 1, 2001. USFA is awaiting NIPC response to its memorandum of agreement.

4

The following is GAO's comment on the Federal Emergency Management Agency's letter dated August 31, 2001.

GAO Comment

After we received FEMA's written comments, FEMA provided us with revised figures for the number of persons trained at the National Fire Academy and Emergency Management Institute from fiscal year 1998 through July 31, 2001, of fiscal year 2001. We incorporated the Agency's comments where appropriate throughout the report.

Appendix XVII: GAO Contacts and Staff Acknowledgments

GAO Contacts:

Counterterrorism:

Raymond J. Decker (202) 512-6020
Stephen L. Caldwell (202) 512-9610

Cyberterrorism:

Robert F. Dacey (202) 512-3317
Jean L. Boltz (202) 512-5247

Acknowledgments

In addition to those named above, Mark A. Pross, Michael W. Gilmore, Richard A. McGeary, Danielle P. Hollomon, James C. Lawson, Krislin M. Nalwalk, Harry L. Purdy, Karl W. Siefert, Yvonne J. Vigil, Keith A. Rhodes, Rahul Gupta, Grace A. Alexander, Jane D. Trahan, and Heather J. Taylor made key contributions to this report.

Related GAO Products

Combating Terrorism: Actions Needed to Improve DOD's Antiterrorism Program Implementation and Management (GAO-01-909, Sept. 19, 2001).

Critical Infrastructure Protection: Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities (GAO-01-1132T, Sept. 12, 2001).

International Crime Control: Sustained Executive-Level Coordination of Federal Response Needed (GAO-01-629, Aug. 13, 2001).

FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters Is Limited (GAO-01-780, July 16, 2001).

Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities (GAO-01-769T, May 22, 2001).

Combating Terrorism: Comments on H.R. 525 to Create a President's Council on Domestic Preparedness (GAO-01-555T, May 9, 2001).

Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities (GAO-01-323, Apr. 25, 2001).

Combating Terrorism: Observations on Options to Improve the Federal Response (GAO-01-660T, Apr. 24, 2001).

Combating Terrorism: Accountability Over Medical Supplies Needs Further Improvement (GAO-01-463, Mar. 30, 2001).

Combating Terrorism: Comments on Counterterrorism Leadership and National Strategy (GAO-01-556T, Mar. 27, 2001).

Combating Terrorism: FEMA Continues to Make Progress in Coordinating Preparedness and Response (GAO-01-15, Mar. 20, 2001).

Combating Terrorism: Federal Response Teams Provide Varied Capabilities; Opportunities Remain to Improve Coordination (GAO-01-14, Nov. 30, 2000).

West Nile Virus Outbreak: Lessons for Public Health Preparedness (GAO/HEHS-00-180, Sept. 11, 2000).

Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies (GAO/AIMD-00-295, Sept. 6, 2000).

Combating Terrorism: Linking Threats to Strategies and Resources (GAO/T-NSIAD-00-218, July 26, 2000).

Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination (GAO/T-AIMD-00-268, July 26, 2000).

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

Security Protection: Standardization Issues Regarding Protection of Executive Branch Officials (GAO/GGD/OSI-00-139, July 11, 2000).

Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance (GAO/RCED-00-75, June 28, 2000).

Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000 (GAO/T-AIMD-00-229, June 22, 2000).

Weapons of Mass Destruction: DOD's Actions to Combat Weapons Use Should Be More Integrated and Focused (GAO/NSIAD-00-97, May 26, 2000).

Security: Breaches at Federal Agencies and Airports (GAO/T-OSI-00-10, May 25, 2000).

Critical Infrastructure Protection: "I LOVE YOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities (GAO/T-AIMD-00-181, May 18, 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).

Critical Infrastructure Protection: National Plan for Information Systems Protection (GAO/AIMD-00-90R, Feb. 11, 2000).

Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection (GAO/T-AIMD-00-72, Feb. 1, 2000).

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

Food Safety: Agencies Should Further Test Plans for Responding to Deliberate Contamination (GAO/RCED-00-3, Oct. 27, 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: The Status of Computer Security at the Department of Veterans Affairs (GAO/AIMD-00-5, Oct. 4, 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).

Information Security: NRC's Computer Intrusion Detection Capabilities (GAO/AIMD-99-273R, Aug. 27, 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: 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: 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).

Chemical Weapons Stockpile: Changes Needed in the Management Structure of Emergency Preparedness Program (GAO/NSIAD-97-91, June 11, 1997).

Aviation Security: FAA's Procurement of Explosives Detection Devices (GAO/RCED-97-111R, May 1, 1997).

Aviation Security: Commercially Available Advanced Explosives Detection Devices (GAO/RCED-97-119R, Apr. 24, 1997).

Terrorism and Drug Trafficking: Responsibilities for Developing Explosives and Narcotics Detection Technologies (GAO/NSIAD-97-95, Apr. 15, 1997).

Federal Law Enforcement: Investigative Authority and Personnel at 13 Agencies (GAO/GGD-96-154, Sept. 30, 1996).

Aviation Security: Urgent Issues Need to Be Addressed (GAO/T-RCED/NSIAD-96-151, Sept. 11, 1996).

Terrorism and Drug Trafficking: Technologies for Detecting Explosives and Narcotics (GAO/NSIAD/RCED-96-252, Sept. 4, 1996).

Aviation Security: Immediate Action Needed to Improve Security (GAO/T-RCED/NSIAD-96-237, Aug. 1, 1996).

Terrorism and Drug Trafficking: Threats and Roles of Explosives and Narcotics Detection Technology (GAO/NSIAD/RCED-96-76BR, Mar. 27, 1996).

Nuclear Nonproliferation: Status of U.S. Efforts to Improve Nuclear Material Controls in Newly Independent States (GAO/NSIAD/RCED-96-89, Mar. 8, 1996).

Aviation Security: Additional Actions Needed to Meet Domestic and International Challenges (GAO/RCED-94-38, Jan. 27, 1994).

Nuclear Security: Improving Correction of Security Deficiencies at DOE's Weapons Facilities (GAO/RCED-93-10, Nov. 16, 1992).

Nuclear Security: Weak Internal Controls Hamper Oversight of DOE's Security Program (GAO/RCED-92-146, June 29, 1992).

Electricity Supply: Efforts Underway to Improve Federal Electrical Disruption Preparedness (GAO/RCED-92-125, Apr. 20, 1992).

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are also accepted.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

Orders by visiting:
Room 1100
700 4th St., NW (corner of 4th and G Sts. NW)
Washington, DC 20013

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

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)

PRINTED ON RECYCLED PAPER