United States General Accounting Office

GAO

Testimony

Before the Senate Committee on Governmental Affairs

For Release on Delivery
Expected at 9:30 a.m., EST
Wednesday
October 31, 2001

HOMELAND SECURITY

A Risk Management Approach Can Guide Preparedness Efforts

Statement of Raymond J. Decker
Director, Defense Capabilities and Management

Mr. Chairman and Members of the Committee:

I appreciate the opportunity to be here today to participate in this hearing on security of the U.S. Mail and postal workers. As requested, my testimony will focus on the work we have done over the past five years on combating terrorism and our recommendations advocating a risk management approach for such programs.[1] Risk management is a systematic process to analyze threats, vulnerabilities, and the criticality (or relative importance) of assets to better support key decisions linking resources with prioritized efforts for results.

With the coordinated terrorist attacks against the World Trade Center and the Pentagon on September 11, 2001, terrorism rose to the top of the country's national security and law enforcement agendas. Funding to combat terrorism, which was originally budgeted for just under $13 billion, may now exceed $50 billion for fiscal year 2002. The funds support efforts to mitigate the effects of the attacks, enhance transportation security, support national security, assist the U.S. commercial aviation industry, and can help in a variety of other related purposes. Moreover, as military operations continue in Afghanistan, letters containing the anthrax bacteria have turned up in congressional offices, federal agency buildings, post offices, and several media companies. On October 29, 2001, the Attorney General indicated the need to be prepared for still more terrorist incidents. The threat of such incidents comes with great uncertainty given the changing nature of terrorist attacks over the last decade—ranging from food poisoning in Oregon, to a truck bomb in Oklahoma, to suicide airline hijackings in New York, to anthrax-laced letters in the District of Columbia.

Much of the discussion in today's hearing will focus on the government's response to incidents involving anthrax delivered through the U.S. Mail. Given the recent nature of these incidents and the ongoing investigation, the thrust of current actions will be short-term crisis management and tactical responses. While we have conducted a number of reviews of federal programs to combat terrorism, we have not conducted any detailed reviews of recent actual events. Thus, my testimony will take a more strategic and longer-term view to help guide future programs and responses to combat terrorism and other threats. First, I will provide some background on our past work related to risk management, including our

[1] A list of related GAO products appears at the end of this statement.

recommendations and individual agencies' experiences. Second, I will provide more details on the elements and benefits of risk management as we face new and uncertain challenges.

In our recent capstone report on combating terrorism, we made several recommendations to improve the federal government's ability to combat terrorism.[2] Our key recommendation was implemented on October 8, 2001 when the President signed Executive Order 13228, establishing the Office of Homeland Security as the single focal point for overall leadership and coordination. While we have not reviewed the functions and responsibilities of the newly established Office or the associated Homeland Security Council, we believe that its efforts to develop a national strategy for homeland security should include a risk management approach.

Summary

Since 1996, we have produced more than 60 reports and testimonies on the federal government's efforts to combat terrorism. Several of these reports have recommended that the federal government use risk management as an important element in developing a national strategy. Individual federal agencies have efforts underway, but the results to date have been inconclusive. In September 1999, we recommended that the Department of Justice, specifically the Federal Bureau of Investigation (FBI), conduct threat and other assessments at the national level as part of a risk management approach that could be useful nationwide. In April 1998, we asked Congress to consider requiring that the domestic preparedness program use a risk management approach with state and local governments in preparing state and local governments for terrorist attacks involving weapons of mass destruction. The Department of Justice is working with state and local governments to complete risk management tools for the domestic preparedness program. The Department was nearing completion of these assessments, but has told us they will be delayed by the September 11, 2001, terrorist attacks. However, the FBI has advised us that these will be limited to threat assessments only and will not include other important aspects of risk management that we advocate. In September 2001, we recommended that the Department of Defense (DOD) take steps to improve its risk management approach in force protection through better assessments of threats, vulnerabilities, and

[2]See *Combating Terrorism: Selected Challenges and Related Recommendations* (GAO-01-822, Sept. 20, 2001).

criticality. The DOD concurred with our recommendations and agreed to make changes to strengthen its approach.

Despite these inconclusive results, we continue to believe the federal government can benefit from risk management. Risk management is a systematic and analytical process to consider the likelihood that a threat will endanger an asset (e.g., a structure, individual, or function) and to identify actions that reduce the risk and mitigate the consequences of an attack. An effective risk management approach includes a threat assessment, a vulnerability assessment, and a criticality assessment. A threat assessment identifies and evaluates threats based on various factors, including capability and intentions as well as the potential impact of an event. Nonetheless, we will never know whether we have identified every threat or event and may not have complete information about the threats that we have identified. Consequently, two other elements of the approach, vulnerability assessments and criticality assessments, are essential to prepare better against threats. A vulnerability assessment is a process that identifies weaknesses that may be exploited and suggests options to eliminate or mitigate those weaknesses. A criticality assessment is a process to systematically identify and evaluate an organization's assets based on a variety of factors, including the importance of its mission or function, whether people are at risk, or the significance of a structure or system. Criticality assessments are important because they provide a basis for prioritizing which assets require higher or special protection. A risk management approach can be applied at all levels of activity in our country—from federal agencies to state and local governments and across the public and private sector. The approach that we have described could help our nation prepare against threats that it faces and permit better direction of national finite resources to areas of highest priority. Recent events render it imperative to adopt and implement this risk management approach now.

Background

As demonstrated by the terrorist attacks of September 11, 2001, the United States and other nations face increasingly diffuse threats. Potential adversaries are more likely to strike vulnerable civilian or military targets in nontraditional ways to avoid direct confrontation with our military forces on the battlefield, to try to coerce our government to take some action terrorists desire, or simply to make a statement. Moreover, according to the President's December 2000 national security strategy,[3]

[3] *A National Security Strategy for a Global Age*, December 2000.

such threats are more viable today because of porous borders, rapid technological change, greater information flow, and the destructive power of weapons now within the reach of states, groups, and individuals who may aim to endanger our values, way of life, and the personal security of our citizens.

Hostile nations, terrorist groups, and even individuals may target Americans, our institutions, and our infrastructure with weapons of mass destruction—including biological, chemical, radiological, nuclear, or high explosive weapons. Although they would have to overcome significant technical and operational challenges to make and release many chemical or biological agents of a sufficient quality and quantity to kill large numbers of people, it has been tried, as demonstrated by the current incidents of anthrax-laced letters. Previous attempts have been made such as in 1995 when the Aum Shinrikyo group succeeded in killing 12 people and injuring thousands by releasing the nerve agent sarin in the Tokyo subway. Prior to the Aum Shinrikyo attack, in 1984, the Rajneeshee religious cult in Oregon contaminated salad bars in local restaurants with salmonella bacteria to prevent people from voting in a local election. Although no one died, hundreds of people were diagnosed with food-borne illness.

A fundamental role of the government under our Constitution is to protect America from both foreign and domestic threats. The government must be able to prevent and deter attacks on our homeland as well as detect impending danger before attacks or incidents occur. Although it may not be possible to detect, prevent, or deter every attack, steps can be taken to manage the risk posed by the threats to homeland security.

Risk Management Efforts by Individual Agencies Have Been Inconclusive

We have conducted numerous cross-agency reviews of programs to combat terrorism and have made recommendations that the federal government adopt a risk management approach which could be used at the national as well as the state and local level. Efforts by individual federal agencies related to risk management are underway by the Department of Justice (in conjunction with state governments), the FBI, and DOD. However, the results to date have been inconclusive.

National Level Threat Assessments Approaching Completion

In September 1999, we recommended that the Department of Justice, specifically the FBI, conduct threat and other assessments at the national level as part of a risk management approach that could be useful

nationwide. In response to our report, the FBI agreed to lead two assessments.

The first assessment 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 stockpiles, production capabilities, or funding). Because of limitations on intelligence, the FBI decided to focus on chemical and biological agents. While not identifying specific terrorist groups, this assessment would still be useful in determining requirements for programs to combat terrorism. The FBI is sponsoring this assessment in conjunction with the Department of Justice's National Institute of Justice and the Technical Support Working Group.[4] This assessment will be provided to state and local governments to help them conduct their own risk management assessments. The Department of Justice had estimated that the final assessment would be published in December 2001.

The second 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 this assessment which will encompass domestic terrorism, international terrorism, weapons-of-mass-destruction terrorism, cyber-terrorism, and proliferation of weapons of mass destruction. The report will assess the current threat, the projected threat, emerging threats, and related FBI initiatives. The Department had estimated that this classified assessment would be completed in October 2001.

Department of Justice and FBI officials told us that the September 11 terrorist attacks may dictate revisions to these assessments and delay their completion. While we view both of these assessments as positive, the FBI noted that these would be limited to threat assessments only and will not include other important aspects of risk management that we discuss below.

State and Local Threat Assessments Underway

In April 1998, we asked the Congress to consider requiring the domestic preparedness program—then run by the DOD—to use a risk management approach in its efforts to prepare state and local governments for terrorist

[4] The Technical Support Working Group is the national interagency research and development program for combating terrorism.

attacks involving weapons of mass destruction.[5] The Department of Justice took over that program in fiscal year 2001, and has worked with the FBI to create a risk management tool for state and local governments.[6] This tool includes a step-by-step methodology for assessing threats, risks, and requirements. It also includes information on how to prioritize programs and to project spending amounts. The information from the assessments 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, vulnerabilities, and public health assessments. This design feature enables the program to focus resources on preparing for the most likely scenarios. The Department of Justice plans to use the results of these assessments to drive the allocation of its resources for equipment, training, and exercise programs, consistent with our recommendation. According to Department of Justice officials, these assessments have been completed by four states—Rhode Island, South Carolina, Hawaii, and Utah.

DOD Uses a Risk Management Approach in Antiterrorism Efforts

In September 2001, we recommended that the DOD take steps to improve its risk management approach in its force protection efforts through better assessments of threats, vulnerabilities, and criticality.[7] Regarding DOD's threat assessments, we recommended that the Department expand its methodology to increase the awareness of the consequences of changing business practices at installations that may create workplace violence situations or new opportunities for individuals not affiliated with the DOD to gain access to installations. We also recommended that installation commanders form threat working groups and personally and actively engage state, local, and federal law enforcement officials to provide threat information from these sources on a regular basis. The Department agreed with these recommendations and stated it would review its methodology to ensure that no threat indicators are overlooked and that it would

[5] The domestic preparedness program, originally conducted by the DOD, was directed by the Defense Against Weapons of Mass Destruction Act of 1996 (P.L. 104-201, Sept. 23, 1996). The program also was known as the Nunn-Lugar-Domenici program, named after the senators who authored the original bill.

[6] 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.

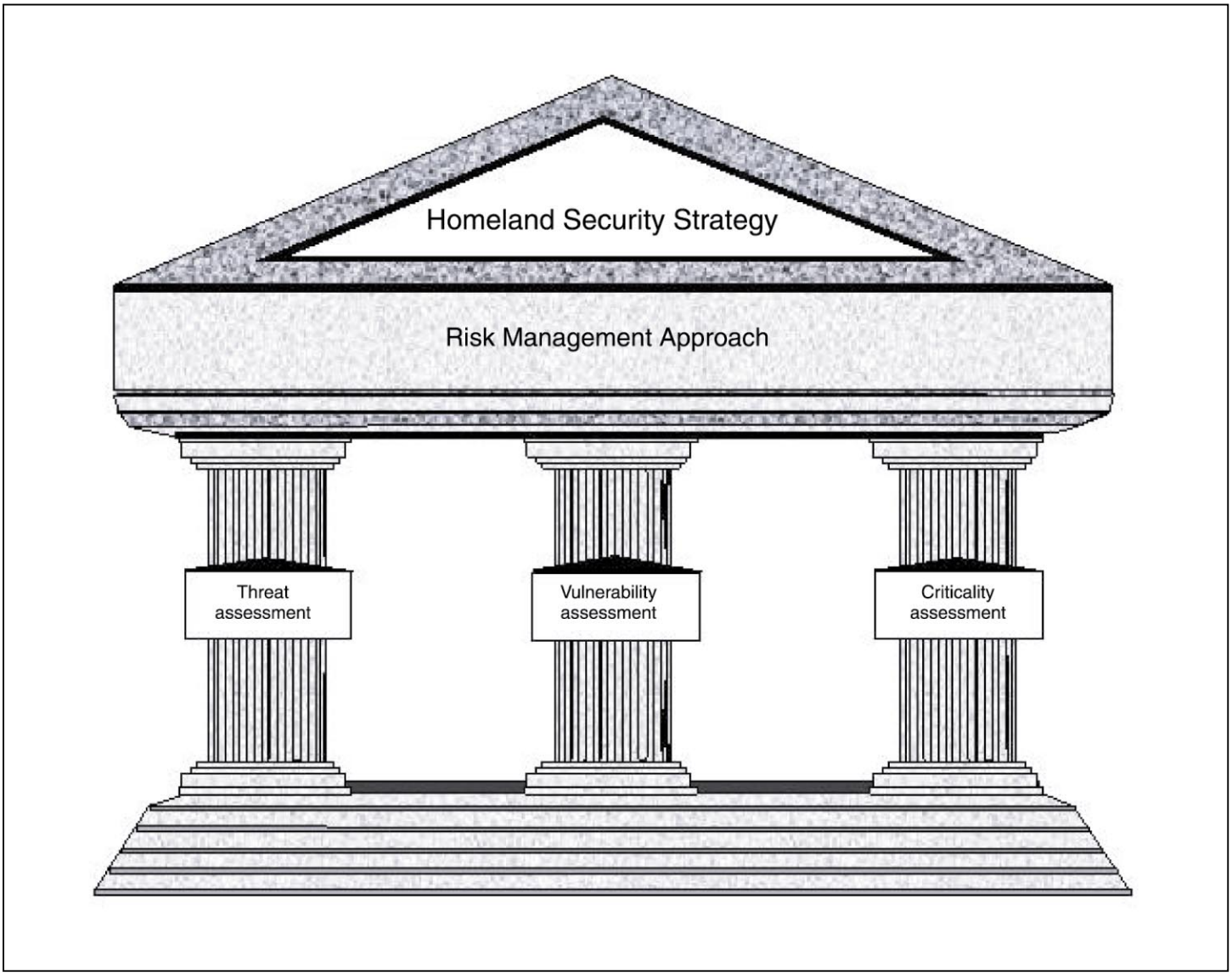
[7] *Combating Terrorism: Actions Needed to Improve DOD Antiterrorism Program Implementation and Management* (GAO-01-909, Sept. 19, 2001).

require installation commanders to establish threat working groups. To improve its vulnerability assessments, we recommended that DOD identify those installations that serve a critical role in support of our national military strategy, and ensure that that they receive a vulnerability assessment. We further recommended that the Department develop a strategy to conduct vulnerability assessments at National Guard installations and develop a mechanism to record and track all vulnerability assessments conducted. DOD agreed with these recommendations and is changing its program standards and procedures to implement these recommendations. Regarding criticality assessments, we recommended that DOD require criticality assessments be done at all installations. DOD agreed with this recommendation and has revised its program standards to require this assessment.

A Risk Management Approach Can Guide Preparedness Efforts

Risk management is a systematic, analytical process to consider the likelihood that a threat will harm an asset or individuals and to identify actions that reduce the risk and mitigate the consequences of an attack or event. Risk management principles acknowledge that while risk generally cannot be eliminated, enhancing protection from known or potential threats can reduce it. As described in detail below, a risk management approach can have three elements: assessments of threat, vulnerabilities, and criticality (or relative importance). This general approach is used or endorsed by federal agencies, government commissions, and multi-national corporations. Figure 1 below is a graphical representation of the risk management approach we discuss.

Figure 1: Risk Management Approach



Source: GAO analysis.

Threat Assessments Are an Important First Step

A threat assessment is used to evaluate the likelihood of terrorist activity against a given asset. It is a decision support tool that helps to establish and prioritize security-program requirements, planning, and resource allocations. A threat assessment identifies and evaluates each threat on the basis of various factors, including capability, intention, and impact of

an attack. Intelligence and law enforcement agencies assess the foreign and domestic terrorist threats to the United States. The U.S. intelligence community—which includes the Central Intelligence Agency, the Defense Intelligence Agency, and the State Department's Bureau of Intelligence and Research, among others—monitors the foreign-origin terrorist threat to the United States. The FBI gathers information and assesses the threat posed by domestic sources of terrorism. Threat information gathered by both the intelligence and law enforcement communities can produce threat assessments for use in national security strategy planning.

Several federal government organizations as well as companies in the private sector apply some formal threat assessment process in their programs, or such assessments have been recommended for implementation. For example, DOD uses threat assessments for its antiterrorism program designed to protect military installations. DOD evaluates threats on the basis of several factors, including a terrorist group's intentions, capabilities, and past activities. The assessments provide installation commanders with a list of credible threats that can be used in conjunction with other information (such as the state of the installation's preparedness) to prepare against attack, to recover from the effects of an attack, and to adequately target resources.

Similarly, the Interagency Commission on Crime and Security in U.S. Seaports reported that threat assessments would assist seaports in preparing for terrorist threats. [8] The Commission recommended that the federal government establish baseline threat assessments for terrorism at U.S. seaports and, thereafter, conduct these assessments every 3 years. Additionally, a leading multi-national oil company attempts to identify threats in order to decide how to manage risk in a cost-effective manner. Because the company operates overseas, its facilities and operations are exposed to a multitude of threats, including terrorism, political instability, and religious or tribal conflict. In characterizing the threat, the company examines the historical record of security and safety breaches and obtains location-specific threat information from government organizations and other sources. It then evaluates these threats in terms of company assets that represent likely targets.

[8] *Report of the Interagency Commission on Crime and Security in U.S. Seaports*, Fall 2000.

While threat assessments are key decision support tools, it should be recognized that, even if updated often, threat assessments might not adequately capture emerging threats posed by some terrorist groups. No matter how much we know about potential threats, we will never know that we have identified every threat or that we have complete information even about the threats of which we are aware. Consequently, we believe that a risk management approach to prepare for terrorism with its two additional assessments, discussed below, can provide better assurance of preparedness for a terrorist attack.

Vulnerability Assessments Are a Way to Identify Weaknesses

A vulnerability assessment is a process that identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may be exploited by terrorists and may suggest options to eliminate or mitigate those weaknesses. For example, a vulnerability assessment might reveal weaknesses in an organization's security systems, financial management processes, computer networks, or unprotected key infrastructure such as water supplies, bridges, and tunnels. In general, these assessments are conducted by teams of experts skilled in such areas as engineering, intelligence, security, information systems, finance, and other disciplines. For example, at many military bases, experts have identified security concerns including the distance from parking lots to important buildings as being so close that a car bomb detonation would damage or destroy the buildings and the people working in them. To mitigate this threat, experts have advised that the distance between parking lots and some buildings be increased. Another security enhancement might be to reinforce the windows in buildings to prevent glass from flying into the building if an explosion occurs.

The Seaport Commission recommended similar vulnerability assessments be conducted. It identified factors to be considered that include the accessibility of vessels or facilities, avenues of ingress and egress, and the ease of access to valuable or sensitive items such as hazardous materials, arms, ammunition, and explosives. For private sector companies, such assessments can identify vulnerabilities in the company's operations, personnel security, and physical and technical security.

With information on both vulnerabilities and threats, planners and decision-makers are in a better position to manage the risk of a terrorist attack by more effectively targeting resources. However, risk and vulnerability assessments need to be bolstered by a criticality assessment, which is the final major element of the risk management approach. Because we may not be able to afford the same level of protection for all

vulnerable assets, it is necessary to prioritize which are most important and thus would get the highest level of protection.

Criticality Assessments Are Necessary to Prioritize Assets for Protection

A criticality assessment is a process designed to systematically identify and evaluate important assets and infrastructure in terms of various factors, such as the mission and significance of a target. For example, nuclear power plants, key bridges, and major computer networks might be identified as "critical" in terms of their importance to national security, economic activity, and public safety. In addition, facilities might be critical at certain times, but not others. For example, large sports stadiums, shopping malls, or office towers when in use by large numbers of people may represent an important target, but are less important when they are empty. Criticality assessments are important because they provide a basis for identifying which assets and structures are relatively more important to protect from an attack. The assessments provide information to prioritize assets and allocate resources to special protective actions. These assessments have considered such factors as the importance of a structure to accomplish a mission, the ability to reconstitute this capability, and the potential cost to repair or replace the asset.

The Seaports Commission has identified potential high-value assets (such as production, supply, and repair facilities; transfer, loading, or storage facilities; transportation modes; and transportation support systems) that need to be included in a criticality analysis, but it reported that no attempt has been made to identify the adverse effect from the loss of such assets. To evaluate the risk to an asset, the Seaports Commission advised that consideration be given to the mission and the military or economic impact of its loss or damage. The multi-national company we reviewed uses descriptive values to categorize the loss of a structure as catastrophic, critical, marginal, or negligible. It then assigns values to its key assets. This process results in a matrix that ranks as highest risk, the most important assets with the threat scenarios it believes are most likely to occur.

Conclusion

Some federal agencies have taken steps related to risk management, but the results have been inconclusive. We continue to believe that risk management is the best approach to guide programs and responses to better prepare against terrorism and other threats. After threat, vulnerability, and criticality assessments have been completed and evaluated in this risk-based decision process, key actions can be taken to better prepare ourselves against potential attacks or events. Threat assessments alone are insufficient to support the key judgments and

decisions that must be made. However, in conjunction with vulnerability and criticality assessments, leaders and managers can make better decisions based on this risk management approach. If the federal government were to apply this approach universally and if similar approaches were adopted by other segments of society, we could more effectively and efficiently prepare in-depth defenses against acts of terrorism and other threats directed against our country. Without a risk management approach, there is little assurance that programs to combat terrorism are prioritized and properly focused.

This concludes my prepared statement. I will be pleased to respond to any questions you or other members of the Committee may have.

Contacts and Acknowledgements

For further information about this testimony, please contact me at (202) 512-6020. Stephen L. Caldwell, Brian J. Lepore, Mark A. Pross, Lorelei St. James, and Lee Purdy also made key contributions to this statement.

Related GAO Products

Terrorism Insurance: Alternative Programs for Protecting Insurance Consumers (GAO-02-199T, Oct. 24, 2001).

Terrorism Insurance: Alternative Programs for Protecting Insurance Consumers (GAO-02-175T, Oct. 24, 2001).

Combating Terrorism: Considerations for Investing Resources in Chemical and Biological Preparedness (GAO-02-162T, Oct. 17, 2001).

Homeland Security: Need to Consider VA's Role in Strengthening Federal Preparedness (GAO-02-145T, Oct. 15, 2001).

Homeland Security: Key Elements of a Risk Management Approach (GAO-02-150T, Oct. 12, 2001).

Bioterrorism: Review of Public Health Preparedness (GAO-02-149T, Oct. 10, 2001).

Bioterrorism: Public health and Medical Preparedness (GAO-02-141T, Oct. 9, 2001).

Bioterrorism: Coordination and Preparedness (GAO-02-129T, Oct. 5, 2001).

Bioterrorism: Federal Research and Preparedness Activities (GAO-01-915, Sept. 28, 2001).

Homeland Security: A Framework for Addressing the Nation's Issues (GAO-01-1158T, Sept. 21, 2001).

Combating Terrorism: Selected Challenges and Related Recommendations (GAO-01-822, Sept. 20, 2001).

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

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

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

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

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

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

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

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

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

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

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

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

Combating Terrorism: 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).