United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at
10:00 a.m., EDT
Friday
October 12, 2001

HOMELAND SECURITY

Key Elements of a Risk Management Approach

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 discuss with you an approach to manage the risk from terrorism directed at Americans in our homeland. With the initiation of military operations against terrorist targets in Afghanistan, senior government officials indicated the need to be prepared for the potential of another attack on our homeland. There may be ways to prepare better in the event such an attack does come. We have undertaken a body of work in the area of combating terrorism, which has evaluated various facets of federal efforts to address this challenge. From this work, we identified three essential elements in an effective risk management approach to prepare better against acts of terrorism. My testimony today will focus on the three key elements that the federal government as well as state and local governments and private entities should adopt to enhance their timely preparedness against potential threats.

Summary

Risk management is a systematic and analytical process to consider the likelihood that a threat will endanger an asset, individual, or function and to identify actions to reduce the risk and mitigate the consequences of an attack. Risk management principles acknowledge that while risk generally cannot be eliminated, enhancing protection from known or potential threats can reduce it. A good risk management approach includes three primary elements: a threat assessment, a vulnerability assessment, and a criticality assessment. Threat assessments are important decision support tools that can assist organizations in security-program planning and key efforts. A threat assessment identifies and evaluates threats based on various factors, including capability and intentions as well as the potential lethality of an attack. Over the past several years, we have recommended that a comprehensive, national threat assessment be conducted by the appropriate federal agencies. Nonetheless, we will never know whether we have identified every threat, nor will we have complete information about the threats that we have identified. Consequently, we believe that the two other elements of the approach, vulnerability assessments and criticality assessments, are essential and required to prepare better against terrorist attacks. A vulnerability assessment is a process that identifies weaknesses that may be exploited by terrorists and suggests options to eliminate or mitigate those weaknesses. A criticality assessment is a process designed to systematically identify and evaluate an organization's assets based on the importance of its mission or function, the group of people at risk, or the significance of a structure. Criticality assessments are important because they provide a basis for prioritizing which assets and structures require higher or special protection from an attack. The

approach that we have described could help prepare us against the threat we face and permit better direction of our resources to areas of highest priority.

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,[1] 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, the possibility exists that it could be done and it has been attempted. For example, in 1995, 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.

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

A Risk Management Approach Can Help Prepare Against Terrorism

Risk management is a systematic, analytical process to consider the likelihood that a threat will harm an asset or individuals and to identify actions to reduce the risk and mitigate the consequences on an attack. Risk management principles acknowledge that while risk generally cannot be eliminated, enhancing protection from known or potential threats can reduce it.

A risk management approach exists that may be used to enhance our level of preparedness for terrorist threats. This approach is based on assessments of threat, vulnerabilities, and criticality (importance). A variation of this approach is currently used by DOD, which we discuss in our September 2001 report on combating terrorism.[2] One of the largest U.S. multi-national corporations uses another variation of the approach. In addition, the Interagency Commission on Crime and Security in U.S. Seaports has proposed a similar approach to assess the security of U.S. seaports.

Threat Assessments Are An Important Step in Implementing the Approach

A threat assessment is used to evaluate the likelihood of terrorist activity against a given asset or location. 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 lethality 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 (CIA), 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. By identifying and assessing threats, organizations do not have to rely on worst-case scenarios to guide planning and resource allocations. Worst-case scenarios tend to focus on vulnerabilities, which are virtually unlimited, and would require extraordinary resources to address. Therefore, in the absence of detailed threat data, it is essential that a careful balance exists using all three elements in preparing and protecting against threats.

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

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. In 1999, and again in our recent report on combating terrorism, we recommended that the FBI prepare a formal intelligence assessment that specifically assesses the chemical and biological agents that could be used by domestic terrorists without the assistance or support of a foreign laboratory.[3] The FBI concurred and expects to complete its assessment in December 2001, although it noted a limitation in its methodology. The FBI stated that its law enforcement role placed limitations on its collection and use of intelligence data, and the Bureau added that it had little intelligence on specific domestic terrorist groups. We also recommended that the FBI sponsor a national-level threat assessment that uses both intelligence estimates[4] and inputs from the intelligence community and others to form the basis for, and to prioritize, programs developed to combat terrorism. The FBI concurred and stated last month that the assessment is being finalized. This latter assessment is expected to be classified. The Department of Defense (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 to their installations and 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, 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

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

[4] A national intelligence estimate analyzes issues of major importance and long-term interest to the United States and is the intelligence community's most authoritative projection of future developments in a particular subject area.

that represent likely targets. Additionally, the Interagency Commission on Crime and Security in U.S. Seaports reported that threat assessments would assist seaports in preparing for terrorist threats. [5] 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.

While threat assessments are a key decision support tool, 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 preparing for terrorism with its two additional assessments 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, DuringDAA a vulnerability assessment might reveal weaknesses in an organization's security systems 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.

For private sector companies, such assessments can identify vulnerabilities in the company's operations, personnel security, and physical and technical security. The Seaport Commission recommended

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

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. 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.

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. 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 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 most likely to occur. The Seaports Commission has also 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 affect 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.

Conclusion

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 terrorist attacks. Threat assessments alone are insufficient to support the key judgements and decisions that must be made. However, in conjunction with vulnerability and criticality assessments, leaders and managers will 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 against our country.

This concludes my prepared statement. I will be pleased to respond to any questions you may have.

Related GAO Products

Homeland Security

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

Combating Terrorism

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).

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).