United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Transportation Security and Infrastructure Protection, Homeland Security Committee, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Wednesday, June 25, 2008

RISK MANAGEMENT

Strengthening the Use of Risk Management Principles in Homeland Security

Statement of Norman J. Rabkin, Managing Director, Homeland Security and Justice

June 25, 2008

RISK MANAGEMENT

Strengthening the Use of Risk Management Principles in Homeland Security

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-08-904T, a testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Homeland Security Committee, House of Representatives

Why GAO Convened This Forum

From the terrorist attacks of September 11, 2001, to Hurricane Katrina, homeland security risks vary widely. The nation can neither achieve total security nor afford to protect everything against all risks. Managing these risks is especially difficult in today's environment of globalization, increasing security interdependence, and growing fiscal challenges for the federal government. Broadly defined, risk management is a process that helps policymakers assess risk, strategically allocate finite resources, and take actions under conditions of uncertainty.

GAO convened a forum of 25 national and international experts on October 25, 2007, to advance a national dialogue on applying risk management to homeland security. Participants included federal, state, and local officials and risk management experts from the private sector and academia.

Forum participants identified (1) what they considered to be effective risk management practices used by organizations from the private and public sectors and (2) key challenges to applying risk management to homeland security and actions that could be taken to address them. Comments from the proceedings do not necessarily represent the views of all participants, the organizations of the participants, or GAO. Participants reviewed a draft of this report and their comments were incorporated, as appropriate.

To view the full product, click on GAO-08-904T. For more information, contact Norman J. Rabkin at (202) 512-8777 or rabkinn@gao.gov.

What Participants Said

Forum participants identified what they considered to be effective public and private sector risk management practices. For example, participants discussed the private sector use of a chief risk officer, though they did not reach consensus on how to apply the concept of the chief risk officer to the public sector. One key practice for creating an effective chief risk officer, participants said, was defining reporting relationships within the organization in a way that provides sufficient authority and autonomy for a chief risk officer to report to the highest levels of the organization. Participants stated that the U.S. government needs a single risk manager. One participant suggested that this lack of central leadership has resulted in distributed responsibility for risk management within the administration and Congress and has contributed to a lack of coordination on spending decisions. Participants also discussed examples of public sector organizations that have effectively integrated risk management practices into their operations, such as the U.S. Coast Guard, and compared and contrasted public and private sector risk management practices.

According to the participants at our forum, three key challenges exist to applying risk management to homeland security: improving risk communication, political obstacles to risk-based resource allocation, and a lack of strategic thinking about managing homeland security risks. Many participants agreed that improving risk communication posed the single greatest challenge to using risk management principles. To address this challenge, participants recommended educating the public and policymakers about the risks we face and the value of using risk management to establish priorities and allocate resources; engaging in a national discussion to reach a public consensus on an acceptable level of risk; and developing new communication practices and systems to alert the public during an emergency. In addition, to address strategic thinking challenges, participants recommended the government develop a national strategic planning process for homeland security and governmentwide risk management guidance. To improve public-private sector coordination, forum participants recommended that the private sector should be more involved in the public sector's efforts to assess risks and that more state and local practitioners and experts be involved through intergovernmental partnerships.

Madam Chairwoman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on the use of risk management principles in homeland security. As shown by the terrorist attacks of September 11, 2001, and Hurricane Katrina, homeland security risks vary widely. The nation can neither achieve total security nor afford to protect everything against all risks. Managing these risks is especially difficult in today's environment of globalization, increasing security interdependence, and growing fiscal challenges for the federal government. It is increasingly important that organizations effectively target homeland security funding—totaling nearly $65 billion in 2008 federal spending alone—to address the nation's most critical priorities.

Using principles of risk management can help policymakers reach informed decisions regarding the best ways to prioritize investments in security programs so that these investments target the areas of greatest need. Broadly defined, risk management is a strategic process for helping policymakers make decisions about assessing risk, allocating finite resources, and taking actions under conditions of uncertainty. The Department of Homeland Security (DHS) has established a risk management framework to help the department target its investments in security programs based on risk. This framework defines risk as a function of threat, vulnerability, and consequence, or, in other words, a credible threat of attack on a vulnerable target that would result in unwanted consequences.

Our prior work has shown that using risk management principles to prioritize which programs to invest in and to measure the extent to which such principles mitigate risk is a challenging endeavor. For this reason, to assist both Congress and federal agencies, including DHS, GAO convened an expert panel to advance the national dialogue on strengthening the use of risk management principles to manage homeland security programs. Today, I'll discuss the highlights of our panel's thoughts on the issues we asked them to identify: (1) effective risk management practices used by organizations from the public and private sectors and (2) key challenges faced by public and private organizations in adopting and implementing a risk-based approach to manage homeland security programs and actions that could be taken to address them.

Summary

Participants identified effective public and private sector risk management practices. For example, participants discussed the private sector use of the chief risk officer. However, participants discussed but did not reach

consensus on how to apply this concept of a chief risk officer to the public sector. They also discussed examples of public sector organizations that have effectively integrated risk management practices into their operations, such as the U.S. Coast Guard, and compared and contrasted public and private sector risk management practices.

According to the participants at our forum, three key challenges exist to applying risk management to homeland security: improving risk communication, political obstacles to allocating resources based on a consideration of risk, and a lack of strategic thinking about managing homeland security risks. Many participants, 35 percent, agreed that improving risk communication posed the single greatest challenge to using risk management principles. Further, 19 percent of participants stated political obstacles to risk-based resource allocation was the single most critical challenge, and the same number of participants, 19 percent, said the single most critical challenge was a lack of strategic thinking. The remaining participants identified other key challenges, for example, technical issues such as the difficult but necessary task of analyzing threat, vulnerability, and consequences of a terrorist attack in order to assess risk; partnership and coordination challenges; and the need for risk management education.

The expert panel also identified ways to address some of these challenges. To better communicate about risks, participants recommended that we educate the public and policymakers about the risks we face and the value of using risk management to establish priorities and allocate resources; engage in a national discussion to reach a public consensus on an acceptable level of risk; and develop new communication practices and systems to alert the public during an emergency. To better allocate resources based on risk, participants recommended that public officials and organizations consider investing in protective measures that yield long-term benefits. In addition, to address strategic thinking challenges, participants recommended the government develop a national strategic planning process for homeland security and governmentwide risk management guidance. To improve public-private sector coordination, forum participants recommended that the private sector should be more involved in the public sector's efforts to assess risks and that more state and local practitioners and experts be involved through intergovernmental partnerships.

Background

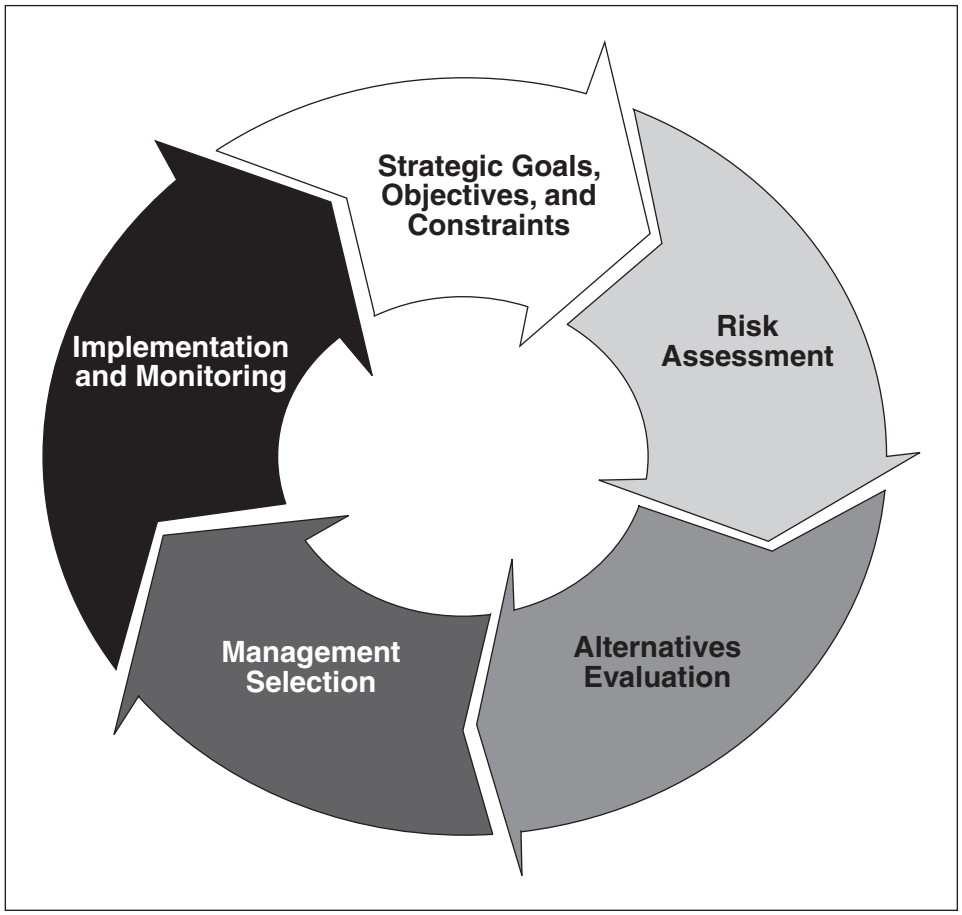
The Comptroller General convened this expert panel from the U.S. and abroad to advance a national dialogue on strengthening the use of risk management principles to better manage homeland security programs. The forum brought together a diverse array of experts from the public and private sectors, including, from the public sector, a former governor, a former DHS under secretary, a U.S. Coast Guard Admiral, and senior executives from DHS, the U.S. Army, and the National Intelligence Council, as well as state and local officials with homeland security responsibilities. From the private sector, participants included executives from leading multinational corporations such as Swiss Re, Westfield Group, JPMorgan Chase, and Wal-Mart. In addition, several of the world's leading scholars from major universities, the National Research Council, and the RAND Corporation participated in the forum. (See app. I for a list of participants.)

Recognizing that risk management helps policymakers make informed decisions, Congress and the administration have charged federal agencies to use a risk-based approach to prioritize resource investments. Nevertheless, federal agencies often lack comprehensive risk management strategies that are well integrated with program, budget, and investment decisions. To provide a basis for analyzing these strategies, GAO has developed a risk management framework[1] based on industry best practices and other criteria. This framework, shown in figure 1, divides risk management into five major phases: (1) setting strategic goals and objectives, and determining constraints; (2) assessing risks;[2] (3) evaluating alternatives for addressing these risks; (4) selecting the appropriate alternatives; and (5) implementing the alternatives and monitoring the progress made and results achieved.

[1]For a description of this framework, see Appendix I of GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005).

[2]Risk assessment is the process of qualitatively or quantitatively determining the probability of an adverse event and the severity of its impact on an asset.

Figure 1: GAO Risk Management Framework



Source: GAO.

Our work has indicated that while DHS is making progress in applying risk management principles to guide its operational and resource allocation decisions, challenges remain. GAO has assessed DHS's risk management efforts across a number of mission areas—including transportation security, port security, border security, critical infrastructure protection, and immigration enforcement—and found that risk management principles have been considered and applied to varying degrees. For example, in June 2005 we reported that the Coast Guard had developed security plans for seaports, facilities, and vessels based on risk

assessments.[3] However, other components had not always utilized such an approach. As we reported in August 2007, while the Transportation Security Administration has developed tools and processes to assess risk within and across transportation modes, it had not fully implemented these efforts to drive resource allocation decisions.[4] Moreover, in February 2007, we reported that DHS faced substantial challenges related to strengthening its efforts to use information on risk to inform strategies and investment decisions, for example, by integrating a consideration of risk into annual budget and program review cycles.[5] We also reported that while integrating a risk management approach into decision-making processes is challenging for any organization, it is particularly difficult for DHS given its diverse set of responsibilities. The department is responsible for dealing with all-hazards homeland security risks—ranging from natural disasters to industrial accidents and terrorist attacks. The history of natural disasters has provided experts with extensive historical data that are used to assess risks. By contrast, data about terrorist attacks are comparatively limited, and risk management is complicated by the asymmetric and adaptive nature of our enemies.

In addition to helping federal agencies like DHS focus their efforts, risk management principles can help state and local governments and the private sector—which owns over 85 percent of the nation's critical infrastructure—prioritize their efforts to improve the resiliency of our critical infrastructure and make it easier for the nation to rebound after a catastrophic event. Congress has recognized state and local governments and the private sector as important stakeholders in a national homeland security enterprise and has directed federal agencies to foster better information sharing with these partners. Without effective partnerships, the federal government alone will be unable to meet its responsibilities in protecting and securing the homeland. A shared national approach—among federal, state, and local governments as well as between public and private sectors—is needed to manage homeland security risk.

[3]GAO, *Strategic Budgeting: Risk Management Principles Can Help DHS Allocate Resources To Highest Priorities*, GAO-05-824T (Washington, D.C.: June 29, 2005).

[4]GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-454 (Washington, D.C.: Aug. 17, 2007).

[5]GAO, *Homeland Security: Applying Risk Management Principles to Guide Federal Investments*, GAO-07-386T (Washington, D.C.: Feb. 7, 2007).

Identifying Effective Risk Management Practices in the Private and Public Sectors

Participants discussed effective risk management practices used in the public and private sector. For example, they discussed the concept of a chief risk officer but did not reach consensus on how to apply the concept to the public sector. The participants also identified examples of public sector organizations that effectively integrated risk management into their operations and compared and contrasted public and private sector risk management practices.

Chief Risk Officer

Participants said that private sector organizations have established the position of the chief risk officer, an executive responsible for focusing on understanding information about risks and reporting this information to senior executives. One key practice for creating an effective chief risk officer, participants said, was defining reporting relationships within the organization in a way that provides sufficient authority and autonomy for a chief risk officer to report to the highest levels of the organization. However, participants did not reach consensus on how to apply the concept of the chief risk officer to the public sector. Participants stated that the U.S. government needs a single risk manager. One participant suggested that this lack of central leadership has resulted in distributed responsibility for risk management within the administration and Congress and has contributed to a lack of coordination on spending decisions.

Another participant stated that the Secretary of DHS fills the chief risk officer role. Participants identified various challenges associated with appointing a chief risk officer within the public sector, including (1) balancing the responsibilities for protection against seizing opportunities for long-range risk reduction, (2) creating a champion but not another silo that is not integrated with other components of the organization, and (3) generating leadership support for the position.

Integration of Risk Management Principles into Public Sector Operations

Participants identified examples of organizations that effectively integrated risk management into the operations of public sector organizations, including the U.S. Coast Guard, the U.S. Army Corps of Engineers, and the Port Authority of New York and New Jersey. Participants stated that the Coast Guard uses risk management principles to allocate resources, balance competing needs of security with the efficient flow of commerce, and implement risk initiatives with its private sector partners, for example, through Area Maritime Security Committees. According to another participant, the Army Corps developed flood risk management practices that he saw as notable because this information

was used to digest and share critical information with the public. One participant noted that the Port Authority of New York and New Jersey developed and implemented a risk assessment program that guided the agency's management in setting priorities for a 5-year, $500 million security capital investment program. According to this participant, this methodology has since been applied to over 30 other transportation and port agencies across the country, and the Port Authority has moved from conducting individual risk assessments to implementing an ongoing program of risk management.

Comparing and Contrasting Public and Private Sector Risk Management Practices

Participants observed that while, in some instances, the public and private sector should apply risk management principles in similar ways, in other instances, the public and private sectors manage risk differently. One participant stated in both the public and private sectors the risk management process should include the systematic identification and assessment of risks through scientific efforts; efforts to mitigate risks; and risk adaptation to address financial consequences or to allow for effective transfer of risk. However, participants noted that the private and public sectors also manage risk differently. One participant said the private sector manages risk by "pre-funding" and diversifying risk through insurance. In addition, the private sector creates incentives for individuals to lower the risks they face from, for example, a car accident or a natural disaster, by offering to reduce insurance premiums if the policy holder takes certain steps to mitigate these risks. Similarly, the public sector also plays a unique role in managing risk, for instance, regulating land use and establishing building codes; organizing disaster protection, response, and recovery measures; setting regulatory frameworks; and supplementing the insurance industry.

In addition, participants noted that the private sector organizations have more flexibility than the public sector to select which risks to manage. For instance, participants stated that the private sector could avoid risks in cases where the costs of ensuring these risks are too high. Additionally, a participant noted that the private sector tends to naturally consider opportunity analysis—or the process of identifying and exploring situations to better position an organization to realize desirable objectives—as an important part of risk management. In contrast, participants observed, public sector organizations have less flexibility to select which risks to address through protective measures. Like the private sector, the government has to makes choices about which risks to protect against—since it cannot protect the nation against all hazards. Unlike the private sector, the government has a wide responsibility for

preparing for, responding to, and recovering from all acts of terrorism and natural or manmade disasters and is accountable to the public for the investment decisions it makes.

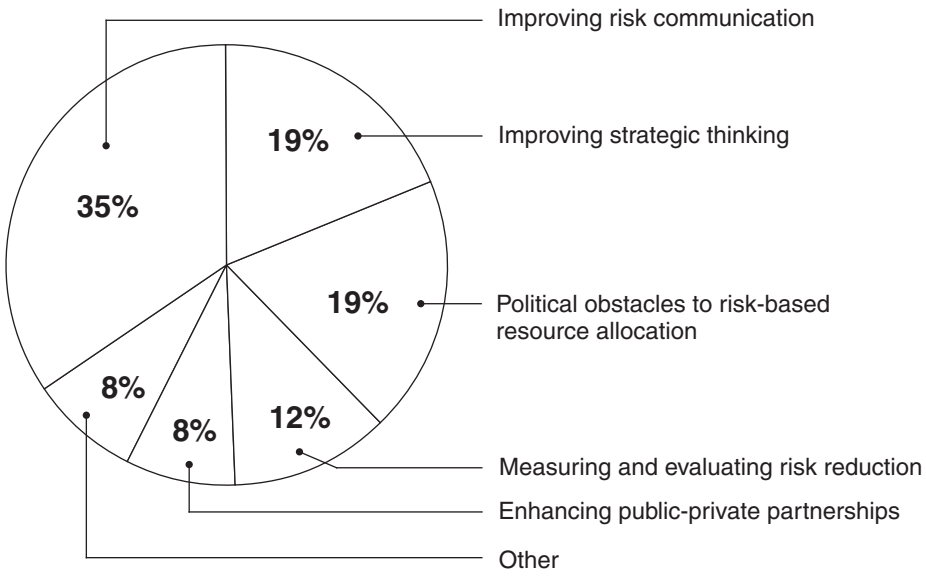
Identifying and Addressing the Most Critical Homeland Security Risk Management Challenges

Participants identified three key challenges to strengthening the use of risk management in homeland security—risk communication, political obstacles to making risk-based investments, and a lack of strategic thinking. Participants also recommended ways to address them.

Key Challenges

Many participants, 35 percent, agreed that improving risk communication posed the single greatest challenge to using risk management principles (see fig. 2 below). Further, 19 percent of participants stated political obstacles to risk-based resource allocation was the single most critical challenge, and the same proportion of participants, 19 percent, said the single most critical challenge was a lack of strategic thinking. The remaining participants identified other key challenges, for example, technical issues such as the difficult but necessary task of analyzing threat, vulnerability, and consequences of a terrorist attack in order to assess and measure risk reduction; and partnership and coordination challenges.

Figure 2: Key Challenges in Applying Risk Management to Homeland Security



Source: GAO analysis of participants' forum polling responses.

Risk Communication Challenges

Participants identified several risk communication challenges and recommended actions to address them as follows:

- *Educate the public about risks and engage in public discourse to reach consensus on an acceptable level of risk.* Participants said that the public lacks a fact-based understanding of what homeland security risks the nation faces. Participants attributed these problems to media coverage that undermines a fact-based public discussion of risk by sensationalizing acts of terrorism that have dramatic consequences but may be unlikely to occur. In addition, participants stated that even though it is not possible to prevent all disasters and catastrophes, public officials need to engage the public in defining an acceptable level of risk of a terrorist attack or natural disaster in order to make logical, risk-based resource allocation decisions. To communicate with the public about risks in a meaningful way, participants recommended educating the public on how risk is defined, providing fact-based information on what risks we face and the probability they might occur, and explaining how risk informs decision-making. One expert recommended the government communicate about risks through public outreach in ways that calms the public's fears while raising awareness of risks. Another participant recommended that the country

engage in a national public discourse to reach consensus on an acceptable level of risk.

- *Educate policymakers and establish a common lexicon for discussing risk.* Participants emphasized the importance of educating elected officials on risk management. Several participants believed that the distinction between risk assessment—involving scientific analysis and modeling—and risk management—involving risk reduction and evaluation—is not widely understood by policymakers. In addition, one expert also noted that the nation should do more to train a cadre of the next generation of risk management professionals. Given differences in education and levels of understanding about risk management, the participants felt it would be important to develop a common lexicon that can be used for dialogue with both the layman and the subject matter expert. Without a common, shared understanding of risk management terms, communicating about risks is challenging. Some members of our expert panel recommended focusing specifically on educating elected officials and the next generation of policymakers about risk management. One participant pointed out that a new administration and Congress will soon enter office with a new set of policy objectives, and it will be important to highlight the importance of risk management to incoming policymakers and to persuade them to discuss it. Panelists also recommended creating a common vocabulary or lexicon that defines common risk management terms.

- *Develop new risk communication practices to alert the public during emergencies*. Participants said that government officials lack an understanding of what information to share and how to communicate with the public during an emergency. Participants said that risk analysis, including predictive modeling, tends to neglect a consideration of how the public's expectations and emotions can impact the effectiveness of response efforts and affect the likelihood the public will respond as predicted or directed by government officials during an emergency. According to one participant, Hurricane Katrina demonstrated that the efficacy of emergency response efforts depends on how the public behaves, as some people chose to shelter in place while others followed directions to evacuate. Participants recommended that governments consider what information should be communicated to the public during a crisis and how best to communicate that information. For instance, one participant suggested that experts look at existing risk communication systems, such as the National Weather Service, that could be used as models for a homeland security risk communication system. The participant noted that the service provides both national and local weather information, looks at overall risks, and effectively provides actionable

information to be used by both the public and private sectors. Participants criticized the current color-coded DHS Homeland Security Advisory System as being too general, suggesting that the public does not understand what is meant by the recommended actions such as being vigilant.

Political Obstacles to Risk-Based Resource Allocation

Participants said political obstacles pose challenges to allocating homeland security resources based on risk. Participants identified the reluctance of politicians and others to make risk-based funding decisions. Participants noted that elected officials' investment priorities are informed by the public's beliefs about which risks should be given the highest priority, beliefs that are often based on incomplete information. As a result, participants stated that there is less incentive for officials to invest in long-term opportunities to reduce risk, such as investing in transportation infrastructure, when the public does not view these investments as addressing a perceived risk. To better allocate resources based on risk, participants recommended that public officials and organizations consider investing in protective measures that yield long-term benefits.

Need to Improve Strategic Thinking

Participants agreed that a lack of strategic thinking was a key challenge to incorporating risk-based principles in homeland security investments. In particular, participants noted that challenges existed in these areas:

- *A national strategic planning process is needed to guide federal investments in homeland security*. Participants said there is a lack of a national strategic planning process to guide federal investments in homeland security. Balancing the security concerns of various federal government agencies that have diverse missions in areas other than security, such as public safety and maintaining the flow of commerce, poses a significant strategic challenge, some participants stated. One participant stated that the President had developed a strategy to guide, organize, and unify the nation's homeland security efforts in the October 2007 National Strategy for Homeland Security. However, several other participants said that a better process is needed for strategic planning. For example, to think strategically about risk they recommended that stakeholders discuss trade-offs, such as whether more resources should be spent to protect against risks from a conventional bomb, nuclear attack, biological attack, or a hurricane. Another participant noted that the purpose of risk assessment is to help answer these strategic questions. One participant also recommended that the short-term goal for a national strategic planning process should be identifying the big problems that strategic planning needs to address, such as measuring the direct and indirect costs of reducing risk.

- *Fragmented approaches to managing security risk within and across the federal government could be addressed by developing governmentwide risk management guidance.* Some participants agreed that approaches to risk management were fragmented within and across the federal government. For example, one participant said that each of the Department of Defense combatant commands has its own perspective on risk. According to this participant, this lack of consistency requires recalculations and adjustments as each command operates without coordinating efforts or approaches. Three participants also said that there is a lack of governmentwide guidance on using risk management principles to manage programs. To address this problem, participants said governmentwide guidance should be developed. Two participants suggested that OMB or another government agency should play a lead role in outlining goals and general principles of risk assessment and getting agencies to implement these principles.

Partnership and Coordination Challenges

Participants agreed that risk management should be viewed as the responsibility of both the public and private sector. They identified challenges related to public-private collaboration:

- *Private sector should be more involved in public risk assessments.* Participants said that public-private partnerships are important and should be strengthened. One reason partnerships may not be as strong as they could be is that the private sector may not be appropriately involved in the public sector's risk assessments or risk-based decision-making. Participants agreed that the private sector should be involved in developing risk assessments because when these stakeholders are not sufficiently involved they lose faith in government announcements and requirements related to new risks and threats. To this end, DHS has established coordinating councils for critical infrastructure protection that allow for the involvement of representatives from all levels of government and the private sector, so that collaboration and information sharing can occur to assess events accurately, formulate risk assessments, and determine appropriate protective measures.

- *Increase the involvement of state and local practitioners and experts.* Participants observed that intergovernmental partnerships—between federal, state, local, and tribal governments—are important for effective homeland security risk management. They recommended that more state and local practitioners and experts become involved in applying risk management principles to homeland security.

This concludes my prepared statement. I would be pleased to answer any questions you and the Subcommittee Members may have.

Appendix I: List of Participants

Moderators

Cathleen A. Berrick	Director, Homeland Security and Justice U.S. Government Accountability Office
Sallyanne Harper	Chief Administrative Officer and Chief Financial Officer U.S. Government Accountability Office
Norman J. Rabkin	Managing Director, Homeland Security and Justice U.S. Government Accountability Office

Participants

Michael Balboni	Deputy Secretary for Public Safety State of New York
Esther Baur	Director, Group Communications Head of Issue Management & Messages Swiss Re
Baruch Fischhoff	Howard Heinz University Professor Department of Social and Decision Sciences and Department of Engineering and Public Policy Carnegie Mellon University
George W. Foresman	President Highland Risk & Crisis Solutions, Ltd. Former Under Secretary for National Protection and Programs Former Under Secretary for Preparedness U.S. Department of Homeland Security
Tina W. Gabbrielli	Director, Office of Risk Management and Analysis National Protection and Programs Directorate U.S. Department of Homeland Security

James Gilmore	Partner, Kelley Drye & Warren, LLP Chairman, Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction Governor of Virginia, 1998-2002
Corey D. Gruber	Assistant Deputy Administrator National Preparedness Directorate Federal Emergency Management Agency U.S. Department of Homeland Security
Brian Michael Jenkins	Senior Advisor to the President RAND Corporation
RDML Wayne E. Justice	Rear Admiral Director of Response Policy United States Coast Guard
Kenneth L. Knight, Jr.	National Intelligence Officer for Warning National Intelligence Council Office of the Director of National Intelligence
Howard Kunreuther	Cecilia Yen Koo Professor Department of Decision Sciences and Public Policy Wharton School, University of Pennsylvania Co-Director Wharton Risk Management and Decision Processes Center
Peter Lowy	Group Managing Director Westfield Group
Thomas McCool	Director of the Center for Economics U.S. Government Accountability Office
Susan E. Offutt	Chief Economist U.S. Government Accountability Office
John Paczkowski	Director, Emergency Management and Security Port Authority of New York and New Jersey

John Piper	Senior Security Consultant Talisman, LLC
William G. Raisch	Director, International Center for Enterprise Preparedness New York University
Joseph A. Sabatini	Managing Director Head of Corporate Operational Risk JPMorgan Chase
Kenneth H. Senser	Senior Vice President for Global Security, Aviation and Travel Wal-Mart Stores, Inc.
Hemant Shah	President and Chief Executive Officer Risk Management Solutions
Steven L. Stockton	Deputy Director of Civil Works U.S. Army Corps of Engineers
William F. Vedra, Jr.	Executive Director Ohio Homeland Security
Detlof von Winterfeldt	Professor, Industrial and Systems Engineering Viterbi School of Engineering, University of Southern California Professor of Public Policy and Management School of Policy Planning Director Center for Risk and Economic Analysis of Terrorism Events University of Southern California
Scott T. Weidman	Director, Board on Mathematical Sciences and Their Applications National Research Council
Henry H. Willis	Policy Researcher RAND Corporation

.

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Norman J. Rabkin, (202) 512-8777, rabkinn@gao.gov
Cathleen A. Berrick, (202) 512-3404, berrickc@gao.gov

Acknowledgments

In addition to the contacts named above, Anne Laffoon, Assistant Director; Tony Cheesebrough; Jason Barnosky; David Messman; and Maylin Jue managed all aspects of the work, and Susanna Kuebler and Adam Vogt made important contributions to producing this report.

Related GAO Products

Aviation Security: Transportation Security Administration Has Strengthened Planning to Guide Investments in Key Aviation Security Programs, but More Work Remains. GAO-08-456T. Washington, D.C.: February 28, 2008.

Transportation Security: Efforts to Strengthen Aviation and Surface Transportation Security are Under Way, but Challenges Remain. GAO-08-140T. Washington, D.C.: October 16, 2007.

Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions. GAO-07-454. Washington, D.C.: August 17, 2007.

Homeland Security: Applying Risk Management Principles to Guide Federal Investments. GAO-07-386T. Washington, D.C.: February 7, 2007.

Homeland Security Grants: Observations on Process DHS Used to Allocate Funds to Selected Urban Areas. GAO-07-381R. Washington, D.C.: February 7, 2007.

Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts. GAO-07-225T. Washington, D.C.: January 18, 2007.

Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics. GAO-07-39.Washington, D.C.: October 16, 2006.

Interagency Contracting: Improved Guidance, Planning, and Oversight Would Enable the Department of Homeland Security to Address Risks. GAO-06-996. Washington, D.C.: September 27, 2006.

Border Security: Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program. GAO-06-1090T. Washington, D.C.: September 7, 2006.

Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System. GAO 06-618. Washington, D.C.: September 6, 2006.

Aviation Security: TSA Oversight of Checked Baggage Screening Procedures Could Be Strengthened. GAO-06-869. Washington, D.C.: July 28, 2006.

Border Security: Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program. GAO-06-854. Washington, D.C.: July 28, 2006.

Passenger Rail Security: Evaluating Foreign Security Practices and Risk Can Help Guide Security Efforts. GAO-06-557T. Washington, D.C.: March 29, 2006.

Hurricane Katrina: GAO's Preliminary Observations Regarding Preparedness, Response, and Recovery. GAO-06-442T. Washington, D.C.: March 8, 2006.

Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure. GAO-06-91. Washington, D.C.: December 15, 2005.

Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts. GAO-05-851. Washington, D.C.: September 9, 2005.

Strategic Budgeting: Risk Management Principles Can Help DHS Allocate Resources to Highest Priorities. GAO-05-824T. Washington, D.C.: June 29, 2005.

Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges. GAO-05-327.Washington, D.C.: March 28, 2005.

Transportation Security: Systematic Planning Needed to Optimize Resources. GAO-05-357T. Washington, D.C.: February 15, 2005.

Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security. GAO-05-33.Washington, D.C.: January 14, 2005.

Homeland Security: Observations on the National Strategies Related to Terrorism. GAO-04-1075T. Washington, D.C.: September 22, 2004.

9/11 Commission Report: Reorganization, Transformation, and Information Sharing. GAO-04-1033T. Washington, D.C.: August 3, 2004.

Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors. GAO-04-780. Washington, D.C.: July 9, 2004.

Homeland Security: Communication Protocols and Risk Communication Principles Can Assist in Refining the Advisory System.GAO-04-682. Washington, D.C.: June 25, 2004.

*Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sector*s. GAO-04-699T. Washington, D.C.: April 21, 2004.

Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspections. GAO-04-557T. Washington, D.C.: March 31, 2004.

Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain. GAO-04-598T.Washington, D.C.: March 23, 2004.

Homeland Security: Risk Communication Principles May Assist in Refinement of the Homeland Security Advisory System. GAO-04-538T.Washington, D.C.: March 16, 2004.

Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism. GAO-04-408T. Washington, D.C.: February 3, 2004.

Catastrophe Insurance Risks: Status of Efforts to Securitize Natural Catastrophe and Terrorism Risk. GAO-03-1033. Washington, D.C.: September 24, 2003.

Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues. GAO-03-1165T. Washington, D.C.: September 17, 2003.

Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened. GAO-03-760. Washington, D.C.: August 27, 2003.

Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues. GAO-03-715T. Washington, D.C.: May 8,2003.

Transportation Security Research: Coordination Needed in Selecting and Implementing Infrastructure Vulnerability Assessments. GAO-03-502. Washington, D.C.: May 1, 2003.

Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing. GAO-03-322. Washington, D.C.: April 15, 2003.

Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown. GAO-03-439. Washington, D.C.: March 14, 2003.

Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors. GAO-03-233. Washington, D.C.: February 28, 2003.

Major Management Challenges and Program Risks: Department of Homeland Security. GAO-03-102. Washington, D.C.: January 30, 2003.

Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats. GAO-03-173. Washington, D.C.: January 30, 2003.

Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts. GAO-02-208T. Washington, D.C.: October 31, 2001.

Homeland Security: Key Elements of a Risk Management Approach. GAO-02-150T. Washington, D.C.: October 12, 2001.

Homeland Security: A Framework for Addressing the Nation's Issues. GAO-01-1158T. Washington, D.C.: September 21, 2001.

Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks. GAO/NSIAD-99-163.Washington, D.C.: September 7, 1999.

Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments. GAO/NSIAD-98-74. Washington, D.C.: April 9, 1998.

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

PRINTED ON RECYCLED PAPER