



Highlights of a
FORUM

Convened by the
**Comptroller General of
the United States**

**STRENGTHENING
THE USE OF RISK
MANAGEMENT
PRINCIPLES IN
HOMELAND SECURITY**

April 2008

GAO-08-627SP



Highlights of [GAO-08-627SP](#), a GAO forum

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. 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.

GAO convened a forum of experts on October 25, 2007, to advance a national dialogue on applying risk management to homeland security. Broadly defined, risk management is a process that helps policymakers assess risk, strategically allocate finite resources, and take actions under conditions of uncertainty. Participants included federal, state, and local officials and risk management experts from the private sector and academia.

The forum addressed effective practices, challenges federal agencies face in applying risk management to homeland security, and actions that can strengthen homeland security risk management. Comments expressed during the proceedings do not necessarily represent the views of any one participant, the organizations they represent, or GAO. Participants reviewed a draft of this report and their comments were incorporated, as appropriate.

To view the full product, click on [GAO-08-627SP](#). For more information, contact Cathleen Berrick at (202) 512-3404 or berrickc@gao.gov.

HIGHLIGHTS OF A GAO FORUM

Strengthening the Use of Risk Management Principles in Homeland Security

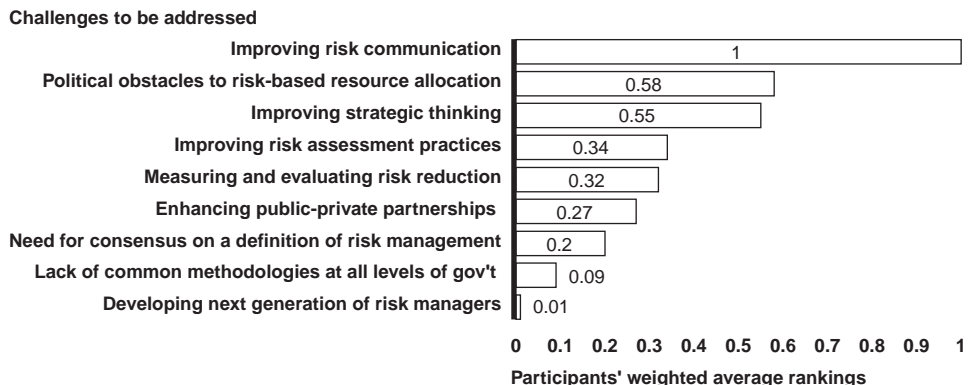
What Participants Said

Forum participants discussed risk management practices currently used or being considered in the private and public sectors, such as the position of chief risk officer (CRO). Private sector CROs communicate information about risks to the business executives responsible for mitigating risks and steer mitigation efforts. A government CRO could address the need for leadership in public sector risk management initiatives, such as improving emergency response and disaster recovery efforts. Participants also noted differences between the public and private sectors. For example, the private sector has the flexibility to choose which risks to insure against, while the public sector must accommodate the public’s beliefs about risks and preferences for risk management.

Participants identified and ranked the challenges in applying risk management principles to homeland security that in their view were the most critical to address. The top three challenges were (1) improving risk communication, for instance, addressing the lack of a common vocabulary to discuss risk management and lack of a public dialogue about acceptable levels of risk; (2) political obstacles to risk-based resource allocation, such as the reluctance of policymakers, at times, to make difficult choices about what to protect; and (3) lack of strategic thinking, including lack of a governmentwide discussion and strategy related to homeland security investments.

When asked to rank which challenge should be addressed first, participants most often selected improving risk communication followed by political obstacles and improving strategic thinking, as shown in the figure below. The expert panel proposed a number of actions to strengthen the use of risk management principles, such as increasing meaningful public outreach to provide fact-based estimates of risk, highlighting the importance of risk management to incoming policymakers, and identifying effective risk assessment practices.

Rankings by Participants of Challenges in the Order They Should Be Addressed



Source: GAO analysis of participants' forum polling responses.

Note: This presents the weighted average rankings of the participants' assessment of the overall order that each of the challenges should be addressed on a scale of 1 to 0, with 1 being the highest ranking and 0 being the lowest.

Contents

Letter		1
	Introduction	1
	Current Risk Management Practices in the Private and Public Sectors	4
	Homeland Security Risk Management Challenges	12
	Addressing Homeland Security Risk Management Challenges	25
	Suggested Next Steps	31
Appendix I	Agenda	33
Appendix II	List of Participants	34
Appendix III	Presentation by Norman Rabkin, Managing Director, Homeland Security and Justice, GAO	37
Appendix IV	GAO Contacts and Staff Acknowledgments	43
Related GAO Products		44
Figures		
	Figure 1: Pre-Forum Polling—Most Critical Challenge in Applying Risk Management to Homeland Security	15
	Figure 2: Forum Polling—Most Critical Challenge in Applying Risk Management to Homeland Security	16
	Figure 3: Forum Polling—Rankings by Participants of Challenges in the Order They Should Be Addressed	26

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.



G A O

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

Introduction

GAO has highlighted the practice of effective risk management as a challenge for both Congress and the administration. 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. 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.

While integrating a risk management approach into decision-making processes is challenging for any organization, GAO has reported that it is particularly difficult for the Department of Homeland Security (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. Despite these and other challenges, DHS is making progress in applying risk management principles to guide its operational and resource allocation decisions.

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. However, substantial challenges remain in strengthening risk-based efforts and using this information to inform strategies and investment decisions. Addressing these challenges will take time, leadership, and attention. Moreover, risk management needs to be viewed strategically—that is, with a view that goes beyond assessing specific risks and integrates a consideration for risk into annual budget and program review cycles.

In addition to helping federal agencies like DHS focus their efforts, risk management can assist state and local governments and the private sector—which owns over 85 percent of the nation's critical infrastructure—with prioritizing 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.

GAO convened this forum on October 25, 2007, to assist Congress and federal agencies, including DHS, by advancing the national dialogue on risk management challenges in homeland security and by helping to identify potential solutions to these complex challenges. The forum focused on (1) lessons that can be learned from leading organizations about the effective use of risk management practices, (2) key challenges faced by public and private organizations in adopting and implementing a risk-based approach for homeland security, and (3) actions that should be taken in the near and long term to address the most pressing of these challenges. (See app. I for the agenda.) In addition to addressing these objectives, participants spoke generally about potential next steps to be taken in the near term to help strengthen risk management practices.

The forum brought together a diverse array of experts, including representatives from all levels of government, nonprofit organizations, industry, and academia. (See app. II for a list of participants.) The forum was designed so that participants could comment on these issues openly, without individual attribution, to facilitate a rich, frank, and substantive discussion.

This summary captures the ideas and themes that emerged at the forum, the collective discussion of participants, and comments received from participants based on a draft of this summary. Thus, the summary does not necessarily represent the views of any individual participant or the organizations that these participants represent, including GAO.

I would like to thank the forum participants for taking the time to share their knowledge, insights, and perspectives on this important topic. Others will benefit from these insights. We look forward to working with the participants on these and other issues of mutual interest and concern in the future.

A handwritten signature in black ink that reads "Gene L. Dodaro". The signature is written in a cursive style with a large, prominent "D" and a long horizontal flourish extending to the right.

Gene L. Dodaro
Acting Comptroller General of the United States

April 15, 2008

Current Risk Management Practices in the Private and Public Sectors

The forum was opened with two presentations: the first, provided by Norman Rabkin of GAO, described the importance of risk management in strengthening homeland security resource allocations given current and projected fiscal challenges. The second presentation, provided by Esther Baur of Swiss Re, set the stage for a group discussion on current risk management practices in the private and public sectors. Overall, participants discussed the concept of a chief risk officer (CRO) and public sector examples of effective risk management practices used by organizations such as the U.S. Coast Guard (USCG) and compared and contrasted public and private sector risk management practices.

Presentation by Norman Rabkin, GAO

Norman Rabkin is Managing Director of GAO's Homeland Security and Justice Team. Mr. Rabkin presented on behalf of the Comptroller General, who was unable to attend the forum. He opened the forum with a presentation on the United States' current fiscal crisis—based on the Comptroller General's Fiscal Wake-up Tour—and the importance of using risk management principles to focus resources on our most pressing concerns. (See app. III for Mr. Rabkin's presentation.) He noted that homeland security risks are complex and stretch across numerous hazards because of either human actions or natural causes, including terrorism, natural disasters such as hurricanes Katrina and Rita, and accidents such as the I-35W bridge collapse in Minneapolis. Mr. Rabkin stated that the nation will never be completely safe, total security is an unachievable goal, and we cannot afford to protect everything against all threats.

According to Mr. Rabkin, projections of growing fiscal challenges for federal, state, and local governments underscore this issue. He stated that in 2006, the United States' costs exceeded revenues by \$450 billion, and cash outlays exceeded cash receipts by \$248 billion. Mr. Rabkin described the primary source of the problem as the long-range liabilities and commitments that have increased during the past 6 years from \$20 trillion to \$50 trillion—or about \$440,000 for every U.S. household. He noted that state and local governments are also facing increasing fiscal pressures—in particular, health care costs such as states' obligations under the Medicaid program—and that these in turn contribute to the federal government's fiscal challenges. Mr. Rabkin added that the country is on an imprudent and unsustainable fiscal path and will not grow out of this problem.

Mr. Rabkin noted that there are some possible ways to address the nation's long-term fiscal problems. He said that our nation needs more discussion about where we are and where we are headed and that we need to reexamine what the government does, how the government does

business, and who does the government's business. Mr. Rabkin said that the application of risk-based principles can help the nation in this regard through more informed decision making regarding the allocation of federal resources. He noted that Congress and the administration have recognized the value of risk management in helping policymakers make resource allocation decisions and have charged federal agencies with incorporating these principles into program planning and budgeting processes. He further noted that DHS is making progress in applying risk management to guide its operational and resource allocation decisions and cited the creation of the department's Office of Risk Management and Analysis in 2007 to lead efforts to address the overall management and analysis of homeland security risk.

Mr. Rabkin described GAO's risk management¹ framework that the office uses, along with other criteria, in assessing DHS's risk management² efforts. He stated that this framework is based on industry best practices and consists of five phases: (1) setting strategic goals and objectives, and determining constraints; (2) assessing risks;³ (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. He said that applying risk management in a homeland security context is a relatively new endeavor and that approaches will continue to evolve as processes mature and lessons are learned.

Mr. Rabkin closed his presentation by stating that GAO invited the participants to the forum to discuss the most critical challenges in applying risk management principles to homeland security and how best to address these challenges. He thanked the participants for responding to a pre-forum poll and noted that this information was used to shape the forum's agenda.

¹For a description of this framework, see Appendix I of *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.

²Risk management is a continuous process of managing—through a series of mitigating actions that permeate an entity's activities—the likelihood of an adverse event and its negative impact.

³Risk assessment is the process of qualitatively or quantitatively determining the probability of an adverse event and the severity of its impact on an asset.

Presentation by Esther
Baur, Swiss Re

Esther Baur is Director of Group Communications and Head of Issue Management & Messages at Swiss Re, a multinational reinsurance firm recognized for expertise in risk and capital management. Ms. Baur began the forum's session on risk management practices with a presentation entitled "Risk Management in the Private and Public Sectors." Ms. Baur noted Swiss Re's participation in the World Economic Forum's (WEF) Global Risk Network (GRN), which produced the 2008 *Global Risk Report* for the WEF Annual Meeting in Davos, Switzerland. She noted that the GRN members collaborated in workshops to define and assess global risks based on their likelihood and severity, and developed a map of 23 core risks that the international community faces over the next 10 years.

Ms. Baur began the presentation by discussing the history of the discipline of risk management, beginning with its roots in banking and finance. She emphasized its evolution from a discipline based largely on intuition into a more quantitative and systematic approach. Ms. Baur described Swiss Re's model for applying risk management to reinsurance, which is based on three conceptual pillars: (1) quantitative risk management, or identifying and assessing risks; (2) risk governance, or determining who manages risks and examining lines of defense to prevent and mitigate risks; and (3) risk disclosure or transparency, to help provide a sound basis for decision making.

Ms. Baur outlined overall roles and responsibilities in risk management as they apply to the public and private sectors. She noted that in both sectors overall roles and responsibilities in the risk management process should include the systematic identification and assessment of risks through scientific efforts; risk mitigation, either through direct legislation, executive action, or incentives; and risk adaptation to address financial consequences or to allow for effective transfer of risk. Ms. Baur stated that the unique role of the private sector is to "pre-fund" and diversify risk through insurance, and to support risk prevention by reflecting the quality of such measures in premiums. Public sector responsibilities include regulating land use and building codes; organizing disaster protection, response, and recovery measures; setting regulatory frameworks; and supplementing the insurance industry. She observed that government decisions are influenced by the public's perception of risk and called for better management of risk perception through government dissemination of factual information.

Given the interdependent nature of public and private sector roles and responsibilities, Ms. Baur emphasized the importance of public-private coordination and partnerships in providing insurance for natural

catastrophes and terrorism. As an example, she described an effort by the government of Mexico to seek private sector support to pre-fund potential natural disaster losses by issuing earthquake bonds.⁴ She stated that terrorism risk is uninsurable without a public-private partnership for the following two reasons. First, she explained that terrorism risk cannot be quantified as effectively as natural disaster risk because historical data are more limited and potentially have less predictive relevance. Second, terrorism may impose extreme losses correlated over time and types of risks (e.g., to property, human lives, and financial markets). As a result, governments play important roles in managing terrorism risk, such as regulating insurance coverage, providing backstop financing as the “insurer of last resort,” deploying antiterrorism measures, and providing for emergency response and recovery. Ms. Baur noted that public-private arrangements exist in several countries—including in the United States through the Terrorism Risk Insurance Act—and that Swiss Re supports permanent market solutions based on a risk partnership among the insured, insurers, reinsurers, capital markets, and governments.

Ms. Baur concluded her presentation by suggesting an idea for group discussion—the establishment of a CRO for government. She noted that many private sector organizations, including Swiss Re, have designated CROs whose role is to focus on understanding and communicating information about risks to the business managers responsible for mitigating risk and to steer risk mitigation efforts. A government CRO would ideally work jointly with the private sector to identify emerging risks, establish a risk landscape of frequency and severity based on the best scientific knowledge, communicate this risk landscape to policymakers and the general public, steer mitigation efforts toward the biggest risks, and pool and manage those risks that cannot be carried by the (re)insurance industry alone.

The Role of a Chief Risk Officer

Participants discussed the potential applicability of a CRO in the public sector. Participants emphasized the importance of defining reporting relationships through an organizational structure that provides sufficient authority to a CRO, while also facilitating the flow of information. One

⁴Given the high risk of earthquakes in Mexico, Swiss Re issued a special catastrophe bond for the Mexican government in 2006 to finance rescue and rebuilding in the case of a disastrous earthquake. If there is no disaster within 3 years, investors who buy the bonds receive the premium and the interest. If there is a disastrous earthquake, the Mexican government will receive the full value of the bonds.

participant noted that the CRO at his firm reported separately to both the chief executive officer and the board of directors to help ensure accountability.

Participants suggested that a public sector CRO could address the need for leadership in public sector risk management initiatives. As an example, one participant noted that the United Kingdom (U.K.) established a cabinet-level risk management unit called the Civil Contingencies Secretariat (CCS) in response to the “3 Fs” crises— fuel strike, flooding, and foot-and-mouth disease. In response to public concerns over the U.K.’s risk preparedness, the CCS developed a risk map and defined criteria for assessing losses, and to date, the focus of the CCS in the U.K. has been on improving emergency response and disaster recovery efforts. According to this participant, planned next steps include engaging a broader array of stakeholders in risk assessments.

One participant stated that the Secretary of DHS is analogous to a domestic CRO for the federal government. Through Homeland Security Presidential Directive 5, the President has designated the Secretary of DHS as the principal federal official for domestic incident management, responsible for coordinating federal operations within the United States and across all federal agencies to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. According to this participant, Secretary Chertoff has recently designated the new DHS Office of Risk Management and Analysis (RMA) as his executive agent for risk management across all DHS components. The participant stated that through RMA, the process of establishing a domestic risk management function for homeland security has begun and is intended to include a coordinating role across other departments and agencies outside of DHS in the future.

Participants identified various challenges associated with the development of a CRO position, 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.

Examples of Public Sector Organizations with Effective Risk Practices

During the discussion of current risk management practices, participants highlighted examples that they believed demonstrated the effective integration of risk management into the operations of several public sector organizations, including USCG, the U.S. Army Corps of Engineers

(USACE), the Port Authority of New York and New Jersey (PANYNJ), and China's Liquid Natural Gas (LNG) operations.

Four participants pointed to USCG as an example of an agency that effectively uses risk management. According to one participant, since September 11, 2001, USCG has expanded its traditional port security program to a wide-ranging maritime security strategy that includes an enhanced counterterrorism role. This participant stated that USCG uses risk analysis and threat assessments from the intelligence community to implement a risk-based strategy to concentrate maritime security measures when and where relative risk is the greatest. The participant stated that USCG uses its long-standing principles of risk management, which are continually improved through the risk analysis cycle, at the highest levels of the organization to prepare for the impact of high-risk scenarios and to balance security needs with the need to ensure an efficient flow of commerce. The participant further stated that risk-based principles are being institutionalized through Area Maritime Security Committees—a routine process for working together with regional partners. According to another participant, USCG is pushing its processes for managing risk down to its captains to let them work with private and public sector partners on implementation of risk management initiatives. For example, a participant noted that USCG and U.S. Customs and Border Protection (CBP) work together daily when boarding vessels to reduce risk as well as to ensure the efficient flow of commerce.⁵

Another participant stated that USACE developed flood risk management practices that have been used to digest and share critical information with the public. For example, after Hurricane Katrina, USACE ran supercomputer Advanced Circulation Model programs to model residual risk and the potential impact of rebuilding in affected areas. According to the participant, these complex models were made available to the public through Google Earth, and despite fears of confusion, this information-

⁵USCG carries out two efforts related to vessels entering ports and waterways to mitigate the risk that such vessels pose: security code compliance examinations and armed security boardings. Armed security boardings are conducted on targeted foreign and U.S. vessels that are deemed to pose a high relative security risk before they enter U.S. ports. The purpose is to inspect a vessel's cargo, documentation, and persons on board in order to assess whether any additional security measures are warranted to deter acts of terrorism or a security incident before permitting the vessel's entry into port. Other law enforcement agencies, such as CBP, may also participate if special expertise is needed, such as if a closer look is needed at a vessel's cargo, or if their mission requires them to board the same vessel.

sharing project empowered people to locate their own addresses and make informed, risk-based decisions about rebuilding.

One participant noted that PANYNJ 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 the participant, this methodology has since been applied to over 30 other transportation and port agencies across the country, and PANYNJ itself has moved from conducting individual risk assessments to implementing an ongoing program of risk management. The participant noted that PANYNJ's risk management program conducts security risk assessments on a 2-year cycle, where the risk of an array of potential security threats is assessed for a set list of individual critical assets and subcomponents of assets. The participant said that as each successive risk assessment is conducted, the results are compared against the prior assessment, and the change in relative risk is calculated to show not only improvement in the agency's risk profile as the result of new security investment but also any potential worsening in that risk profile as the result of a changing threat picture. In this way, the participant stated that PANYNJ has successfully compared successive risk assessment results to measure the buy-down of risk as a metric for security program performance. PANYNJ has also implemented a methodology for risk and cost-benefit analysis that facilitates the comparative analysis of competing high-cost security alternatives.

Finally, one participant discussed China as an international example of the public sector's use of risk management in homeland security. The participant stated that the Chinese government requires security risk assessments of maritime LNG shipping operations before granting operating permits. According to the participant, this requirement makes an important contribution to securing petrochemicals by promoting consistent risk management practices from the beginning of operations.

Comparing and Contrasting Public and Private Sector Risk Management Practices

Participants compared and contrasted public and private sector risk management practices. One participant noted that risk management is challenging in both the public and private sectors and is a function that tends to evolve over time. Participants suggested that for both sectors, the development of risk management capabilities requires a multidisciplinary approach, involving a wide range of skills. It was further suggested that it is necessary to constantly incorporate new skills and to work collaboratively with universities when particular specialists do not reside in-house.

Participants stated that the private sector has the flexibility to choose which risks to insure against and 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. For example, the private sector actively considers which markets to pursue through an analysis of the opportunities they present. By contrast, participants stated that the public sector must accommodate the public’s beliefs about risks and preferences for risk management, which are often based on incomplete information and seen through the filter of complex political processes. According to one participant, the public sector is particularly challenged by the public’s unrealistic expectations of government—namely, for “total and complete security”—and an unrealistically low tolerance for risk. Participants said that in the public sector, risk decisions are often influenced by the public’s perception of risk, regardless of whether those perceptions are accurate. As a result, participants stated that there is less incentive for the public sector to use risk management to identify and seize long-term opportunities to reduce risk, such as investing in transportation infrastructure.

Finally, one participant noted that private organizations must often make decisions based on incomplete information because of restricted access to classified information. Several participants indicated that better information sharing between the public and private sectors would be beneficial, as industry relies on government to reveal threats, and government relies in part on industry to reveal vulnerabilities.

Homeland Security Risk Management Challenges

Dr. Henry Willis of the RAND Corporation began the forum's second session with a presentation entitled "Homeland Security Risk Management Challenges Faced by Federal Agencies." A discussion of a variety of challenges in applying risk management principles followed, including improving risk communication,⁶ political obstacles to risk-based resource allocation, a lack of strategic thinking about managing homeland security risks, partnership and coordination challenges, and the need for risk management education. Many participants emphasized that the nature of these key challenges related primarily to leadership rather than technical issues, such as methods used to assess risks. Following the discussion, participants were polled on the risk management challenges they viewed as most critical.

Presentation by Dr. Henry Willis, RAND

Dr. Willis is a Policy Researcher at the RAND Corporation, a nonprofit research and analysis organization recognized for its strategic planning and risk management expertise. He discussed risk management challenges related to risk analysis at DHS, as well as ideas for strengthening the application of risk management in homeland security. He began by stating that risk management is fundamental to homeland security, whether for protecting emergency responders, defending infrastructure, countering Man Portable Air Defense Systems, inspecting shipping containers, or documenting travelers.

Dr. Willis noted that DHS has defined risk as a function of threat, vulnerability, and consequence:⁷ a credible threat of attack on a vulnerable target that would result in unwanted consequences. He stated that this definition lays a foundation for DHS strategic planning, serves as a common starting point for discussions of risk, and provides a structure for considering challenges in managing terrorism risk. Dr. Willis noted that assessing each factor of terrorism risk is challenging. For example, given the uncertainties involved, it is difficult to anticipate changes in threats, and one challenge is linking intelligence analysis and risk analysis. He further stated that vulnerability assessments are very detailed analyses and that it is difficult to develop practical methods for identifying

⁶According to the National Research Council, risk communication is the exchange of information among individuals and groups regarding the nature of risk, reactions to risk messages, and legal and institutional approaches to risk management.

⁷White House Homeland Security Council, *National Strategy for Homeland Security*, (Washington, D.C.: October 5, 2007).

vulnerabilities of large numbers of potential targets while at the same time satisfying technical feasibility and cost constraints. Finally, he stated that the consequences of terrorism can spread widely because of (1) system linkages through cascading failures in linked systems, such as a power outage, and (2) social amplification of risk, such as the Washington, D.C., sniper event resulting in school closings and changes in purchase patterns, for example, consumers purchasing gas outside of the area.⁸

Beyond the challenges in assessing risk, Dr. Willis stated that we have to better understand how to manage risk. For example, he noted that countermeasures can reduce threats, but we need to be able to estimate the level of deterrence resulting from the countermeasures implemented. He said that system design and operations can reduce vulnerability, but we need to know how security benefits change as adversaries adapt technologies and tactics. He stated that effective response can reduce consequences, so we need to know how the public will respond during the immediate aftermath of a terrorist attack. Finally, he suggested that layered defenses provide robustness and flexibility, but we must determine how a portfolio of measures, programs, and policies can be evaluated.

Dr. Willis concluded with some observations about addressing terrorism risk management challenges. First, he noted that homeland security programs should be accountable to standards of effectiveness, using metrics such as cost-effectiveness or residual risk (a measure of how much a program reduces the level of risk). Second, he offered that risk management must be analytic—addressing all three factors of risk—and deliberative. He stated that a deliberative process is necessary because values and judgment are a part of the process of managing homeland security risk and requires transparency and a comprehensive public discussion of outcomes. As an example, he asked whether more should be spent to protect a skyscraper in downtown Los Angeles from terrorism or earthquakes. Dr. Willis said that public discourse is the only way to credibly address trade-offs between risks to people from risks to property and among risks from a conventional bomb, nuclear attack, biological attack, or even hurricane or other natural disaster. Third, he stated that sufficient resources must be provided to enable capacity within DHS for homeland security risk analysis and strategic planning, noting that

⁸In the fall of 2002, sniper shootings resulted in the deaths of 10 Washington D.C.-area residents. Some of the shootings took place at gas stations, shopping centers, and a school.

maturing risk analysis methods and processes takes time and that progress is being made. For example, he said that shortly after September 11, 2001, decisions about how to make grants to protect localities from terrorism were dominated by the use of crude indicators, such as population, which were intended to serve as a surrogate measure for the consequences of terrorist events. He said that this approach failed to differentiate scenarios that were more likely because of terrorists' capabilities and intentions or because targets were more vulnerable to attack. More recently, he stated that the Secretary of DHS has called on the department to adopt risk-based decision making and that methods of risk analysis were being established.

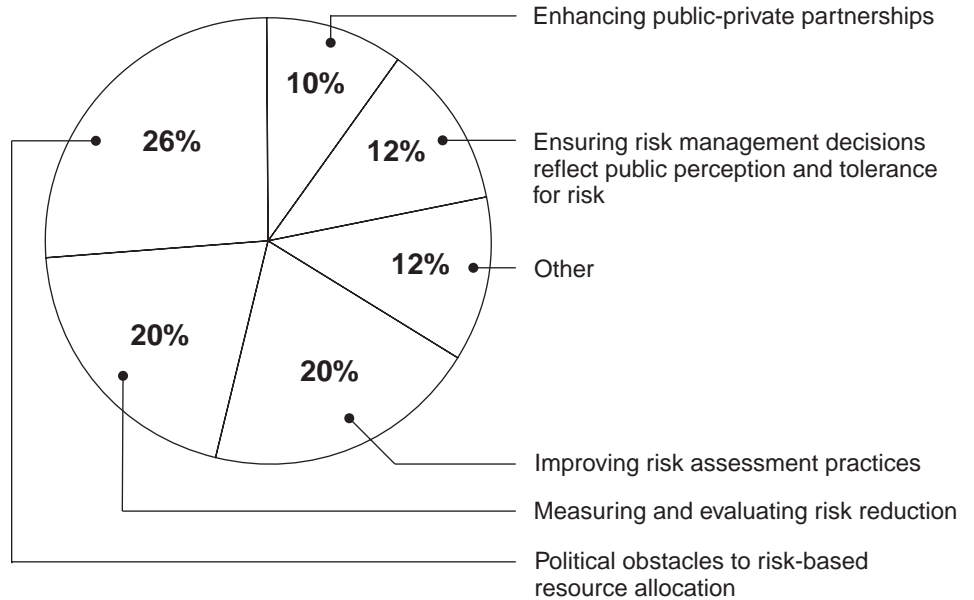
Participants Polled on Most Critical Risk Management Challenge

Prior to the forum, we polled the participants by asking them what they viewed as the single most critical challenge in applying principles of risk management to homeland security. Specifically, participants were asked to select one challenge from the following list of those that we identified during our collective interviews conducted earlier with forum participants or to identify any additional challenges not listed using the "Other" category:

- Improving the practice of risk assessment.
- Overcoming political obstacles to risk-based resource allocation.
- Enhancing partnerships between the public and private sectors.
- Ensuring that risk management decisions reflect an understanding of the public's perception of and tolerance for risk.
- Measuring and evaluating the risk reduction achieved by programs and countermeasures.
- Other.

The results of our pre-forum polling demonstrated a lack of consensus regarding what the most critical challenges were, with responses fairly evenly distributed among several of the challenges, as illustrated in figure 1.

Figure 1: Pre-Forum Polling—Most Critical Challenge in Applying Risk Management to Homeland Security



Source: GAO analysis of participants' pre-forum polling responses.

On the day of the forum, following the presentation by Dr. Willis and subsequent discussion on challenges in applying risk management principles to homeland security, participants were polled a second time and were asked to choose the most critical challenge in applying the principles of risk management to homeland security. The forum poll contained the same five close-ended options listed above with three changes. First, “Ensuring that risk management decisions reflect an understanding of the public’s perception of and tolerance for risk” was abbreviated as “Improving risk communication.” Second, the two most common pre-forum responses suggested under the open-ended “Other” option were added as close-ended options:

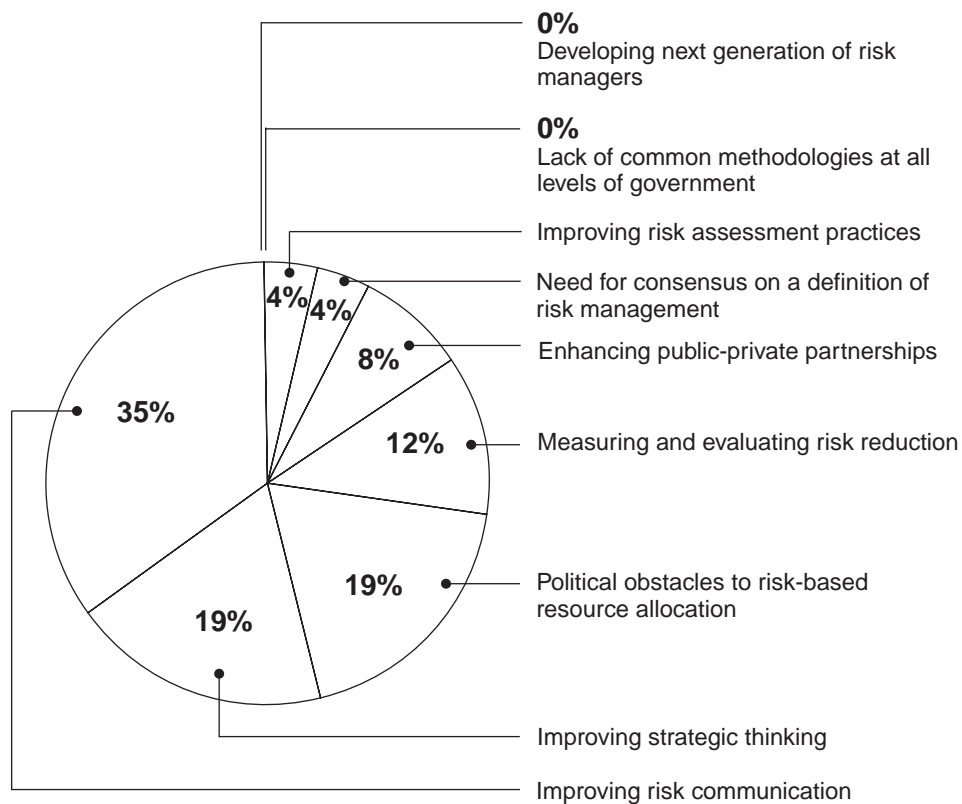
- Improving strategic thinking.
- Need for consensus on risk management definition.

Third, two options discussed by the participants at the forum were added:

- Developing the next generation of risk managers.
- A lack of common methodologies at all levels of government.

The resulting vote identified that a consensus began to emerge during the discussion, with a clear plurality of the participants voting that the most critical challenge in applying risk management to homeland security was improving risk communication. Two challenges tied for the second most number of votes: political obstacles to risk-based resource allocation and improving strategic thinking about managing homeland security risks. The results of the vote are shown in figure 2.

Figure 2: Forum Polling—Most Critical Challenge in Applying Risk Management to Homeland Security



Source: GAO analysis of participants' forum polling responses.

Note: Individual percentages may not sum to 100 because of rounding.

Risk Communication Challenges

As shown through the forum polling, 35 percent of participants responded that improving risk communication was the most critical challenge in applying risk management to homeland security. Participants discussed several risk communication challenges outlined below, including the lack of a common lexicon or vocabulary for risk management, a focus on

unlikely risks with dramatic consequences, the need to engage the public in a dialogue about an acceptable level of risk, and a lack of consideration of behavioral impacts.

- *Lack of a common lexicon for risk management.* Participants said that a lack of a common lexicon for risk management makes communication and collaboration particularly challenging. Participants stated that there is no common lexicon of terms in use, complicating communication among the public and private sectors and other stakeholders.
- *Focus on unlikely risks with dramatic consequences.* Participants noted that media coverage sensationalizes acts of terrorism, regardless of how likely they are to occur, and that terrorism is characterized by infrequent but potentially catastrophic events.⁹ Participants stated that this coverage creates fear among the public and undermines society's ability to engage in a fact-based discussion of risk.
- *Need to engage public in dialogue about an acceptable level of risk.* Participants suggested that since it is not possible to prevent all disasters and catastrophes, it is necessary to engage the public in defining an acceptable level of risk in order to make logical resource allocation decisions. Participants observed that effective risk communication involves information flows that move in both directions between government and the public. They explained that while it is important that government share information about risks with the public, government also needs to obtain the public's input on homeland security concerns as well as on the prioritization of risks and associated resource allocation decisions. In this regard, participants noted the need to increase efforts to share information with the public and to obtain information about public opinion. They further observed that the government does not always provide the public with sufficient information on specific risks or engage the public in decision making related to addressing these risks.
- *Lack of consideration of behavioral impacts.* Participants noted that risk communication is often wrongly viewed as an exercise in public relations and press releases. They argued that effective risk communication requires input from social science experts to determine

⁹Such acts are often referred to as low probability-high consequence events among risk management scholars and practitioners.

the communication needs of the public. Participants further noted that human behavior affects risks and should be considered explicitly in risk assessments and in the development of risk management models. For example, one participant noted that 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 evacuated. Another participant noted that human behavior introduces unknowns and questioned whether people would venture outside to pick up their medications if an anthrax attack were to occur. Participants said that risk analysis, including predictive modeling, tends to mistakenly neglect to account for the public's expectations and emotions in these ways. Participants stated that the identification of behaviors that may affect risks will be more effective with the input of behavioral scientists.

Political Obstacles to Risk-Based Resource Allocation

Participants agreed that overcoming political obstacles was necessary to allocate homeland security resources based on risk. They recommended the adoption of risk-informed processes for making federal resource allocation decisions and identified a number of political obstacles to risk-based resource allocation, including the reluctance of politicians and others, at times, to make difficult trade-offs and changes in the public's perception of risk, an absence of clarity related to federal spending decisions, conflicts between federal grant programs and national priorities for homeland security, and inconsistencies in resource allocations across the country.

- *Reluctance of politicians and others to focus on long-term trade-offs and shifts in perceptions of risk over time.* Participants noted that elected officials understand that their ability to deliver services to constituents directly affects their ability to be elected. According to participants, at times this pressure on politicians creates a political disincentive for elected leaders to make strategic risk management decisions that require trade-offs. Participants suggested that individuals—whether they are elected officials, organizational decision makers, or the members of the general public—tend to focus on short-term returns in deciding on whether to invest in protective measures. As a result, there is often a reluctance to incur up-front costs of protective measures that would be viewed as cost-effective from a long-term perspective. This was designated by one participant as the “Not In My Term of Office” or NIMTOF view of the world. Participants observed that understanding factors that affect the perception of risk is critical for effectively managing risk. They agreed that in general, the public's perception of the risk of an event, such as a natural disaster, is

high immediately following such an event but declines over time, irrespective of whether the event is likely or unlikely to occur again. Participants suggested that this tendency hinders risk mitigation by creating disincentives for stakeholders or officials to take actions that are likely to yield only long-term benefits. Participants also agreed that organizations must overcome this tendency by considering probable future events as well as short-term possibilities.

- *Absence of clarity related to federal spending decisions.* Participants observed that the federal government faces many challenges in making decisions about how to direct its spending most effectively against today's backdrop of fiscal constraints. Six participants called for more information and clarity regarding the level and direction of homeland security spending, suggesting that there is insufficient understanding of the total amount being invested in homeland security and how it is being used. Further, it was suggested that there is no clear understanding of where federal dollars *should* be spent to enhance security. Seven participants suggested that federal money has not been spent in a cost-effective manner or in a manner that buys down the maximum level of risk. For example, two participants criticized congressional earmarks and attempts to provide resources equitably among all geographic areas as inhibiting a rational risk-based approach to resource allocation. One participant remarked that both the public and private sectors had overspent on homeland security investments. Another suggested that homeland security investment decisions are being driven by emotion rather than information and logic.
- *Federal grant programs may conflict with national priorities.* Five participants stated that national priorities for homeland security may conflict with the results of competitive grant processes. In the view of two participants, DHS urges state and local governments to collaborate on homeland security within regions but also asks the same states and localities to compete for federal funding through the grant allocation process. As a result, federal grants were described by one participant as creating an unhealthy process of gaming and competition, and for this reason, grants were criticized as a poor instrument for buying down risk. Participants stated that the competition between regional, state, and local governments for limited grant funding for homeland security investments creates a disincentive for those regional stakeholders to coordinate on critical homeland security issues.
- *Inconsistent resource allocation across the country.* One participant, citing significant variations in port security across the nation, suggested that investments in homeland security often reflect local

politics rather than risk and vary inappropriately across the country. For example, this participant noted that while the same LNG tanker from St. Croix travels to Savannah and Boston each week, each city responds to the same ship and essentially the same risk in very different ways. According to this participant, a fleet of escort ships and helicopters is deployed in Boston while just two USCG cutters are dispatched to escort the tanker in Savannah.

Lack of Strategic Thinking

Participants agreed that a lack of strategic thinking about risk management was a key challenge to incorporating risk-based principles in homeland security investments. Participants noted, in particular, that challenges existed in the following areas: the need for public discourse to create a strategy for homeland security, the lack of opportunity analysis in the public sector, the lack of a single public risk manager, and insufficient governmentwide risk management guidance.

- *Need for public discourse to create a strategy for homeland security.* One participant noted that the President issued a *National Strategy for Homeland Security* in October 2007, to guide, organize, and unify the nation's homeland security efforts.¹⁰ However, eight participants echoed Dr. Willis's presentation by suggesting that a public discourse is needed to strategically address homeland security trade-offs. One participant suggested that our nation has managed to have a coherent dialogue for national security in which we discuss national security issues and decide how to allocate national security funding. According to this participant, a similar dialogue has not taken place among all stakeholders to create a strategy for homeland security, including the general public; the private sector; and federal, state, local, and tribal governments. Participants noted that in creating a strategy for homeland security, a significant challenge will be to balance security concerns within federal government agencies that have diverse missions in areas other than security, such as public safety and maintaining the flow of commerce.
- *Public sector lacks opportunity analysis.* Participants observed that the government's unique responsibilities emphasize the downside of

¹⁰See White House Homeland Security Council, *National Strategy for Homeland Security*, October 5, 2007, Page 41: "The assessment and management of risk underlies the full spectrum of our homeland security activities... We must apply a risk-based framework across all homeland security efforts... A disciplined approach to managing risk will help to achieve overall effectiveness and efficiency in securing the Homeland."

risks, focusing only on preparing for, responding to, and recovering from disasters. As a result, it was noted that the public sector lacks the opportunity analysis needed to identify and achieve desirable long-range goals, such as measures that simultaneously produce economic gains while improving security over the long term. As an example, participants suggested that improving transportation system resiliency could be achieved by investing in the underlying infrastructure and promoting redundancy through the creation of alternate transportation systems.

- *Lack of a single public risk manager discourages coordination.* Participants identified the lack of a single risk manager for the U.S. government as a key challenge. One participant suggested that this lack of central leadership has resulted in distributed responsibility for risk management within the administration and Congress and that this distributed responsibility has resulted in uncoordinated spending decisions. In addition, participants noted that without any overarching risk management framework for the federal government, the federal government tends to focus on reacting to immediate demands, without giving attention to indirect and long-term costs.
- *Governmentwide risk management guidance is insufficient.* Three participants described this lack of governmentwide guidance as presenting a challenge because different parts of government are at various levels of maturity in understanding and applying principles of risk management. One participant noted that the proposed risk assessment bulletin circulated by the Office of Management and Budget (OMB) in 2006¹¹ was found to be fundamentally flawed by a National Research Council scientific review.¹² According to participants, the council's review identified that "one size does not fit all," finding OMB's proposed bulletin to be inappropriate as across-the-board guidance for all risk assessments conducted throughout the federal government, and recommended that the bulletin be withdrawn. However, this participant stated that the council also recommended that the spirit of the bulletin—increasing the quality and objectivity of risk assessment in the federal government—was needed to help guide federal agencies in developing their own technical risk assessment

¹¹Office of Management and Budget, *Proposed Risk Assessment Bulletin*, January 9, 2006.

¹²Committee to Review the OMB Risk Assessment Bulletin, National Research Council, *Scientific Review of the Proposed Risk Assessment Bulletin from the Office of Management and Budget* (Washington, D.C.: 2007).

guidance. Two participants suggested that OMB or another government agency could play a role in helping to outline goals and general principles of risk assessment and could help agencies to implement these principles.

Partnership and Coordination Challenges

Participants agreed that risk management should be viewed as both a public and private sector issue, requiring partnerships and coordination rather than being an isolated, government-centered challenge. Participants identified several challenges related to public-private collaboration, including differences in public and private sector flexibility and expectations, the need to strengthen public-private partnerships, and the lack of intergovernmental partnerships.

- *Public and private sector flexibility and expectations differ.* Participants observed that while the public sector can learn a great deal from the private sector about risk management, there are key differences between the two. Participants acknowledged that the private sector can do some things not possible in the public sector. For instance, they said that private organizations have more flexibility because they can be selective about pursuing business lines and operational locations and can more easily dismiss surplus staff. Participants also noted that the private sector is able to transfer risk through financial mechanisms, such as insurance. Furthermore, participants said that consequences in the private sector can often be reduced to costs in dollar terms, whereas expectations for the public sector are much broader and complex.
- *Public-private partnerships need to be strengthened.* Participants observed that homeland security decision-making models in the federal government are often not complementary to both private and public sector objectives. Participants noted that this situation is caused, in part, by a lack of stakeholder involvement in the decision-making process, and stated that some DHS decisions have not been made in a sufficiently inclusive manner. Participants agreed that when the private sector is not sufficiently involved in risk assessments, its stakeholders lose faith in government announcements and requirements related to new risks and threats. For example, participants stated that private sector leaders have found spending DHS grant moneys difficult because they did not have access to government information and other data on terrorism to help them understand the risks. Three specifically noted that they experienced a high level of uncertainty about what actions to take to protect against terrorism because of a lack of information from the federal government related to the threats posed

by terrorism. As an example, it was noted that insurers take into account regulation and enforcement of building codes in hazard-prone areas in determining actuarially based rates that reflect risks. However, state insurance regulations may not allow them to charge these premiums. Participants agreed that improved coordination between the public and private sectors could help to mitigate disasters and improve risk management following disasters. One participant suggested that insurance premiums reflect risk and that any subsidies provided to individuals deserving special treatment should come in the form of general public funding and through artificially low insurance premiums.

- *Lack of intergovernmental partnerships.* Participants observed that intergovernmental partnerships—between federal, state, local, and tribal governments—are important for effective homeland security risk management. Participants stated that for these partnerships to succeed, it will be necessary to develop a common lexicon for communication and to reconcile the many existing risk management models that often vary by jurisdiction and homeland security mission. Participants further stated that there has not been a sufficient mobilization of state and local practitioners and experts in applying risk management principles to homeland security. They added that this lack of state and local involvement was a lost opportunity, since there is a great deal of knowledge at these levels that is largely an untapped resource. Participants also noted that congressionally authorized DHS Centers of Excellence exist, but work independently.¹³ Even within the federal government, approaches to risk management were described as fragmented. 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.

Need for Risk Management Education

Participants identified a need for increased efforts to promote risk management education, both to educate future practitioners and to inform stakeholders in the short term about the value of applying risk management to homeland security decision making. Discussion touched on the lack of risk management educators, intelligence analysts needing

¹³Centers of Excellence conduct research and education for homeland security solutions and are led by universities in collaboration with partners from other institutions, agencies, laboratories, think tanks, and the private sector.

risk analysis training, and the need for the federal government to collaborate with state and local governments in risk management education.

- *Lack of risk management educators.* Participants observed that more risk management educators and educated practitioners are needed at all levels of government. They stated that a whole new profession needs to be developed to deal with long-term risk management challenges. However, one participant noted that the nation is not currently training such a cadre of the next generation of risk management professionals.
- *Intelligence analysts need risk analysis training.* One participant said that intelligence professionals are not typically trained in risk analysis, but rather are trained to focus on fact-based versus possibility-based information. In addition, this participant noted a lack of appreciation in the intelligence community for the rationales, responsibilities, and methodologies of risk assessment. According to this participant, the result is a lack of risk-based opportunity analysis and strategic awareness within the intelligence community. For example, the participant suggested that if you ask a top intelligence analyst to explain the strategic reasons for U.S. foreign policy toward the country in which they specialize, the analyst may not know.
- *Federal government needs to collaborate with state and local governments in risk management education.* Participants observed that risk management education is a particular challenge from the perspective of state and local governments. On the one hand, participants said that the federal government has not educated state and local government agencies and police departments on the value of risk management. On the other hand, participants stated that the federal government asks other levels of government to spend money according to national priorities and grant specifications. One participant said that decision makers at the state and local levels do not have visibility over the total threat position and are asked to trust the wisdom of the federal government. Participants agreed that more effort at the federal level is needed to collaborate with state and local governments in developing commonly shared homeland security risk management models and training that can work across all levels of government and the private sector.

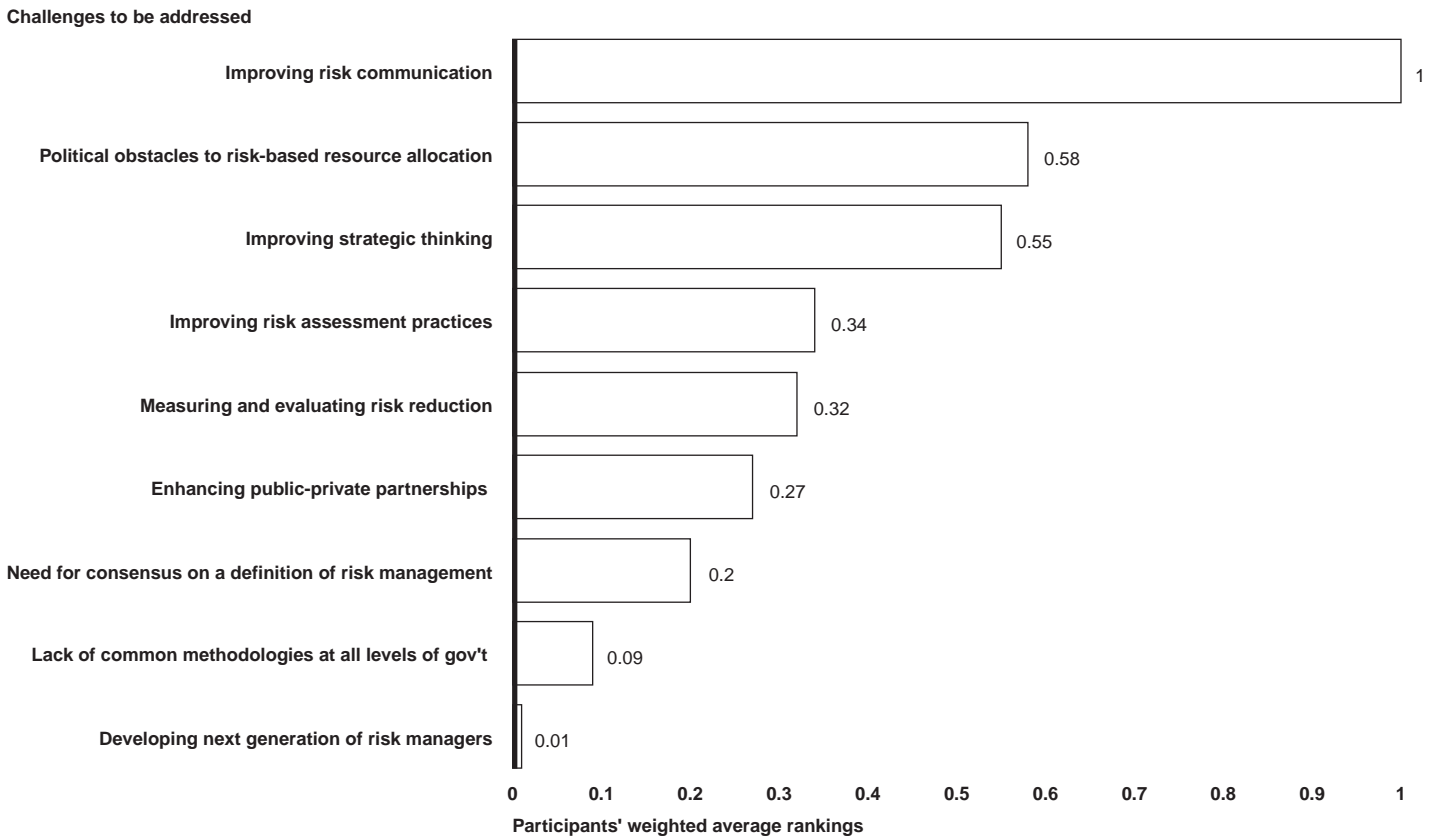
Addressing Homeland Security Risk Management Challenges

After the discussion of homeland security risk management challenges, participants discussed how to best address these challenges. Participants prioritized the order in which the identified challenges should be addressed by ranking them through a poll. Overall, participants agreed that risk communication should be addressed before all other challenges, and discussed ways in which risk communication could be used to educate and inform the public. Participants then discussed overcoming political obstacles to risk management, and provided additional suggestions to address other challenges that were identified in applying risk management principles in homeland security.

Participants Polled on Ranking the Order in Which Risk Management Challenges Should Be Addressed

Participants were asked to rank the order in which challenges to applying principles of risk management to homeland security should be addressed. Specifically, participants were asked to vote on the challenges they identified during the previous discussion three times, by indicating the challenge they believed should be addressed first, second, and third. The results paralleled those from the previous poll, with participants choosing risk communication as the challenge to be addressed first, political obstacles as the challenge to be addressed second, and improving strategic thinking as the challenge to be addressed third, as shown in figure 3.

Figure 3: Forum Polling—Rankings by Participants of Challenges in the Order They Should Be Addressed



Source: GAO analysis of participants' forum polling responses.

Note: Figure presents the weighted average rankings of the assessment by the participants of the overall order that each of the challenges should be addressed on a scale of 1 to 0, with 1 being the highest ranking and 0 being the lowest.

Using Risk Communication Practices to Educate and Inform the Public

Participants suggested increasing the dissemination of factual information to help decision makers in all sectors by empowering people with fact-based risk analysis, rather than leaving them to make decisions based on perceived risk. One participant noted that risk analysis is not about making decisions but rather about informing decisions, and that it is the role of leaders and policymakers to make decisions based on well-defined information. The participant noted that information should be provided in a way that is useful for decision making. For example, if there is time to allow people to deliberate, leaders should provide them with information to allow them to make choices; conversely, if there is no time to deliberate, leaders should instruct citizens on specific actions to take. Participants stated that engaging the public in a meaningful way involves

providing sufficient information for people to make informed decisions. In doing so, there is a need to distinguish between risks to the individual citizen and risks to the homeland.

Participants agreed that outreach to the public will help to inform and educate citizens while enhancing risk communications. The participants suggested a number of ways to inform the public effectively on risk-related issues. One participant stated that risk communication is an educational process that can be used to help the public make better decisions. Therefore, this participant said that there is a need to have a public discourse so that the public understands how risk is defined and how risk informs decision making, so that our nation ultimately reaches consensus on acceptable risk levels. Similarly, another participant noted that given differences in education and levels of understanding about risk management, it is important to develop a common lexicon that can be used for dialogue with both the layman and the subject matter expert. Participants emphasized the importance of educating elected officials and the public on risk management, including key definitions, such as that risk is a function of threat, vulnerability, and consequence. Three participants noted that such education is needed to illuminate the distinction between risk assessment, involving scientific analysis and modeling, and risk management, involving risk reduction and evaluation.

One participant noted that leadership should effectively communicate what the hazards are and the probability of those hazards occurring. The participant stated that this information will allow the public and private sectors to make informed, intelligent decisions on how to allocate resources to manage risk. According to the participant, this information will also help the public understand how government actions contribute to risk reduction efforts. The participant went on to say that leaders need to calm the public's fears while making them aware of risk, and suggested that providing this public outreach is important since the effectiveness of the government's response to a terrorist attack or natural disaster will depend on how the public behaves. Another participant offered that the equivalent of an environmental impact study could be conducted prior to implementing a new security measure or passing a new major initiative to answer questions about the long-term effect and impact an initiative will have on homeland security. Along these lines, another participant noted that public and private sector leaders need to communicate better on issues of interdependency, or the ways in which the decisions of an individual or an organization affect others. This participant explained that leaders need to show the public that if they protect asset A, it will help someone else protect asset B, and ultimately benefit everyone.

Another participant suggested that experts look at existing risk communication systems that could be used as models on which to base the development of a homeland security risk communication system. For example, the government consolidates weather-related information and informs public actions through the National Weather Service. 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 objected to the current color-coded DHS Homeland Security Advisory System¹⁴ as being too general, suggesting that the public does not understand what is meant by the recommended activities, such as being vigilant. One participant noted the importance of developing simple messages that are easy for the public to remember and pass on, citing “stop, drop, and roll” as an example of what to do if on fire.

Finally, participants stated that the events of Hurricane Katrina showed the importance of and need for a good risk communication strategy, and suggested that the nation needs a communications strategy that ties back to national homeland security objectives. Another participant agreed and added that the United States also needs a systematic assessment of threats to the country as well as a periodic assessment of the nation’s risk strategy. For this, participants suggested that stakeholders will need to be engaged to establish an acceptable level of risk for the nation.

Overcoming Political Obstacles to Risk Management

Participants were generally sympathetic to the complexity of the political process, where leaders must reconcile competing resource demands from the public as well as the sometimes conflicting priorities of the administration and members of Congress. However, participants agreed that political obstacles to applying principles of risk management to homeland security can be overcome by highlighting the importance of risk management to policymakers. One participant pointed out that a new administration and Congress will soon enter office with a new set of policy

¹⁴Homeland Security Presidential Directive 3 established the Homeland Security Advisory System in March 2002 as a mechanism to inform and facilitate decisions related to securing the homeland among various levels of government, the private sector, and American citizens. The Homeland Security Advisory System comprises five color-coded threat conditions, which represent levels of risk related to potential terror attack: red, or severe alert; orange, or high alert; yellow, or elevated alert; blue, or guarded alert; green, or low alert. See also GAO, *Homeland Security: Communication Protocols and Risk Communication Principles Can Assist in Refining the Advisory System*, GAO-04-682 (Washington, D.C.: June 25, 2004).

objectives, and it will be important to highlight the importance of risk management to incoming policymakers and to persuade them to discuss it. Another participant stated that policymakers should gain a better understanding of what has worked and what has not worked in the private sector to stop simply reacting to past events by better anticipating and preparing for probable future events. Finally, another participant stated that policymakers are actually doing risk management every day; however, corporate executives and government officials do not refer to it as such. According to this participant, risk is considered within the current political process when leaders choose funding levels for the armed services. Recognizing the nature of these discussions could open the way to making risk management a more widely accepted and applied approach to decision making.

Additional Suggestions to Address Other Identified Challenges

Participants discussed additional suggestions to address three other homeland security risk management challenges that had been mentioned: improving strategic thinking, using risk assessments as a tool for decision making, and enhancing information sharing through public-private partnerships.

- *Improve strategic thinking.* One participant suggested that strategic thinking could be improved by defining a problem statement that answers several questions, including the purpose for which we are trying to develop risk management practices, what decisions leadership must make and those they wish to make, and what decisions we as a nation want to make and what decisions we are prepared to make. This participant noted that effective institutions already know the answers to these questions and that risk assessment tools are developed in support of these strategic questions. A second participant agreed, suggesting a need to focus on defining the problem, a set of principles to guide decisions, goals in addressing the problem, and the trade-offs required to achieve these goals. Another participant said there is a need for strategic planning, and that a short-term goal in this process should be identifying the big problems that strategic planning needs to address, such as the direct and indirect costs to reducing risk.
- *Use risk assessments as a tool for decision making.* Participants agreed that risk assessments are useful tools that can be used to inform decisions made by business leaders and policymakers. One participant proposed the development of models using classified information that the public and private sector could use for purposes such as determining regional risk indicators—for example, the risk to New

York City relative to Des Moines. Six participants discussed the availability and utility of information required to inform the three components of risk—defined as a function of threat, vulnerability, and consequence. One participant stated that consequence is the best understood variable of risk, while another disagreed, stating that even consequence is not well understood within the risk framework. One participant noted the importance of specifying the assumptions that are made by experts in undertaking risk assessments, the nature of disagreements between experts on the assessment of specific risks, and the degree of uncertainty surrounding these estimates.

- *Enhance information sharing through public-private partnerships.* Participants agreed that partnerships between the public and private sectors can enhance information sharing and need to result in structured communications that address the goals of diverse groups. According to one participant, the amount of information the private sector receives from governments is extremely important for corporate resource allocation decisions. For example, this participant estimated that corporate security costs in the retail property industry have increased from 5 percent of operating costs before September 11, 2001, to 20 percent today. It was suggested that government provide businesses with a quarterly or biannual threat briefing, or possibly provide direct access to public officials who can provide threat information.

Suggested Next Steps

Participants concluded the forum by reasserting the importance of using risk-based principles to inform decision making related to homeland security. Participants further stated their desire that additional action be taken to move forward on the areas discussed at the forum, and proposed a number of steps that could be taken in the near future to strengthen homeland security risk management practices and stimulate public discussion and awareness of risk management concepts. Suggestions included the creation of a nonpartisan advisory board, identifying effective risk management practices, reviewing DHS's risk management efforts, and developing a white paper to guide Congress's and the administration's understanding of risk-based principles.

Create an Advisory Board

In general, forum participants agreed that a nonpartisan federal advisory board could be created and composed of a subset of the group of participants. They suggested that such an advisory board could assist the federal government in thinking about risk management strategies and in moving forward in applying risk-based principles related to homeland security. Participants emphasized that the leadership of a group of this kind was essential and must be sufficiently positioned so that the board could appropriately support decision makers.

Develop a List of Effective Practices

Participants agreed that there is a need for further exchanges of effective practices in risk management among stakeholders. The forum participants considered reconvening to outline existing effective practices, lessons learned, and even risk management models considered to be controversial. It was suggested that the audience for the outcome of such a meeting could be OMB and the staff of the next administration.

Review DHS's Risk Management Efforts

Participants suggested that there would be value in conducting an overarching review across all DHS offices to determine the current status of all DHS approaches to applying risk management practices in homeland security. Participants suggested that DHS could brief the advisory board noted above on steps taken and progress made in risk management. The advisory board could then provide advice and guidance to DHS, for example, by assessing the gap between DHS's current risk management efforts and known effective practices, including suggestions discussed at the forum.

Develop an Informational White Paper

Participants discussed forming working groups dedicated to developing an informational white paper for decision makers prior to the 2008 elections. Such a white paper would stress the necessity of risk management and describe an approach for applying risk management to homeland security. More specifically, participants discussed the white paper addressing issues such as (1) risk management actions already taken by DHS, (2) examples of effective practices used in the private sector, and (3) specific issues that appropriations staff should take into account before authorizing new expenditures. Participants stated that such a document should be written in accessible language free of technical jargon and offer concrete actions to inform and empower both the public and the private sectors.

Appendix I: Agenda

8:30 a.m.	Check-in/Continental breakfast
8:45 a.m.	Opening session Welcome and Introductions Setting the Stage
9:15 a.m.	Session I: Presentation on effective risk management practices used by leading organizations
9:30 a.m.	Group discussion: What lessons learned from the public and private sectors can inform risk management efforts in homeland security?
10:30 a.m.	Break
10:45 a.m.	Session II: Presentation on the homeland security risk management challenges faced by federal agencies
11:00 a.m.	Group discussion: What are the greatest homeland security risk management challenges facing the public and private sectors?
12:30 p.m.	Break/Buffer Lunch Open
12:45 p.m.	Session III (working lunch): Moderated discussion on ways to strengthen homeland security risk management practices
2:00 p.m.	Wrap-up
2:30 p.m.	Adjournment

Appendix II: 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 III: Presentation by Norman Rabkin, Managing Director, Homeland Security and Justice, GAO

The forum opened with remarks by Norman Rabkin that provided an overview of the United States' current fiscal crisis and the importance of using risk management to focus resources on our most pressing concerns.



Source: GAO.




Addressing Homeland Security Risks: Complexities and Costs

- The terrorist attacks of September 11, 2001, and the catastrophic natural disasters wrought by Hurricanes Katrina and Rita in 2005 demonstrated the diverse nature of homeland security risks
- The nation will never be completely safe, and total security is an unachievable goal; we cannot afford to protect everything against all threats

2

Source: GAO.



Potential Fiscal Outcomes Under Baseline Extended (January 2001)

Revenues and Composition of Spending as a Share of GDP

Percent of GDP

Fiscal year	Net interest	Social Security	Medicare & Medicaid	All other spending
2005	~5%	~5%	~5%	~5%
2015 ^a	~5%	~5%	~5%	~5%
2030 ^a	~5%	~5%	~5%	~5%
2040 ^a	~5%	~5%	~5%	~5%

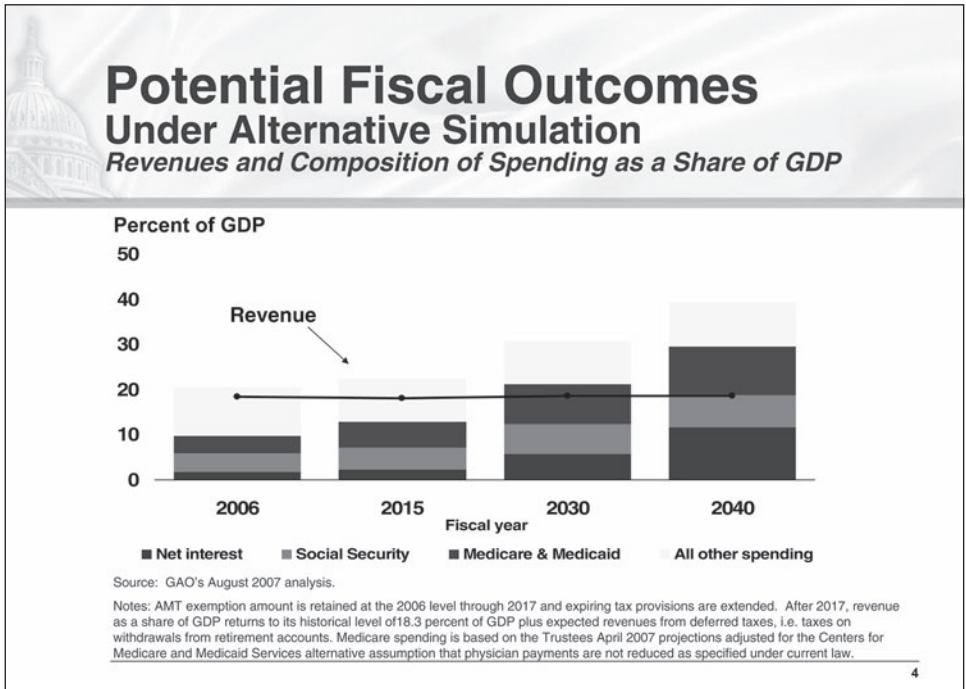
Fiscal year

■ Net interest ■ Social Security ■ Medicare & Medicaid ■ All other spending

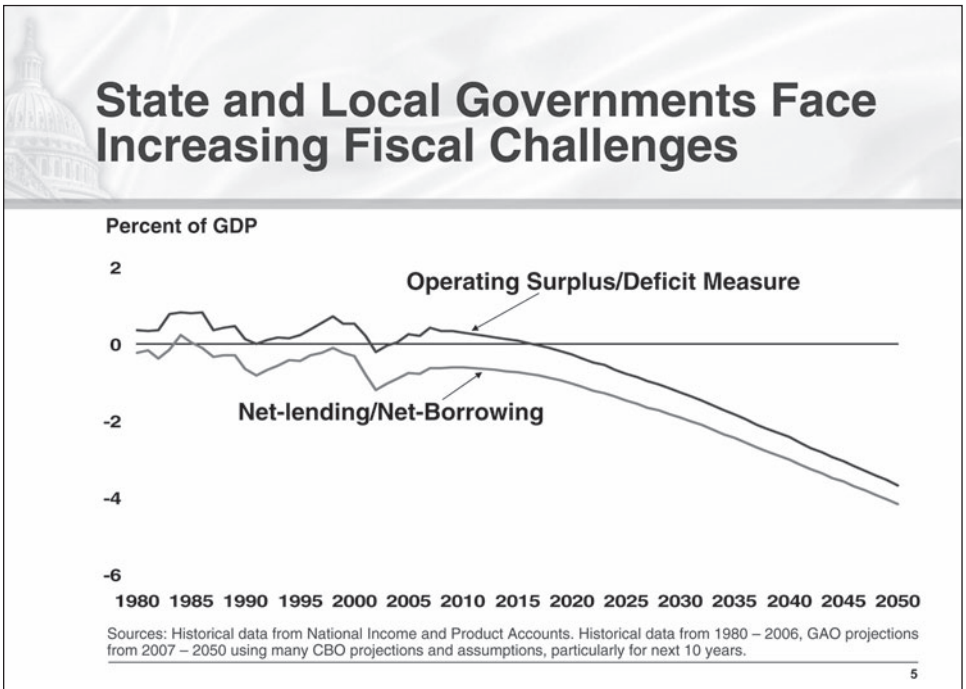
Source: GAO's January 2001 analysis.
^aAll other spending is net of offsetting interest receipts.

3

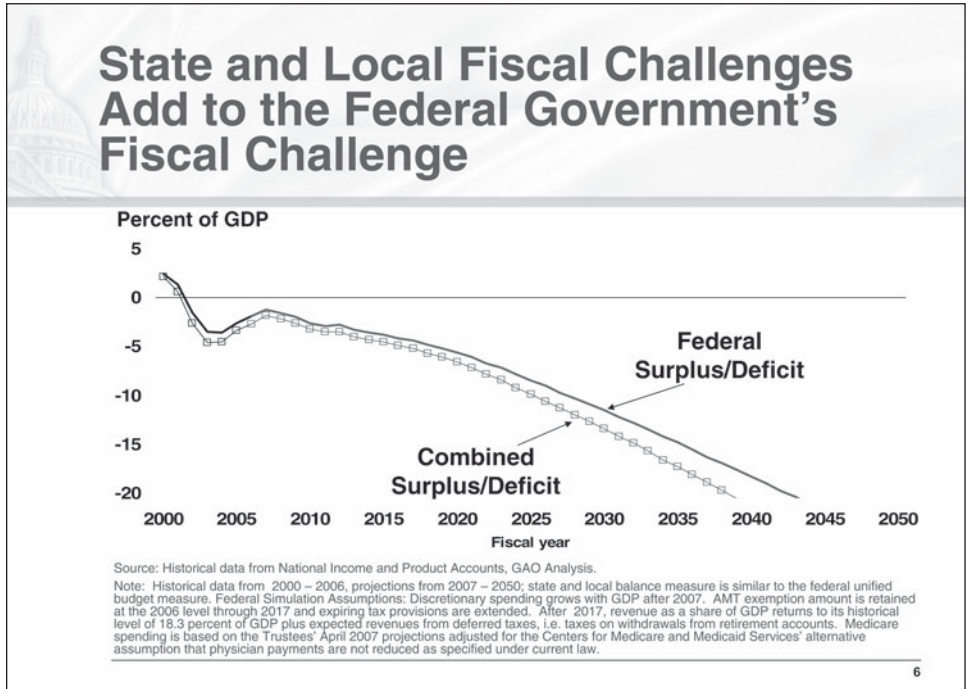
Source: GAO.



Source: GAO.



Source: GAO.



Source: GAO.

Risk Management Can Improve Resource Allocation

- Using approaches that may not consider risk, such as Congressional direction (earmarks), compound these potential fiscal outcomes
- Congress, the President, and the Secretary of DHS have endorsed risk management
- DHS is making progress in applying risk management to guide its operational and resource allocation decisions

7

Source: GAO.

GAO's Risk Management Framework

- Risk management is a strategic process for helping policy makers allocate finite resources
- Consists of 5 phases: setting strategic goals and objectives, assessing risks, evaluating alternatives, management selection, and implementing and monitoring results

Source: GAO.

8

Source: GAO.

Moving Forward: Challenges in Using Risk Management

- Applying risk management to a homeland security context is a relatively new endeavor
- Choices must be made about protection priorities given the risk and how to best allocate available resources
- Strengthening the use of risk management principles in homeland security remains a challenge for many stakeholders

9

Source: GAO.



Using Your Input to Frame the Discussion

- We polled you on challenges in applying risk management to homeland security and actions to address them
- 100 percent response rate
- Your input has been used to shape our agenda and discussion sessions
- We will share results with you in later sessions

10

Source: GAO.



Key Issues in Strengthening the Use of Risk Management in Homeland Security

- What lessons can be learned from leading organizations about the effective use of risk management practices?
- What are the key challenges faced by public and private organizations in adopting and implementing a risk-based approach for homeland security?
- What actions should be taken in the near- and long-term to address the most pressing of these challenges?

11

Source: GAO.

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Norman J. Rabkin, (202) 512-3610, 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; Brett Collins; Amber Lopez; and Emily Rachman managed all aspects of the work, and Jason Barnosky, Chuck Bausell, Kathryn Bolduc, Valerie Colaiaco, Deborah Knorr, Stan Kostylya, Flavio Martinez, Linda Miller, Mona Nichols Blake, Jamie Roberts, April Thompson, 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 Sectors. [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.

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