



TESTIMONY

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND
HOMELAND SECURITY
TRANSPORTATION AND
INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

[Jump down to document](#) ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

[Browse Books & Publications](#)

[Make a charitable contribution](#)

For More Information

Visit RAND at www.rand.org

Explore [RAND Testimony](#)

View [document details](#)

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND PDFs to a non-RAND Web site is prohibited. RAND PDFs are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see [RAND Permissions](#).

TESTIMONY

Challenges of Applying Risk Management to Terrorism Security Policy

HENRY H. WILLIS

CT-310

June 2008

Testimony submitted for the record to the House Homeland Security Committee,
Subcommittee on Transportation Security and Infrastructure Protection on June
24, 2008

This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.



Published 2008 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665

RAND URL: <http://www.rand.org>

To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Henry H. Willis¹
The RAND Corporation

Challenges of Applying Risk Management to Terrorism Security Policy²

**Submitted for the Record to the Committee on Homeland Security
Subcommittee on Transportation Security and Infrastructure Protection
United States House of Representatives**

June 24, 2008

Madame Chair and distinguished members of the subcommittee, thank you for the opportunity to submit this written testimony for the statement of record.

In the six years since the formation of the Department of Homeland Security (DHS), the Department has adopted risk management as an organizing principal that should be used to inform prioritization of missions and allocation of precious resources (DHS 2005). This proclamation by Secretary Michael Chertoff provided a direction, but not the means to get the job done.

Subsequent efforts from within and outside DHS have helped to develop the foundational concepts upon which risk analysis of terrorism security is built: terrorism risk only exists when a person or group has the *capability* and *intent* to present a *threat* of attack on a *vulnerable* target in a manner which would have *consequences* of concern to citizens of the United States (for example, see Willis et al. 2005 and DHS 2006). While these definitions provide a common starting point for discussions of terrorism security, risk analysis is still not consistently used as a means of connecting program activities to budget priorities.

No where is the need for a cross-cutting analysis of budget priorities and risk management more urgently needed than in the Office of the Secretary, where the multiple and diverse program efforts must be integrated into a coherent and rational set of management objectives. Absent a coherent approach for evaluating risk management strategies, it is particularly difficult to communicate with Congressional oversight committees about what tradeoffs may be involved in funding programs of particular interest to specific committees.

¹ The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

² This testimony is available for free download at <http://www.rand.org/pubs/testimonies/CT310/>.

To build such a coherent approach it is necessary to recognize that:

- Risk analysis can provide structure to analysis of many types of problems;
- Each application may require different analytic methods; and
- Developing and applying these methods requires addressing several fundamental analytic challenges.

Risk Analysis Provides Structure to Decisionmaking

Risk analysis is a process for understanding the type and extent of events that can cause harm and helping us make and implement decisions about these events for the purpose of improving the quality of our lives.

Along these lines, a number of organizations have proposed approaches for using risk analysis in public policy problems. Some recent examples of such approaches include those proposed by the Canadian Standards Association (CSA 2007) and the Intergovernmental Council on Risk Governance (IRGC 2005). Though these and other examples have many aspects in common, applications of risk analysis consistent with them are quite diverse.

In traffic safety, the Department of Transportation used risk analysis to guide regulations regarding seat belts and air bags. In air quality, the Environmental Protection Agency relied on risk analysis to set standards for emissions of pollutants that increase the incidence of chronic pulmonary diseases like asthma and emphysema. In nuclear reactor safety, the Nuclear Regulatory Commission uses risk analysis as a guide in processes for permitting and oversight of power plant operations. In areas of natural resources management, multiple state and federal agencies use risk analysis is used to balance ecological impacts from competing interests of fisheries, timber harvesting, and outdoor recreational enthusiasts. Finally, in the domain of security, military and law enforcement agencies used risk analysis to identify and mitigate vulnerabilities in facility designs and standard operating procedures.

Given the broad range of missions associated with terrorism security, it is perhaps not surprising that within the problems addressed by the Department of Homeland Security alone it is possible to identify the use of risk analysis for studying a similarly diverse range of topics. Review of recent studies by the RAND Corporation provide examples of this such as assessments of technologies to counter the threat to commercial aviation from shoulder fired missiles (Chow et al. 2005); use of equipment to protecting emergency responders at disasters and terrorist events (Willis et al. 2006); prioritization of resources for protecting critical infrastructure (Wilson et al. 2007;

Greenberg et al. 2006); justification of increased inspections of shipping containers (Martonosi et al. 2005); and similarly for improving security of travel documents (Willis and LaTourrette 2008).

Analysts have only been applying risk analysis to these types of problems of terrorism security like these for a few years. In doing so DHS has made progress, but fundamental analytic challenges remain. These challenges can be divided into three areas: assessing terrorism risk; assessing alternatives for managing terrorism risk; and building capacity for risk-informed decisionmaking.

Challenges of Assessing Terrorism Risk

The challenges of assessing terrorism risk stem from uncertainties inherent in specifying each of the factors that determine terrorism risk; threat, vulnerability, and consequences.

The most uncertain factor surrounding terrorism risk relates to threat – when, where and how will terrorists choose to attack next. It is difficult to anticipate changes in terrorists' intentions and capabilities, yet the intelligence community directs significant effort to providing answers to exactly these types of questions. The challenge this poses for risk analysis is how to link efforts of intelligence analysis with efforts to estimate and manage terrorism risks.

Where threats are suspected, it is necessary to understand the vulnerabilities of infrastructure and facilities to attack. For example, operators of airports, shipping ports, chemical plants, and entertainment resorts spend significant effort trying to understand where attacks against their properties would be most damaging and most difficult to prevent. This type of analysis requires detailed consideration of how facilities are designed and how operations occur at them. This becomes a daunting task when one considers that there are many thousands of factories, airports, train stations, water treatment plants, hotels, shopping malls, and other types of infrastructure across the country. The challenge this presents is the need to develop practical means of analyzing vulnerabilities given the feasible limits of time and people available to conduct assessments.

Finally, the consequences of terrorism may be far reaching and distributed over time, places, and sectors of the economy, making their specification particularly daunting. The direct consequences of terrorism come to mind quickly. On September 11, 2001 more than 3,000 people died, many others were injured, and tens of billions of dollars of property was destroyed. However, the consequences of terrorism extend beyond these direct effects. Consequences can propagate through interconnections of infrastructure and social amplification of risk through behavioral

systems. For example, consider how disruptions to power supply can trigger disruptions to all industries that rely on power or how the reactions to terrorism led some people to change vacation plans or choose not to fly in the months following September 2001. While the existence of such indirect effects is recognized, they are not well understood. Thus, the challenge is developing means to estimate the magnitude of indirect consequences of terrorism through empirically validated analysis.

Challenges of Assessing Terrorism Risk Management Alternatives

The factors that define terrorism risk also present challenges to assessing management strategies, because opportunities exist to reduce terrorism risk through each factor.

Some efforts to manage terrorism risk are intent on changing terrorist intentions to attack. For example, a common goal of surveillance efforts in border security is to deter illicit activities involving the transport of goods or people across borders. However, experience with efforts to combat cross border drug trafficking suggest that increased surveillance may be more likely to change where illicit border crossers travel than deter them from attempting at all.

Terrorism security can also reduce risk by eliminating vulnerabilities. For example, increased use of traffic barriers or surveillance cameras could be expected to make it more difficult for terrorists to attack government buildings. However, experience of the United Kingdom in countering the Irish Republican Army (IRA) emphasizes that adversaries adapt use of technology and tactics in response to security measures. Thus, it is difficult to assess how long benefits of terrorism security can be anticipated to last (Jackson et al. 2007).

In other instances, the most effective risk management approach is to launch an effective response. For example, through the Cities Readiness Initiative, the Department of Health and Human Services intends to help communities prepare to conduct mass dispensing operations of medical countermeasures to reduce fatalities from public health disasters like large anthrax releases. However, research has demonstrated that the success of efforts like these depends in large part on how the public will respond. For example, following the anthrax attacks in the fall of 2001, a study of postal workers exposed in Washington, DC found that a disproportionate number did not take the antibiotics that were given to them (Stein et al. 2004).

This raises basic questions about how people will respond more generally in the aftermath of a disaster. Will people report to dispensing locations as directed? Will they comply with recommendations to take the distributed medications? The public response to terrorist events is

not well understood, this additional effort is needed to understand how to communicate with the public most effectively during disasters.

Finally, it is well understood that the complexity of countering an adaptive adversary requires a layered defense. For example, securing borders requires efforts at controlled ports of entry, uncontrolled land borders and interior enforcement. This means that it is not meaningful to assess the benefits of any one security measure on its own. Thus, as analytic processes are used to connect budgets to program activities it is necessary to develop means of evaluating portfolios of programs and security measures.

Building Capacity for Risk Informed Decisionmaking at DHS

Because as a country, we face uncountable risks but have limited resources, it is necessary to consider the cost effectiveness of federal policies, regulations, and programs. Terrorism security is no different and risk analysis can be used to hold programs accountable to standards for effectiveness of risk management. However, as risk analysis continues to develop through DHS, it is important to recognize three characteristics of the challenge DHS faces.

First, as illustrated above, terrorism security must address many different types of risk. Thus, it is unrealistic to assume that there is a single model or approach that can be used to answer all risk management problems or that a single organization will be capable of providing answers to all risk analysis problems. A more pragmatic view is that analytic approaches must be attuned to the decisions that they are designed to inform and the questions they are designed to answer. Similarly, it is appropriate that all who take responsibility in making these decisions share the responsibility for developing and improving the analytic methods used to inform the decisions.

Second, the notion of a cold, analytic, actuarial risk assessment is largely a myth. Risk is a social construct that incorporates value judgments about context and cause. Plainly stated, we tend to feel differently ,and have different expectations about government action, about 20 people dying from an anthrax attack in a single city than we do about the same number of people dying in car crashes across the U.S. The point is that risk management requires both an analytic and deliberative process (NRC 1994) that allows the public to discuss and decide how much emphasis should be placed on terrorism security as opposed to managing other types of risk. Efforts to assess and manage terrorism risk will also need to foster public discussions of the value judgments inherent to terrorism security.

Finally, terrorism risk analysis presents many novel analytic challenges which have only been considered recently, so represents a profession whose methods will take some time to mature. This testimony began by providing examples of how risk analysis is used in other parts of the U.S. government. In each of these cases, it has taken decades to develop and integrate methods of risk analysis into decisionmaking. While it is not possible to wait decades for methods to mature before making risk management decisions to protect the country from terrorism, it is necessary to continue building the capacity required to improve the analytic capabilities to support decisionmaking. These investments are needed to develop tools, organizations and people. The investments are necessary to build capacity within components of DHS like the Transportation Security Administration, Customs and Border Protection, Federal Emergency Management Agency, U.S. Coast Guard, and the DHS Offices of Policy, Management, Risk Management and Analysis, and Program Analysis and Evaluation. However, it is also needed directly within the Secretary's office to provide authoritative guidance on the application of risk analysis to cross cutting issues. Continued investment is also needed in the organizations supporting analysis at DHS, like its FFRDCs, to build capacity to provide critical support to the Department.

Risk Analysis Can Help DHS Improve Terrorism Security

None of the challenges I have described briefly here can be overcome easily. If they were, the dedicated public servants at DHS and throughout other parts of federal, state and local governments would certainly have solved them all. However, as Congress and the Administration continue to work to solve problems presented by terrorism, it will be prudent to keep all of these challenges in mind and along the way. Specifically, DHS and Congress should:

- Recognize that the component agencies of DHS must develop new methods of risk analysis to support their own decisionmaking and encourage them to do so.
- Initiate open and informed public discourse on the tradeoffs that must be made when setting priorities for terrorism security.
- Invest in the organizations and people that will provide the capacity for applying risk analysis to connect terrorism security missions to budget priorities, especially in support of the Office of the Secretary of Homeland Security.

References Cited

Chow, J. S., J. Chiesa, P. Dreyer, M. Eisman, T. W. Karasik, J. Kvitky, S. Lingel, D. Ochmanek, C. Shirley (2005). *Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat*. OP-106-RC, RAND Corporation, Santa Monica, CA.

CSA (2007). *Risk Management: Guideline for Decision Makers*. CAN/CSA-Q850-97 (R2007). Canadian Standards Association, Mississauga, Ontario.

DHS (2005). *Remarks for Secretary Michael Chertoff U.S. Department of Homeland Security George Washington University Homeland Security Policy Institute*. March 16, Washington, DC. Available online at http://www.dhs.gov/xnews/speeches/speech_0245.shtm as of June 19, 2008.

DHS (2006). *National Infrastructure Protection Plan*. Department of Homeland Security, Washington, DC. Available on line at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf as of June 19, 2008.

Greenberg, M., P. Chalk, H. H. Willis, I. Khilko, D. S. Ortiz (2006). *Maritime Terrorism: Risk and Liability*. MG-520-CTRMP. RAND Corporation, Santa Monica, CA.

IRGC (2005). *IRGC White Paper No1: Risk Governance – Towards an Integrative Approach*. International Risk Governance Council, Geneva.

Jackson, B. A., P. Chalk, K. Cragin, B. Newsome, J. V. Parachini, W. Rosenau, E. M. Simpson, M. Sisson, D. Temple (2007). *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*. MG-481-DHS. RAND Corporation, Santa Monica, CA.

Martonosi, S. E., D. S. Ortiz, H. H. Willis (2005). Evaluating the viability of 100 percent container inspections at America's ports. In H.W. Richardson, P. Gordon and J.E. Moore II, *The Economic Impacts of Terrorist Attacks*. Cheltenham, UK: Edward Elgar Publishing.

NRC (1994). *Science and Judgment in Risk Assessment*. Committee on Risk Assessment of Hazardous Air Pollutants, Board on Environmental Studies and Toxicology, Commission on Life Sciences, National Research Council, National Academy Press, Washington, DC.

Stein, B.D., T.L. Tanielian, G.W. Ryan, H. J. Rhodes, S. D. Young, and J. C. Blanchard (2004). A Bitter Pill to Swallow: Nonadherence with Prophylactic Antibiotics During the Anthrax Attacks and the Role of Private Physicians. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice and Science*, Volume 2, Number 3, 175 – 185.